Хабаровское отделение Федерального государственного бюджетного
учреждения науки Института прикладной математики
Дальневосточного отделения Российской Академии наук

На правах рукописи

Илларионов Андрей Анатольевич

Статистические свойства полиэдров Клейна и локальных минимумов решеток

01.01.06 — математическая логика, алгебра и теория чисел

Диссертация
на соискание ученой степени
доктора физико-математических наук

Научный консультант:
д.ф.-м.н., чл.-корр. РАН Быковский В.А.

Хабаровск – 2014

Оглавление

Предисловие **3**

Обозначения и соглашения **4**

Введение **6**
§ 1. Актуальность темы 6
§ 2. Основные определения 8
§ 3. Основные результаты 13

Глава I. **Оценки максимального количества локальных минимумов** **23**
§ 1. Вспомогательные оценки 23
§ 2. Оценки количества относительных минимумов 27
§ 3. Оценки количества локальных минимумов 33

Глава II. **Асимптотическое распределение целочисленных матриц** **37**
§ 1. Формулировка основного результата 37
§ 2. Вспомогательные результаты 41
§ 3. Вычисление некоторых сумм 46
§ 4. Доказательство теоремы 1.1 52

Глава III. **Среднее количество относительных минимумов** **63**
§ 1. Двумерный случай 64
§ 2. Трехмерный случай 66
§ 3. Случай произвольной размерности 72
§ 4. Оценки постоянной $\mathcal{C}(s)$ 79

Глава IV. **Статистические свойства многогранников Клейна** **82**
§ 1. Оценки количества элементов многогранников Клейна 83
§ 2. Среднее количество граней фиксированного типа 89
§ 3. Среднее количество вершин 98

Глава V. **Среднее количество цилиндрических минимумов и наилучших приближений линейных форм** **106**
§ 1. Базис Вороного и его свойства 106
§ 2. Среднее количество цилиндрических минимумов. 112
§ 3. Среднее количество наилучших приближений линейных форм 114

Глава VI. **Среднее количество локальных Ф-минимумов** **123**
§ 1. Дополнение локального минимума до базиса: частные случаи 124
§ 2. Дополнение локального минимума до базиса 128
§ 3. Среднее количество локальных минимумов 134

Приложения **137**
§ 1. Приложение к главе V 137
§ 2. Приложение к главе VI 149

Литература **158**

Предисловие

В конце 19 века были предложены два обобщения алгоритма непрерывных дробей на многомерный случай. Одно Ф. Клейном, а другое Г.Ф. Вороным и независимо от него Г. Минковским. Они основаны на рассмотрении полиэдров Клейна и, соответственно, локальных минимумов решеток. Ряд задач теории чисел (построение основных единиц числовых полей, нахождение наилучших приближений, оценки погрешности теоретико-числовых квадратурных формул и отклонений сеток от равномерного распределения) приводят к исследованию этих конструкций. Статистические свойства локальных минимумов и полиэдров Клейна *двумерных* решеток непосредственно вытекают из теории непрерывных дробей. Однако, несмотря на значительный интерес, практически отсутствуют результаты для решеток размерности три и выше. Восполнению этого пробела и посвящена настоящая работа.

В диссертации разработан метод исследования статистических свойств многомерных непрерывных дробей по Клейну и Вороному – Минковскому. Он позволил ответить на некоторые вопросы В.И. Арнольда о свойствах полиэдров Клейна и получить ряд асимптотических формул для средних характеристик локальных минимумов, которые можно рассматривать, как многомерные обобщения классических результатов о вероятностных свойствах цепных дробей. К основным можно отнести следующие результаты диссертации.

1. Доказаны правильные, с точностью до констант, зависящих от размерности, оценки для максимального количества относительных минимумов целочисленных неполных решеток и относительных минимумов неполных (нецелочисленных) решеток, лежащих в заданном кубе. Также получены двусторонние оценки для среднего количества вершин полиэдров Клейна целочисленных решеток с фиксированным определителем.

2. Впервые изучено поведение в среднем количества локальных минимумов многомерных целочисленных решеток. А именно, получена асимптотическая формула для среднего числа локальных минимумов целочисленных многомерных решеток с определителем из заданного отрезка. Также доказано многомерное обобщение классической теоремы Хейльбронна о средней длине конечной непрерывной дроби в терминах относительных минимумов.

3. Получены асимптотические формулы для среднего числа граней фиксированного типа и вершин полиэдров Клейна трехмерных целочисленных решеток фиксированного определителя.

4. Выведены асимптотические формулы для среднего числа наилучших приближений линейных форм с рациональными коэффициентами и математического ожидания количества наилучших приближений форм с вещественными коэффициентами.

Обозначения и соглашения

Главы диссертации разделены на параграфы, нумерация которых начинается заново в каждой главе. Формулы n-го параграфа любой главы нумеруются (n.1), (n.2), (n.3) и т. д. (номер главы не указывается). Аналогичная нумерация используется для теорем, лемм, следствий и замечаний. При ссылке на формулу (теорему, лемму и т.д.) других глав указывается номер этой главы. Считаем, что введение — это глава с номером 0, а приложение — глава с номером A. Например, теорема V.1.1 — это теорема 1.1 из главы V, формула (0.1.1) — это формула (1.1) из введения, лемма A.2.1 — это лемма 2.1 из приложения.

На протяжении всей диссертации используются следующие обозначения:

$\#S$ — количество элементов конечного множества S;

$\mathbb{Z}_+$ — множество неотрицательных целых чисел;

$\mathbb{R}_+$ — множество положительных вещественных чисел;

∂U и $\overline{U}$ — граница и замыкание множества U;

если $x = (x_1, \dots, x_s) \in \mathbb{R}^s$, $p \in [1, +\infty)$, то

$$|x|_p = \left(\sum_{i=1}^{s} |x_i|^p \right)^{1/p}, \quad |x|_\infty = \max_{1 \le i \le s} |x_i|, \quad |x| = |x|_2;$$

mes — мера Лебега;

$\mu(n)$ — функция Мебиуса;

$\zeta(s)$ — дзета-функция Римана;

$\sigma_\alpha(n) = \sum\limits_{d|n} d^\alpha$ (сумма по делителям d натурального n);

нод $(n_1, \dots, n_s)$ — наибольший общий делитель целых $n_1, \dots, n_s$.

$\mathrm{M}_{t,s}(Q)$ — множество матриц размера $t \times s$ с элементами из числового множества Q;

$\mathrm{M}_s(Q) = \mathrm{M}_{s,s}(Q)$;

$\mathrm{M}_s(\mathbb{Z}; N)$ — множество матриц $M \in \mathrm{M}_s(\mathbb{Z})$ таких, что $\det M = N$;

$\mathrm{GL}_s(\mathbb{R})$ — множество невырожденных матриц из $\mathrm{M}_s(\mathbb{R})$;

$\mathrm{GL}_s(\mathbb{Z})$ — множество унимодулярных матриц из $\mathrm{M}_s(\mathbb{Z})$;

если не указано противное, то элементы матрицы X обозначаем через x_{ij} (i — номер строки, j — номер столбца);

если $x_{ij} \in \mathbb{R}$, $x_i^{(j)} \in \mathbb{R}$, $i = \overline{1,t}$, $j = \overline{1,s}$, то

$$(\!(x_{ij})\!) = \begin{pmatrix} x_{11} & \dots & x_{1s} \\ \vdots & & \vdots \\ x_{t1} & \dots & x_{ts} \end{pmatrix}, \quad (\!(x_i^{(j)})\!) = \begin{pmatrix} x_1^{(1)} & \dots & x_1^{(s)} \\ \vdots & & \vdots \\ x_t^{(1)} & \dots & x_t^{(s)} \end{pmatrix},$$

— матрицы из $\mathrm{M}_{t,s}(\mathbb{R})$.

Через $\mathcal{L}_{t,s}(\mathbb{R})$ обозначаем множество всех s-мерных вещественных решеток ранга t ($t \le s$). Любая решетка $\Gamma \in \mathcal{L}_{t,s}(\mathbb{R})$ имеет вид

$$\Gamma = \left\{ n_1 a^{(1)} + \ldots + n_t a^{(t)} : \ \ n_i \in \mathbb{Z},\ i = \overline{1,t} \right\},$$

где $a^{(1)}, \ldots, a^{(t)}$ — некоторые линейно-независимые векторы из $\mathbb{R}^s$ (базис Γ). Матрицу со столбцами ${a^{(1)}}^T, \ldots, {a^{(t)}}^T$ будем называть базисной. Если $t = s$, то решетка называется полный, если $t < s$, то неполной. Модуль определителя базисной матрицы полной решетки называется определителем решетки и обозначается $\det \Gamma$.

Используем следующие обозначения, связанные с решетками:

$\mathcal{L}_{t,s}(\mathbb{Z})$ — множество целочисленных решеток из $\mathcal{L}_{t,s}(\mathbb{R})$;

$\mathcal{L}_s(Q) = \mathcal{L}_{s,s}(Q)$, где $Q = \mathbb{R}$ или $Q = \mathbb{Z}$;

$\mathcal{L}_s(\mathbb{Z}; N)$ — множество решеток $\Gamma \in \mathcal{L}_s(\mathbb{Z})$ таких, что $\det \Gamma = N$;

$\mathcal{L}_s(\mathbb{Z}; [1, R])$ — множество решеток $\Gamma \in \mathcal{L}_s(\mathbb{Z})$ таких, что $\det \Gamma \in [1; R]$;

$\mathcal{R}_s(N) = \#\mathcal{L}_s(\mathbb{Z}; N)$;

$\mathcal{R}_s[1, R] = \#\mathcal{L}_s(\mathbb{Z}; [1, R])$.

Запись

$$f(x) \ll g(x) \quad (\text{либо } f(x) = O(g(x))) \qquad \text{при } x \in X$$

означает, что существует такая абсолютная постоянная $C > 0$, что для любого $x \in X$ имеет место оценка $|f(x)| \le C \cdot g(x)$. Если C зависит от параметра θ, то пишем $f(x) \underset{\theta}{\ll} g(x)$ (либо $f(x) = O_\theta(g(x))$). Запись $f \asymp g$ означает что $f \ll g \ll f$.

Гиперповерхность $S \subset \mathbb{R}^s$ называем кусочно-дифференцируемой, если она состоит из фиксированного числа гиперповерхностей класса C^1.

Множество $K \subset \mathbb{R}^n$ называем конусом, если $\lambda x \in K$ для всех $\lambda \in \mathbb{R}_+$, $x \in K$.

Функция $f : \mathbb{R}^n \to \mathbb{R}$ называется лучевой, если для всех $x \in \mathbb{R}^n \setminus \{0\}$, $\lambda \in \mathbb{R}$

$$0 < f(x); \qquad f(\lambda \cdot x) = |\lambda| \cdot f(x).$$

Введение

§ 1. Актуальность темы

Любое вещественное α единственным образом раскладывается в непрерывную (цепную) дробь:

$$\alpha = [q_0; q_1, q_2, \ldots, q_n, \ldots] = q_0 + \cfrac{1}{q_1 + \cfrac{1}{q_2 + \ldots + \cfrac{1}{q_n + \ldots}}},$$

где $q_0 = [\alpha]$ (целая часть) и $q_n = q_n(\alpha) \in \mathbb{N}$ (неполные частные). Она конечна только для рационального $P/Q = [q_0; q_1, \ldots, q_l]$ и в этом случае накладываем дополнительное условие: $q_l \geq 2$. Несократимая дробь

$$\frac{P_n}{Q_n} = [q_0; q_1, \ldots, q_n] \quad (n \geq 0)$$

называется n-й подходящей для α.

Алгоритм разложения вещественного числа в непрерывную дробь является одним из важнейших инструментов теории чисел, восходящим еще к античному алгоритму Евклида нахождения наибольшего общего делителя. Начало современной теории непрерывных дробей положил в 1613 г. П. Катальди и продолжил Д. Валлис, предложивший термин «непрерывная дробь». Применялись эти дроби в первую очередь для рационального приближения вещественных чисел; например, Х. Гюйгенс использовал их для проектирования зубчатых колес своего планетария. Алгоритм цепных дробей занял видное место в теории чисел после трудов Л. Эйлера и Ж. Лагранжа, которые применили его к решению уравнения Пелля, что привело к пониманию фундаментальной роли непрерывных дробей в теории квадратичных иррациональностей. Эйлер открыл, а Лагранж доказал одно из важнейших свойств: «непрерывная дробь периодична только у квадратичных иррациональностей». Лагранж также доказал следующее основополагающее свойство рациональных приближениях вещественных чисел.

Напомним, что дробь P/Q ($P \in \mathbb{Z}$, $Q \in \mathbb{N}$) называется *наилучшим приближением* (второго рода) вещественного α, если не существует дроби P'/Q' ($P' \in \mathbb{Z}$, $Q' \in \mathbb{N}$) такой, что

$$\begin{aligned} |Q'\alpha - P'| &\leq |Q\alpha - P|, \\ Q' &\leq Q, \end{aligned}$$

причем хотя бы одно из неравенств является строгим.

Теорема (Лагранж)**.** *Для любого* $\alpha \in [0,1)$

а) любая подходящая дробь для α *есть наилучшее приближение, за исключением случая* $\alpha \in (1/2,1)$*,* $P_0/Q_0 = 0/1$*;*

б) любое наилучшее приближение α *есть подходящая дробь, за исключением случая* $\alpha = 1/2$*,* $P/Q = 1/1$*.*

Исследование иррациональностей степени три и выше, а также поиск многомерных наилучших приближений привели к необходимости обобщения цепных дробей на многомерный случай.

Первое формальное обобщение алгоритма непрерывных дробей было дано еще Эйлером [94], идеи которого развивали и дополняли К. Якоби, А. Пуанкаре, П. Бахман, О. Перрон и другие авторы. Следующий этап начал Л. Дирихле, а продолжили Л. Кронекер, Ш. Эрмит, Шарв, Е. Золотарев, которые пытались построить обобщение непрерывной дроби, имеющее для общей теории алгебраических чисел такое же значение, какое имеют цепные дроби для квадратичных числовых полей. Черту под этими исследованиями подвел Г.Ф. Вороной. В 1896 г. он защитил диссертацию «Об одном обобщении алгорифма непрерывных дробей», в которой дал метод нахождения основных единиц кубического числового поля как положительного, так и отрицательного дискриминанта. Алгоритм основан на рассмотрении взаимного расположения некоторых специальных узлов решеток. Эти узлы Вороной называл «относительными минимумами». Одновременно и независимо от Вороного минимумы трехмерных решеток изучал Г. Минковский [125, 126], который использовал термин «локальный минимум» (исследования Минковского относятся к случаю чисто вещественного расширения числового поля). Относительные (локальные) минимумы решеток представляют собой геометрическую интерпретацию многомерных наилучших приближений. Они являются естественным объектом с точки зрения целочисленного линейного программирования, а также возникают при изучении теоретико-числовых квадратурных формул [10, 11] и в теории равномерного распределения [15, 73].

Еще одно интересное геометрическое обобщение непрерывных дробей было дано Ф. Клейном [111] и основано на рассмотрении, так называемых, полиэдров (многогранников) Клейна, которые определяются как выпуклая оболочка узлов решетки, лежащих в заданном симплициальном конусе. Исходно исследуя A-градуированные алгебры [78], В.И. Арнольд столкнулся с полиэдрами Клейна. Начиная с 1989 г. он сформулировал множество задач о геометрических и статистических свойствах многомерных непрерывных дробей (см. [3, 4, 79, 80]), возобновляя тем самым интерес к этим вопросам.

В двумерном случае конструкции Клейна и Вороного – Минковского совпадают, и их статистические свойства непосредственно вытекают из теории непрерывных дробей. Однако, несмотря на значительный интерес, практически отсутствуют результаты для решеток размерности три и выше. Целью настоящей работы является исследование статистических свойств полиэдров Клейна и локальных минимумов многомерных решеток.

§ 2. Основные определения

Локальные минимумы

Определение 2.1. Ненулевой узел γ s-мерной решетки Γ будем называть *относительным минимумом*, если не существует ненулевого узла $\gamma' \in \Gamma$ такого, что

$$|\gamma'_i| \le |\gamma_i|, \quad i = \overline{1,s},$$

причем хотя бы одно из неравенств является строгим.

Возьмем любую неотрицательную функцию $f : \mathbb{R}^{s-1} \to [0, +\infty)$.

Определение 2.2. Ненулевой узел γ s-мерной решетки Γ будем называть *цилиндрическим f-минимумом*, если не существует ненулевого узла $\gamma' \in \Gamma$ такого, что

$$f(\gamma'_1, \ldots, \gamma'_{s-1}) \le f(\gamma_1, \ldots, \gamma_{s-1}), \quad |\gamma'_s| \le |\gamma_s|.$$

причем хотя бы одно из неравенств является строгим.

С геометрической точки зрения, это означает, что цилиндр

$$\left\{x \in \mathbb{R}^s : f(x_1, \ldots, x_{s-1}) \le f(\gamma_1, \ldots, \gamma_{s-1}), \quad |x_s| \le |\gamma_s|\right\}$$

не содержит ненулевых узлов Γ, за исключением точек, лежащих на границах оснований цилиндра. В дальнейшем, мы ограничимся случаем, когда функция f является лучевой и кусочно-дифференцируемой.

Рассмотрим теперь более общую конструкцию, включающую в себя и относительные, и цилиндрические минимумы. Пусть $\mathbf{\Phi} = (\Phi_1, \ldots, \Phi_r) : \mathbb{R}^s \to [0, +\infty)^r$.

Определение 2.3. Ненулевой узел γ s-мерной решетки Γ будем называть *локальным $\mathbf{\Phi}$-минимумом*, если не существует ненулевого узла $\gamma' \in \Gamma$ такого, что

$$\Phi_l(\gamma') \le \Phi_l(\gamma), \quad l = \overline{1,r},$$

причем хотя бы одно из неравенств строгое.

Далее всюду считаем, что функции Φ_l имеют следующий вид:

$$\Phi_1(x) = \phi_1(x_1, \ldots, x_{s_1}), \ldots, \Phi_r(x) = \phi_r(x_{s_{r-1}+1}, \ldots, x_s), \tag{2.1}$$

т.е. $\Phi_l(x) = \phi_l(x_{s_{l-1}+1}, \ldots, x_{s_l})$, $l = \overline{1,r}$. Здесь $s_0, \ldots, s_r$ — такие целые, что

$$0 = s_0 < s_1 < \ldots < s_r = s,$$

а $\phi_l : \mathbb{R}^{t_l} \to \mathbb{R}$ ($t_l = s_l - s_{l-1}$, $l = \overline{1,r}$) — лучевые, непрерывные, кусочно-дифференцируемые функции.

Локальные $\mathbf{\Phi}$-минимумы совпадают с относительными, если

$$r = s, \quad \Phi_i(x) = |x_i|, \ i = \overline{1,s}$$

и с цилиндрическими, если

$$r = 2, \quad \Phi_1(x) = f(x_1, \ldots, x_{s-1}), \quad \Phi_2(x) = |x_s|.$$

Локальные минимумы и единицы числовых полей. Пусть K — чисто вещественное расширение степени s поля рациональных чисел $\mathbb{Q}$. Обозначим через $\omega_1^{(1)}, \ldots, \omega_s^{(1)}$ — базис, состоящий из целых поля K. Пусть $\omega_1^{(i)}, \ldots, \omega_s^{(i)}$ — сопряженные базисы ($i = \overline{2, s}$), а K' — порядок поля K с базисом $\omega_1^{(1)}, \ldots, \omega_s^{(1)}$. Для каждого

$$\alpha = \sum_{j=1}^{s} \alpha_j \omega_j^{(1)} \in K'$$

определим геометрическое изображение $\gamma(\alpha) = (\gamma_1(\alpha), \ldots, \gamma_s(\alpha))$ числа α по формуле

$$\gamma_i(\alpha) = \sum_{j=1}^{s} \alpha_j \omega_j^{(i)} \quad i = \overline{1, s},$$

Пусть решетка Γ состоит из узлов $\gamma(\alpha)$, где $\alpha \in K'$. Для любого $\gamma \in \Gamma$ число $\gamma_1 \cdot \ldots \cdot \gamma_s$ является целым. Следовательно,

$$\forall \gamma \in \Gamma \setminus \{0\} \qquad |\gamma_1 \cdot \ldots \cdot \gamma_s| \geq 1.$$

Поэтому, если узел $\gamma = \gamma(\alpha) \in \Gamma$ удовлетворяет условию $|\gamma_1 \cdot \ldots \cdot \gamma_s| = 1$ (т.е. α — единица поля K), то он является относительным минимумом решетки Γ.

В общем случае геометрическое изображение (определение см. в [29, с. 29]) единицы числового поля степени $s = s_1 + 2s_2$ (s_1 — количество вещественных, а $2s_2$ — количество комплексных изоморфизмов K в $\mathbb{C}$) является локальным **Φ**-минимумом некоторой s-мерной решетки, если положить

$$\begin{aligned} &r = s_1 + s_2, \\ &\Phi_i(x) = |x_i|, \quad i = \overline{1, s_1}, \\ &\Phi_l(x) = \sqrt{x_{s_1+2l-1}^2 + x_{s_1+2l}^2}, \quad l = \overline{1, s_2}. \end{aligned}$$

Г.Ф. Вороной [19, 20] построил алгоритм вычисления относительных и цилиндрических минимумов трехмерных решеток и с его помощью разработал метод нахождения единиц в кубических полях положительного и отрицательного дискриминанта соответственно. Одновременно и независимо от Вороного относительные минимумы трехмерных решеток изучал Г. Минковский [124, 125] в связи с этими же вопросами. По поводу дальнейшего развития алгоритмов Вороного, Минковского и их обобщений на случай более высоких размерностей см., например, работы [82, 83, 84, 85, 86, 87, 90, 89, 131, 134] и ссылки там. Алгоритмы Вороного и Минковского нахождения единиц чисто вещественного расширения числового поля основаны на изучении взаимного расположения, так называемых, минимальных базисов решеток (составленных из относительных минимумов), при этом ряд важных свойств был сформулирован ими без доказательства. Доказательство, обсуждение, переизложение и дополнение оригинальных результатов Вороного и Минковского можно найти в [32, 95, 97, 130, 18].

Локальные минимумы и наилучшие приближения. Для любого вещественного α определим решетку

$$\Gamma_\alpha = \{(Q, Q \cdot \alpha - P) : \quad Q, P \in \mathbb{Z}\}. \tag{2.2}$$

Пусть $\mathfrak{M}(\Gamma_\alpha)$ — множество относительных минимумов этой решетки. По определению, $\mathfrak{M}(\Gamma_\alpha)$ состоит из $\pm(0,1)$ и точек вида $\pm(Q, \alpha Q - P)$, где P/Q — наилучшее приближение α. Поэтому согласно теореме Лагранжа,

$$\begin{aligned}
\mathfrak{M}(\Gamma_\alpha) &= \{\pm(Q_i, \alpha Q_i - P_i): \quad i = -1, 0, 1, 2, \ldots\} \quad \text{при } \alpha \in [0, 1/2), \\
\mathfrak{M}(\Gamma_\alpha) &= \{\pm(0,1),\ \pm(1,1/2),\ \pm(1,-1/2),\ \pm(2,0)\} \quad \text{при } \alpha = 1/2, \\
\mathfrak{M}(\Gamma_\alpha) &= \{\pm(Q_i, \alpha Q_i - P_i): \quad i = -1, 1, 2, \ldots\ldots\} \quad \text{при } \alpha \in (1/2, 1),
\end{aligned} \tag{2.3}$$

где $P_{-1} = 1$, $Q_{-1} = 0$ и P_i/Q_i — i-я подходящая дробь для α при $i = 0, 1, 2, \ldots$.

Рассмотрим теперь многомерные обобщения понятия наилучшего приближения. Возьмем любую неотрицательную функцию $f : \mathbb{R}^n \to [0, +\infty)$.

Определение 2.4. Ненулевой вектор $(u, v) \in \mathbb{Z}^n \times \mathbb{Z}$ будем называть *f-наилучшим приближением линейной формы* $L : \mathbb{R}^n \to \mathbb{R}$, если не существует ненулевого вектора $(u', v') \in \mathbb{Z}^n \times \mathbb{Z}$ такого, что

$$|Lu' - v'| \le |Lu - v|, \quad f(u') \le f(u),$$

причем хотя бы одно из неравенств строгое.

Определение 2.5. Вектор $(u, v) \in \mathbb{N} \times \mathbb{Z}^n$ будем называть *f-наилучшим совместным приближением* вещественных $\alpha_1, \ldots, \alpha_n$, если

$$\|u\alpha_i\| = |u\alpha_i - v_i|, \quad i = \overline{1, n},$$

и не существует другого натурального u' такого, что

$$f(\|u'\alpha\|) \le f(\|u\alpha\|), \quad u' \le u,$$

причем хотя бы одно из неравенств строгое. Здесь $\|u\alpha\| = (\|u\alpha_1\|, \ldots, \|u\alpha_n\|)$, $\|x\|$ — расстояние от вещественного x до ближайшего целого.

Возьмем теперь две неотрицательные функции: $f : \mathbb{R}^m \to [0, +\infty)$ и $g : \mathbb{R}^n \to [0, +\infty)$, а также набор линейных форм $\mathbf{L} = (L_1, \ldots, L_m) : \mathbb{R}^n \to \mathbb{R}^m$.

Определение 2.6. Ненулевой вектор $(u, v) \in \mathbb{Z}^n \times \mathbb{Z}^m$ будем называть *(f, g)-наилучшим совместным приближением линейных форм* $\mathbf{L}$, если не существует ненулевого вектора $(u', v') \in \mathbb{Z}^n \times \mathbb{Z}^m$ такого, что

$$f(\mathbf{L}u' - v') \le f(\mathbf{L}u - v), \quad g(u') \le g(u),$$

причем хотя бы одно из неравенств строгое.

Отметим, что вместо термина «наилучшее совместное приближение линейных форм $\mathbf{L}$» часто используют «наилучшее приближение матрицы Θ», где i-я строка Θ составлена из коэффициентов линейной формы L_i (см., например, [61]).

Наилучшие приближения неявно использовались еще Г.Ф. Вороным [19, 20], В. Ярником [77, 100, 101, 102] и другими авторами. По-видимому, систематическое изучение *многомерных* наилучших приближений было начато Дж. Лагариасом [117, 118,

119, 120, 121]. Более подробный обзор можно найти в статьях Н. Шевалье [93] и Н.Г. Мощевитина [127, 61].

Согласно определениям задача о нахождении наилучших приближений эквивалентна задаче о вычислении локальных минимумов решеток специального вида. Возьмем, например, линейную форму $L : \mathbb{R}^{s-1} \to \mathbb{R}$ и определим решетку Γ, составленную из узлов вида $\gamma(u, v) = (u, Lu - v)$, где $(u, v) \in \mathbb{Z}^{s-1} \times \mathbb{Z}$. Тогда $\gamma(u, v)$ является цилиндрическим f-минимумом, если и только если (u, v) есть f-наилучшее приближение линейной формы L.

В общем случае, возьмем две функции: $f : \mathbb{R}^m \to [0, +\infty)$ и $g : \mathbb{R}^n \to [0, +\infty)$, а также набор линейных форм $\mathbf{L} = (L_1, \dots, L_m) : \mathbb{R}^n \to \mathbb{R}^m$. Определим $(n+m)$-мерную решетку Γ, состоящую из узлов $\gamma(u, v) = (u, \mathbf{L}u - v)$, где $(u, v) \in \mathbb{Z}^n \times \mathbb{Z}^m$. Положим

$$r = 2, \quad \Phi_1(x) = g(x_1, \dots, x_n), \quad \Phi_2(x) = f(x_{n+1}, \dots, x_{n+m}).$$

В этом случае $\gamma(u, v)$ является локальным $\mathbf{\Phi}$-минимумом решетки Γ тогда и только тогда, когда (u, v) есть (f, g)-наилучшее совместное приближение линейных форм $\mathbf{L}$.

Еще несколько ссылок. Конструкция локальных минимумов возникает и в других областях дискретной математики и анализа. Например, В.А. Быковский доказал, что погрешность теоретико-числовых квадратурных формул (см. [10, 11], [57, § 6.4]), а также отклонение сеток от равномерного распределения [15] определяется множеством относительных минимумах решеток специального вида. Он также разработал [12] алгоритм вычисления всех относительных минимумов решеток (алгоритм Вороного, в общем случае, находит только часть минимумов, которые нужны для построения основных единиц). Модификации этого алгоритма, реализации и приложению к вычислению параметра Бахвалова параллелепипедальных сеток Коробова посвящены работы С.В. Гассана [16, 17].

В ряде статей (см. [14, 21, 72] и ссылки там) рассматривался вопрос о двумерном обобщении теоремы Валена (о соседних подходящих дробях) в терминах относительных минимумов.

Полиэдры Клейна.

Возьмем любую s-мерную решетку Γ и симплициальный конус $\mathfrak{C} \subset \mathbb{R}^s$ с вершиной в начале координат 0.

Определение 2.7. Множество $K = K(\Gamma, \mathfrak{C})$, которое является выпуклой оболочкой ненулевых узлов Γ, содержащихся в $\mathfrak{C}$, называется *полиэдром Клейна решетки* Γ *для конуса* $\mathfrak{C}$.

Пусть линейное отображение $L : \mathbb{R}^s \to \mathbb{R}^s$ является невырожденным. Тогда LK является полиэдром Клейна решетки $L\Gamma$ для конуса $L\mathfrak{C}$. Подходящим образом выбирая L, можно прийти к случаю $L\Gamma = \mathbb{Z}^s$ (решетка фиксирована) либо к случаю $L\mathfrak{C} = [0, +\infty)^s$ (конус фиксирован). В оригинальной конструкции Клейна рассматривался произвольный конус и фиксированная решетка $\mathbb{Z}^s$. Нам будет удобнее рассматривать случай, когда решетка является произвольной, а конус фиксированным. Будем придерживаться следующей терминологии.

Определение 2.8. Пусть $\theta = (\theta_1, \ldots, \theta_s)$, где $\theta_i = \pm 1$. Множество $K_\theta(\Gamma)$, которое является выпуклой оболочкой ненулевых узлов Γ, лежащих в угле

$$\{x \in \mathbb{R}^s : \quad \theta_i x_i \geq 0,\ i = \overline{1,s}\},$$

будем называть *полиэдром Клейна решетки* Γ.

Замечание 2.1. Каждая s-мерная решетка имеет 2^s полиэдров Клейна. В общем случае полиэдр Клейна не является обобщенным многогранником. Более того, он может быть не замкнутым множеством (см. [128]). Если, например, решетка Γ является целочисленной либо не имеет ненулевых узлов на координатных плоскостях (решетка общего положения), то полиэдры Клейна являются обобщенными многогранниками[1]. В этом случае будем ссылаться на полиэдры Клейна, как на многогранники Клейна.

В двумерном случае конструкция Клейна дает следующую геометрическую интерпретацию непрерывной дроби. Если $\alpha \in [0,1) \setminus \{1/2\}$, то множество вершин полиэдров Клейна решетки Γ_α, определяемой формулой (2.2), совпадает с множеством относительных минимумов, которое равно (2.3). Кроме того, если

$$a = (Q_{i-1}, \alpha Q_{i-1} - P_{i-1}) \quad \text{и} \quad b = (Q_{i+1}, \alpha Q_{i+1} - P_{i+1})$$

— две соседние вершины полиэдра Клейна, то

$$q_{i+1}(\alpha) = \#(\Gamma \cap (a, b]), \tag{2.4}$$

то есть количество точек решетки на полуинтервале $(a, b]$ («целочисленная» длина $[a, b]$) равно соответствующему неполному частному.

Отметим, что множество относительных минимумов *любой* двумерной решетки Γ совпадает с множеством вершин полиэдров Клейна $K_\theta(\Gamma)$, за исключением решеток с базисом вида (u, v), $(u, -v)$, для которых вершинами являются узлы $\pm(2u, 0)$, $\pm(0, 2v)$, а минимумами

$$\pm(2u, 0),\ \ \pm(0, 2v),\ \ \pm(u, v),\ \ \pm(u, -v).$$

Начиная с размерности 3 конструкции Клейна и Вороного – Минковского становятся различными. В частности, существуют четырехмерные решетки, имеющие относительные минимумы, лежащие внутри полиэдров Клейна, причем множество таких решеток имеет «положительную меру» (см. [24]). Однако, как доказано В.А. Быковским [13], любая вершина полиэдра Клейна является относительным минимумом.

Не претендуя на полноту изложения, приведем краткий обзор некоторых известных результатов, связанных с полиэдра Клейна. Более полный обзор можно найти в монографии [106].

В 1983 г. Х. Цутихаси [133] установил соответствие между периодическими полиэдрами Клейна и многомерными касповыми особенностями, которое обобщает известное ранее соответствие между периодическими непрерывными дробями и двумерными касповыми особенностями.

Б.Ф. Скубенко [65, 66] обнаружил связь между минимумами произведений линейных форм и многогранниками Клейна.

[1] т.е. их пересечения с любым многогранником также являются многогранниками.

Исходно исследуя A-градуированные алгебры [78], В.И. Арнольд столкнулся с полиэдрами Клейна. Начиная с 1989 г. он сформулировал множество задач о геометрических и статистических свойствах многомерных непрерывных дробей (см. [3, 4, 79, 80]), возобновляя тем самым интерес к этим вопросам.

Примеры некоторых «простейших» полиэдров Клейна для алгебраических трехмерных решеток, а также их свойства рассматривались в работах Е.И. Коркиной [109, 56, 110], Ж. Лашо [114], О.Н. Карпенкова [48, 49, 103, 105], Ж. Муссафир [129], А.Д. Брюно и В.И. Парусникова [7, 62, 63].

Связь между полиэдрами Клейна и базисами Гильберта изучали Ж.О. Муссафир [58] и О.Н. Герман [22], который также вывел эквивалентные формулировки известных гипотез Литтлвуда и Оппенгейма в терминах полиэдров Клейна [23, 96] (см. также [25]).

В ряде работ изучались многомерные аналоги теоремы Лагранжа о периодичности непрерывных дробей у квадратичных иррациональностей в терминах полиэдров Клейна. Комбинаторно-топологический аналог предложен (без доказательства) Е.И. Коркиной [109], а алгебраический — Лашо [114, 115, 116]. Уточнение и полное доказательство результата Коркиной опубликовано в [25]. Еще один вариант многомерного обобщения теоремы Лагранжа см. в [8, 9].

О.Н. Карпенков [104] получил полное описание целочисленно-линейных типов двумерных граней полиэдров Клейна, которые лежат на расстоянии, большем единицы от начала координат.

Ряд публикаций (см. [129, 48, 105] и ссылки там) посвящены разработке алгоритмов построения многогранников Клейна алгебраических решеток, которые тесно связаны с фундаментальными областями чисто вещественных расширений числового поля.

Несмотря на значительный интерес, почти не исследованными являются поставленные Арнольдом задачи о статистических свойствах многомерных аналогов непрерывных дробей. В известной работе М.Л. Концевича и Ю.М. Сухова [108] аннонсированы некоторые результаты о существовании статистик для полиэдров Клейна и предложена схема их доказательства. В диссертации Ж. Муссафир [129] некоторые из этих статистик вычислены приближенно. В статье О.Н. Карпенкова [51] сформулированы гипотезы о частоте появления многогранника заданного целочисленно-линейного типа в качестве грани полиэдра Клейна.

§ 3. Основные результаты

Оценки максимального количества локальных минимумов. Хорошо известен следующий результат о скорости роста знаменателей подходящих дробей: если $Q_k = Q_k(\alpha)$ — знаменатель k-й подходящей дроби для $\alpha \in \mathbb{R}$, то [76, теорема 12]

$$Q_k \geq 2^{(k-1)/2}.$$

Следовательно, для любого $P \geq 2$

$$\#\{k:\ Q_k(\alpha) \leq P\} = O(\log_2 P). \tag{3.1}$$

Аналогичные оценки справедливы и для многомерных наилучших приближений [91, 93, 118, 120]. Неравенство (3.1) можно переписать в следующем виде: для любой

двумерной решетки Γ_α вида (2.2)

$$\#\{\gamma \in \mathfrak{M}(\Gamma_\alpha) : \ |\gamma|_\infty \le P\} \ll \log_2 P.$$

Здесь и далее $\mathfrak{M}(\Gamma)$ — множество относительных минимумов решетки Γ. В главе I мы распространяем этот результат на случай решеток произвольной размерности и ранга.

Назовем решетки Γ_1 и Γ_2 из $\mathcal{L}_{t,s}(\mathbb{R})$ *подобными*, если существует такой набор ненулевых вещественных чисел $(\alpha_1, \dots, \alpha_s)$, что

$$\Gamma_2 = \{(\alpha_1\gamma_1, \dots, \alpha_s\gamma_s) : \quad (\gamma_1, \dots, \gamma_s) \in \Gamma_1\}.$$

Множество относительных минимумов $\mathfrak{M}(\Gamma)$ конечно тогда и только тогда, когда решетка Γ подобна целочисленной (см. [27]).

Для полных целочисленных решеток известны следующие оценки максимального количества относительных минимумов:

$$\sup_{\Gamma \in \mathcal{L}_s(\mathbb{Z};N)} \#\mathfrak{M}(\Gamma) \asymp_s \ln^{s-1} N + 1. \tag{3.2}$$

Верхняя доказана в [10, 11], а нижняя в [1]. Ряд публикаций был посвящен уточнению соответствующих констант (см. [57, 28, 2] и ссылки там). Наилучший результат получен в [2] и имеет вид

$$\frac{1}{(s-1)! \cdot 100 \cdot \log_2^{s-1}(128s)} \le \overline{C}(s) \le \frac{2^s}{(s-1)!}, \tag{3.3}$$

где

$$\overline{C}(s) = \limsup_{N \to +\infty} \left(\frac{\sup\limits_{\Gamma \in \mathcal{L}_s(\mathbb{Z},N)} \#\mathfrak{M}(\Gamma)}{\ln^{s-1} N} \right).$$

Возьмем теперь произвольную решетку $\Gamma \in \mathcal{L}_{t,s}(\mathbb{R})$. Для любого $P \in \mathbb{R}_+$ положим

$$\mathfrak{M}(\Gamma, P) = \{\gamma \in \mathfrak{M}(\Gamma) : \ \ |\gamma|_\infty \le P\}.$$

В главе I диссертации мы докажем оценку

$$\#\mathfrak{M}(\Gamma, P) \ll_{s,t} \ln^{t-1}(P/\lambda) \quad \text{при } P > \lambda, \tag{3.4}$$

где

$$\lambda = \lambda(\Gamma) = \min_{\gamma \in \Gamma \setminus \{0\}} |\gamma|_\infty.$$

Отметим, что для алгебраической решетки $\Gamma \in \mathcal{L}_t(\mathbb{R})$

$$\forall P \in (1, +\infty) \qquad \#\mathfrak{M}(\Gamma, P) \gg_\Gamma \ln^{t-1} P. \tag{3.5}$$

Отсюда вытекает, что оценка (3.4) является правильной с точностью до константы, зависящей от t и s.

Используя (3.4), мы получим следующее неравенство для количества всех относительных минимумов неполной целочисленной решетки $\Gamma \in \mathcal{L}_{t,s}(\mathbb{Z})$

$$\#\mathfrak{M}(\Gamma) \underset{s,t}{\ll} \ln^{t-1} D + 1, \tag{3.6}$$

где $D = D(\Gamma)$ — максимум из модулей миноров t-го порядка базисной матрицы решетки Γ ($D(\Gamma)$ не зависит от выбора базисной матрицы). Из (3.2) вытекает, что оценка (3.6) является правильной с точностью до константы, зависящей от s и t.

В последнем параграфе главы I доказывается следующая оценка для максимального количества локальных $\mathbf{\Phi}$-минимумов:

$$\forall \Gamma \in \mathcal{L}_s(\mathbb{Z}; N) \qquad \#\mathfrak{M}_{\mathbf{\Phi}}(\Gamma) \underset{\mathbf{\Phi}}{\ll} \ln^{r-1} N + 1. \tag{3.7}$$

Асимптотическое распределение целочисленных матриц. Исследование статистических свойств конечных непрерывных дробей приводит к задачам об асимптотическом распределении целочисленных матриц размера 2×2, лежащих в заданной области. Пусть, например, $l = l(P/N)$ — длина разложения рационального $P/N = [0; q_1, \ldots, q_l]$ в непрерывную дробь. Вычисление величины

$$\sum_{1 \le P < N} l(P/N)$$

(средняя длина непрерывной дроби для рациональных чисел фиксированного знаменателя N) сводится к нахождению количества матриц $M \in \mathrm{M}_2(\mathbb{Z}; N)$ следующего вида [98, 132]

$$M = \begin{pmatrix} a_1 & b_1 \\ -a_2 & b_2 \end{pmatrix}, \qquad 0 < b_1 < a_1, \quad 0 < a_2 < b_2.$$

Аналогичным образом при исследовании статистических свойств многомерных аналогов непрерывных дробей возникает задача: найти величину $\#(\Omega \cap \mathrm{M}_s(\mathbb{Z}, N))$, где Ω — заданное подмножество $\mathrm{GL}_s(\mathbb{R})$.

Известен следующий результат. Если

$$\Omega = \{t \cdot X : \quad X \in \Omega', \ \ t \in \mathbb{R}_+\}, \tag{3.8}$$

где Ω' — измеримое по Жордану множество из $\mathrm{SL}_s^+(\mathbb{R}) = \{X \in \mathrm{GL}_s(\mathbb{R}) : \det X = 1\}$, то

$$\#(\Omega \cap \mathrm{M}_s(\mathbb{Z}, N)) \sim \frac{\mathcal{R}_s(N)}{\zeta(2) \cdot \ldots \cdot \zeta(s)} \cdot \mu_H(\Omega') \quad \text{при } N \to +\infty. \tag{3.9}$$

Здесь μ_H — мера Хаара на группе $\mathrm{SL}_s^+(\mathbb{R})$, а $\mathcal{R}_s(N) = \#\mathcal{L}_s(\mathbb{Z}; N)$ — количество целочисленных s-мерных решеток определителя N. Величина $\mathcal{R}_s(N)$ конечная, причем

$$\mathcal{R}_s(N) = \#\left(\mathrm{M}_s(\mathbb{Z}; N)/\mathrm{GL}_s(\mathbb{Z})\right),$$

т.к. множество базисных матриц любой фиксированной решетки инвариантно относительно правого действия группы $\mathrm{GL}_s(\mathbb{Z})$. Явные формулы для $\mathcal{R}_s(N)$ приводятся в § II.2.

Формула (3.9) доказана Ю.В. Линником и Б.Ф. Скубенко в [60] при $s = 2, 3$ (см. также [59]) и в [64] при любом $s \geq 2$ (другое доказательство см. в [81]). Оценка остаточного члена соотношения (3.9) получена в [47].

Однако множества, возникающие в настоящей работе, не удовлетворяют условию (3.8). В главе II диссертации рассматривается случай, когда $\Omega \subset \mathrm{GL}_s(\mathbb{R})$ обладает следующими свойствами:

А) $\Omega = \left\{ \left(\!\left(x_{ij}\right)\!\right) : \quad (x_{i1}, \ldots, x_{is}) \in V_i, \;\; i = \overline{1, s} \right\}$, где V_i — конусы в $\mathbb{R}^s$ с липшицевыми границами;

Б) существует такая постоянная $C > 0$, что для любой $X \in \Omega$ справедлива оценка

$$\prod_{i=1}^{s} \max_{1 \leq j \leq s} |x_{ij}| \leq C \cdot \det X.$$

Подчеркнем, что если выполняются условия А), Б), то Ω нельзя представить в виде объединения конечного набора множеств, каждое из которых удовлетворяет (3.8).

Основной результат главы II заключается в доказательстве соотношения

$$\#\left(\Omega \cap \mathrm{M}_s(\mathbb{Z}; N)\right) = \mathcal{R}_s(N) \cdot \left(\mathcal{C}(\Omega) \cdot \ln^{s-1} N + O_\Omega\left(\chi(N) \cdot \ln^{s-2} N\right) \right), \tag{3.10}$$

где постоянная $\mathcal{C}(\Omega) \geq 0$ зависит только от Ω (явную формулу см. в § II.1), а

$$\chi(N) = 1 + \sum_{p \mid N} \frac{\ln p}{p}.$$

Здесь p — простые делители натурального N. Отметим, что при $N \geq 3$

$$\chi(N) \ll 1 + \ln \omega(N) \ll \ln \ln N,$$

где $\omega(N)$ — количество простых делителей N.

Среднее количество относительных минимумов. В 1968 г. Г. Хейльбронн [98] получил асимптотическую формулу для средней длины конечной цепной дроби:

$$\frac{1}{\#\Phi(d)} \sum_{c \in \Phi(d)} l(c/d) = \frac{2 \ln 2}{\zeta(2)} \cdot \ln d + \xi(d). \tag{3.11}$$

Здесь $l = l(c/d)$ — длина разложения $c/d = [0; q_1, \ldots, q_l]$ в непрерывную дробь; множество $\Phi(d)$ состоит из целых $c \in [1, d]$, которые взаимно просты с d, а $\xi(d) = O\left(\sigma_{-1}^4(d)\right)$. Портер [132] уточнил формулу для остатка:

$$\forall \epsilon > 0 \qquad \xi(d) = C + O_\epsilon(d^{-1/6+\epsilon}),$$

где C — некоторая положительная константа, впоследствии найденная Ренчем [107].

В главе III мы доказываем многомерное обобщение теоремы Хейльбронна в терминах относительных минимумов. А именно, определим среднее количество относительных минимумов полных s-мерных целочисленных решеток определителя N:

$$E(N, s) = \frac{1}{\mathcal{R}_s(N)} \cdot \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z}; N)} \#\mathfrak{M}(\Gamma).$$

Учитывая связь между относительными минимумами двумерных решеток и непрерывными дробями (см. (2.3)), соотношение (3.11) можно переписать так

$$E(N,2) \sim \frac{4 \cdot \ln 2}{\zeta(2)} \cdot \ln N \text{ при } N \to \infty.$$

Основной результат главы III заключается в доказательстве соотношения

$$E(N,s) = \mathcal{C}(s) \cdot \ln^{s-1} N + O_s\left(\chi(N) \cdot \ln^{s-2} N + 1\right) \tag{3.12}$$

для *любой размерности* $s \geq 2$. Здесь $\mathcal{C}(s)$ — положительная постоянная, зависящая только от s. К сожалению, константу $\mathcal{C}(s)$ при $s \geq 3$ даже приближенно вычислить удается только в трехмерном случае. В последнем параграфе главы III доказываются двусторонние оценки:

$$\frac{1}{(s-1)!} \leq \mathcal{C}(s) \leq \frac{2^s}{(s-1)!},$$

Из них, в частности, вытекает следующее уточнение первого неравенства из (3.3):

$$\frac{1}{(s-1)! \cdot \log_2^{s-1} e} \leq \overline{C}(s).$$

Доказательство (3.12) основано на построении алгоритма, который позволяет единственным образом дополнить относительный минимум до базиса (решетки) специального вида. В результате, вычисление суммы

$$\sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z};N)} \#\mathfrak{M}(\Gamma)$$

сводится к нахождению количества всех базисов этого специального вида, то есть к вычислению количества матриц из $\mathrm{M}_s(\mathbb{Z};N)$, лежащих в некоторой области. Для этого применяется формула (3.10).

Статистические свойства полиэдров Клейна. В статье Хейльбронна [98] также доказана асимптотическая формула для среднего количества неполных частных, равных заданному натуральному k:

$$\frac{1}{\#\Phi(d)} \sum_{c \in \Phi(d)} \#\left\{n : q_n(c/d) = k\right\} = \frac{2}{\zeta(2)} \cdot \ln\left(1 + \frac{1}{k(k+2)}\right) \cdot \ln d + R_k(d), \tag{3.13}$$

где $R_k(d,N) = O_k(\sigma_{-1}^4(d))$. А.В. Устинов [70], используя метод Портера [132], уточнил остаток:

$$R_k(d) = C(k) + O_{k,\epsilon}(d^{-1/6+\epsilon}),$$

где постоянная $C(k)$ зависит только от k.

В главе IV доказывается обобщение результатов Хейльбронна (3.11), (3.13) в терминах полиэдров Клейна.

Пусть F_1 и F_2 многогранники из $\mathbb{R}^s$ с вершинами в $\mathbb{Z}^s$. Напомним, что F_1 и F_2 принадлежат одному целочисленно-линейному типу, если существует такое отображение $L \in \mathrm{GL}_s(\mathbb{Z})$, что $LF_1 = F_2$.

Возьмем любую компактную гиперграни F полиэдра Клейна решетки $\Gamma \in \mathcal{L}_s(\mathbb{R})$. Пусть $L : \mathbb{R}^s \to \mathbb{R}^s$ такое линейное преобразование, что

$$L\Gamma = \mathbb{Z}^s. \tag{3.14}$$

Очевидно, что целочисленно-линейный тип многогранника LF не зависит от выбора L. Это позволяет следующим образом классифицировать грани полиэдров Клейна.

Пусть $\mathcal{T}$ — целочисленно-линейный тип $(s-1)$-мерных многогранников из $\mathbb{R}^s$.

Определение 3.1. Будем говорить, что грань F *принадлежит типу* $\mathcal{T}$, если LF принадлежит целочисленно-линейному типу $\mathcal{T}$ для любого линейного преобразования $L : \mathbb{R}^s \to \mathbb{R}^s$ удовлетворяющего (3.14).

Пусть $\mathcal{F}(\Gamma; \mathcal{T})$ — множество граней типа $\mathcal{T}$, а $\mathcal{V}(\Gamma)$ — множество вершин полиэдров Клейна решетки Γ. Для любого натурального N определим среднее количество граней типа $\mathcal{T}$:

$$E_{\mathcal{T}}(N, s) = \frac{1}{\mathcal{R}_s(N)} \cdot \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z}; N)} \#\mathcal{F}(\Gamma, \mathcal{T})$$

и среднее количество вершин:

$$E_{\mathcal{V}}(N, s) = \frac{1}{\mathcal{R}_s(N)} \cdot \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z}; N)} \#\mathcal{V}(\Gamma)$$

многогранников Клейна целочисленных полных s-мерных решеток определителя N.

Пусть $s = 2$. Тогда гиперграни являются отрезками, и их тип однозначно определяется количеством точек решетки, которые лежат на грани. Поэтому, согласно (2.4), вопрос о среднем числе граней фиксированного типа сводится к задаче о частоте появления заданного натурального в качестве неполного частного. Соотношение (3.13) в терминах многоугольников Клейна можно записать так

$$E_{\mathcal{T}_k}(N, 2) \sim \frac{4}{\zeta(2)} \cdot \ln\left(1 + \frac{1}{k(k+2)}\right) \cdot \ln N, \quad N \to +\infty,$$

где $(k+1)$ — количество точек решетки лежащих на грани типа $\mathcal{T}_k$. Кроме того, при $s = 2$ $\mathfrak{M}(\Gamma) = \mathcal{V}(\Gamma)$, за исключением решеток с базисом вида (u, v), $(u, -v)$, для которых

$$\mathcal{V}(\Gamma) = \{\pm(2u, 0),\ \pm(0, 2v)\}, \quad \mathfrak{M}(\Gamma) = \{\pm(2u, 0),\ \pm(0, 2v),\ \pm(u, v),\ \pm(u, -v)\}.$$

Следовательно,

$$\sum_{\Gamma \in \mathcal{L}_2(\mathbb{Z}; N)} \#\mathfrak{M}(\Gamma) = \sum_{\Gamma \in \mathcal{L}_2(\mathbb{Z}; N)} \#\mathcal{V}(\Gamma) + 4 \cdot \sigma_0(N/2)$$

(считаем $\sigma_0(N/2) = 0$ для нечетного N). Поэтому из (3.12) (из (3.11)) следует, что

$$E_{\mathcal{V}}(N, 2) = \frac{4 \ln 2}{\zeta(2)} \ln N + O(\chi(N)).$$

Пусть TF_3 — множество типов граней, которые реализуются на решетках из $\mathcal{L}_3(\mathbb{R})$, т.е.

$$\forall \mathcal{T} \in TF_3 \quad \exists \Gamma \in \mathcal{L}_3(\mathbb{R}) : \quad \mathcal{F}(\Gamma, \mathcal{T}) \neq \emptyset.$$

Возьмем любой $\mathcal{T} \in TF_3$. Основными результатами главы IV являются следующие асимптотические формулы для трехмерных полиэдров Клейна:

$$E_{\mathcal{T}}(N,3) = C_{\mathcal{T}} \cdot \ln^2 N + O_{\mathcal{T}}(\chi(N) \cdot \ln N), \tag{3.15}$$

$$E_{\mathcal{V}}(N,3) = C_{\mathcal{V}} \cdot \ln^2 N + O(\chi(N) \cdot \ln N), \quad N > 1. \tag{3.16}$$

Здесь $C_{\mathcal{T}}$ — положительная постоянная, зависящая только от $\mathcal{T}$; $C_{\mathcal{V}}$ — абсолютная положительная постоянная. Аналитические выражения для них приведены в § IV.2 и § IV.3 соответственно.

Доказательство (3.15) основано на построении алгоритма, который грани типа $\mathcal{T}$ ставит в соответствие некоторый базис специального вида. В результате, задача о вычислении суммы

$$\sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z};N)} \#\mathcal{F}(\Gamma;\mathcal{T})$$

сводится к нахождению количества всех базисов этого специального вида, то есть к вычислению количества матриц из $\mathrm{M}_s(\mathbb{Z};N)$, лежащих в некоторой области. Для этого применяется формула (3.10).

Доказательство (3.16) основано на следующих соображениях.

1. Согласно [13] любая вершина полиэдра Клейна является относительным минимумом. Поэтому достаточно подсчитать количество минимумов, которые не являются вершинами, и использовать (3.12).

2. В [24] получено описание относительных минимумов трехмерных решеток, которые не являются вершинами. Согласно [24], вычисление суммы

$$\sum_{\Gamma \in \mathcal{L}_3(\mathbb{Z};N)} \#(\mathfrak{M}(\Gamma) \setminus \mathcal{V}(\Gamma))$$

сводится к подсчету суммарного количества треугольных граней некоторого специального вида. Для этого используются идеи доказательства (3.15) и результаты О.Н. Карпенкова [104] о классификации граней.

К сожалению, результаты главы IV не удается распространить на случай $s \geq 4$. При $s \geq 4$ получены только оценки (см. § IV.1)

$$E_{\mathcal{V}}(N,s) \underset{s}{\asymp} \ln^{s-1} N + 1 \quad .$$

Среднее количество цилиндрических минимумов. Пусть f — лучевая, непрерывная и кусочно-дифференцируемая функция, определенная на $\mathbb{R}^{s-1}$.

Определим среднее число $E_{c,f}[1,R]$ цилиндрических f-минимумов s-мерных целочисленных решеток с определителем из отрезка $[1,R]$ по формуле

$$E_{c,f}[1,R] = \frac{1}{\#\mathcal{L}_s(\mathbb{Z};[1,R])} \cdot \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z};[1,R])} \#\mathfrak{M}_{c,f}(\Gamma)$$

где $\mathfrak{M}_{c,f}(\Gamma)$ — множество цилиндрических f-минимумов Γ.

В первых двух параграфах главы V доказывается асимптотическая формула

$$E_{c,f}[1,R] = \mathcal{C}_{c,f} \cdot \ln R + O_f(1), \tag{3.17}$$

где $\mathcal{C}_{c,f}$ — положительная постоянная, зависящая только от f.

Доказательство основано на специальной процедуре дополнения цилиндрического минимума до базиса решетки, основанной на идеях Г.Ф. Вороного (см. [32, глава 5, § 60]). В результате, вычисление суммы

$$\sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z};[1,R])} \#\mathfrak{M}_{c,f}(\Gamma)$$

сводится к нахождению количества целочисленных матриц M таких, что

$$M \in \Omega_{c,f}, \quad |\det M| \in [1,R], \tag{3.18}$$

где $\Omega_{c,f}$ — некоторое подмножество $\mathrm{GL}_s(\mathbb{R})$. Доказательство технических результатов о количестве целочисленных матриц в $\Omega_{c,f}$ вынесено в приложение.

Среднее количество наилучших приближений линейных форм. По-видимому, первые результаты о статистических свойствах конечных непрерывных дробей получил G. Lochs [122], который, в частности, доказал следующую формулу

$$\frac{2}{R(R+1)} \sum_{1 \le d \le R} \sum_{1 \le c \le d} l(c/d) = \frac{2\ln 2}{\zeta(2)} \cdot \ln R + C_1 + \xi_1(R), \tag{3.19}$$

где C_1 — абсолютная положительная постоянная, а $\xi_1(R) = O(R^{-1/2})$. Ряд работ был посвящен улучшению оценки остатка $\xi_1(R)$. Последний результат получен Д.А. Фроленковым [74] и имеет вид

$$\xi_1(R) = O(R^{-1} \cdot \ln^3 R).$$

В работе А.В. Устинова [69] получена следующая асимптотическая формула для математического ожидания количества подходящих знаменателей, не превосходящих фиксированного $P \ge 2$:

$$\int_0^1 \#\{j : Q_j(\alpha) \le P\}\, d\alpha = \frac{2\ln 2}{\zeta(2)} \cdot \ln P + C_1 + O(P^{-1} \ln P), \tag{3.20}$$

где C_1 — абсолютная положительная постоянная.

В последнем параграфе главы V доказывается многомерное обобщение результатов (3.19), (3.20) в терминах наилучших приближений линейных форм.

Пусть $\mathfrak{B}_f(\alpha)$ — множество f-наилучших приближений линейной формы $x \in \mathbb{R}^n \to \alpha_1 x_1 + \ldots + \alpha_n x_n$. Множество $\mathfrak{B}_f(\alpha)$ конечно только в случае, когда числа $\alpha_1, \ldots, \alpha_n$ линейно зависимы над полем $\mathbb{Q}$.

Для любого $P \ge 2$ и $\alpha \in [0,1)^n$ определим множество

$$\mathfrak{B}_f(\alpha, P) = \{(u,v) \in \mathfrak{B}_f(\alpha) : f(u) \le P\}.$$

Оно конечно, причем

$$\#\mathfrak{B}_f(\alpha, P) \underset{f}{\ll} \ln P. \tag{3.21}$$

Если функция f выпуклая, то неравенство (3.21) вытекает из известных результатов об экспоненциальном росте наилучших приближений [120, теорема 1]. В общем случае, оно является тривиальным следствием из теоремы I.3.1 настоящей работы.

Кроме того, согласно результатам Шевалье [92] существует такая положительная постоянная C'_f, зависящая только от f, что для почти всех (по Лебегу) $\alpha \in [0,1)^n$

$$\limsup_{P\to\infty} \frac{\#\mathfrak{B}(\alpha, P)}{\ln P} \geq C'_f. \tag{3.22}$$

Для любого вещественного $R > 1$ определим множество $\Delta_n(R)$, состоящее из векторов $\alpha \in [0,1)^n$ с координатами $\alpha_i = P_i/Q$, где P_i, Q — целые, причем

$$0 \leq P_i < Q \leq R, \quad i = \overline{1,n}.$$

Определим среднее количество

$$E_{\mathfrak{B},f}([1,R],P) = \frac{1}{\#\Delta_n(R)} \sum_{\alpha\in\Delta_n(R)} \#\mathfrak{B}_f(\alpha,P),$$

f-наилучших приближений, удовлетворяющих условию $f(u) \leq P$, линейных форм с рациональными коэффициентами из $\Delta_n(R)$, а также математическое ожидание

$$\mathcal{E}_{\mathfrak{B},f}(P) = \int_{[0,1)^n} \#\mathfrak{B}_f(\alpha,P)\, d\alpha$$

количества f-наилучших приближений, удовлетворяющих условию $f(u) \leq P$, линейных форм с вещественными коэффициентами.

Отметим, что функция $\alpha \in [0,1)^n \to \#\mathfrak{B}_f(\alpha,P)$ измеримая по Лебегу (см. лемму V.3.5) и ограниченная (согласно (3.21)). Поэтому интеграл Лебега $\mathcal{E}_{\mathfrak{B},f}(P)$ существует и конечен.

В одномерном случае (т.е. при $n = 1$, $f(x) = |x|$) асимптотические формулы для определенных средних величин вытекают из известных статистических свойств непрерывных дробей (см. (3.19), (3.20)). В частности,

$$\mathcal{E}_{\mathfrak{B},f}(P) = \frac{4\cdot\ln 2}{\zeta(2)} \cdot \ln P + O(1).$$

Рассмотрим теперь случай произвольной размерности. Согласно (3.21), (3.22)

$$\limsup_{P\to\infty} \frac{\mathcal{E}_{\mathfrak{B},f}(P)}{\ln P} \underset{f}{\asymp} 1.$$

В § 3 главы V мы докажем, что для любого $n \geq 1$ и любой непрерывной, кусочно-дифференцируемой, лучевой функции $f : \mathbb{R}^n \to \mathbb{R}$

$$E_{\mathfrak{B},f}([1,R],P) = \mathcal{C}_{c,f}\cdot n\cdot \ln P + O_f(1) \qquad \text{при } P^n \underset{f}{\ll} R, \tag{3.23}$$

$$\mathcal{E}_{\mathfrak{B},f}(P) = \mathcal{C}_{c,f}\cdot n\cdot \ln P + O_f(1). \tag{3.24}$$

Постоянная $\mathcal{C}_{c,f}$ такая же, как и в формуле (3.17)

Обоснование (3.23) основано на следующих соображениях. Как уже отмечалось, существует взаимно однозначное соответствие между наилучшими приближениями линейной формы и цилиндрическими минимумами некоторой решетки. Поэтому $E_{\mathfrak{B},f}([1,R],P)$ равно среднему количеству цилиндрических f-минимумов γ, у которых $f(\gamma_1,\ldots,\gamma_{s-1}) \le P$, решеток специального вида. В результате, вычисление $E_{\mathfrak{B},f}([1,R],P)$ сводится к нахождению количества целочисленных матриц M, удовлетворяющих (3.18) и условиям:

$$f(m_{11},\ldots,m_{(s-1)1}) \le P, \quad d_{s-1}(M) = 1,$$

где $s = n+1$, а $d_{s-1}(M)$ — наибольший общий делитель алгебраических дополнений к элементам последней строки M.

Формула (3.24) получается предельным переходом в (3.23) при $R \to \infty$.

Доказательство технических результатов о количестве целочисленных матриц в $\Omega_{c,f}$ вынесено в приложение.

Среднее количество локальных Φ-минимумов. Пусть $E_{\mathbf{\Phi}}[1,R]$ — среднее число локальных $\mathbf{\Phi}$-минимумов s-мерных целочисленных решеток с определителем из отрезка $[1,R]$, то есть

$$E_{\mathbf{\Phi}}[1,R] = \frac{1}{\#\mathcal{L}_s(\mathbb{Z};[1,R])} \cdot \sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};[1,R])} \#\mathfrak{M}_{\mathbf{\Phi}}(\Gamma),$$

где $\mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$ — множество локальных $\mathbf{\Phi}$-минимумов решетки Γ.

Основной результат главы V заключается в следующем. Пусть функция $\mathbf{\Phi}$ удовлетворяет условиям (2.1). Тогда для любого $R \ge 2$

$$E_{\mathbf{\Phi}}[1,R] = C_{\mathbf{\Phi}} \cdot \ln^{r-1} R + O_{\mathbf{\Phi}}(\ln^{r-2} R), \tag{3.25}$$

где $C_{\mathbf{\Phi}}$ — положительная постоянная, зависящая только от $\mathbf{\Phi}$.

Как и в предыдущих случаях, доказательство основано на построении специальной процедуры дополнения локального минимума до базиса решетки. В результате, вычисление суммы

$$\sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};[1,R])} \#\mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$$

сводится к нахождению количества целочисленных матриц с определителем из отрезка $[1,R]$, лежащих в некотором множестве $\Omega_{\mathbf{\Phi}} \subset \mathrm{GL}_s(\mathbb{R})$.

Используемый метод дополнения минимума до базиса похож на тот, который применяется для случая относительных минимумов, и отличен от использованного для цилиндрических минимумов.

Также как и главе V доказательство технических результатов о количестве целочисленных матриц из $\Omega_{\mathbf{\Phi}}$ вынесено в приложение.

Глава I
Оценки максимального количества локальных минимумов

В этой главе мы получим верхние и нижние оценки для максимального количества локальных минимумов (неравенства (0.3.4), (0.3.5), (0.3.6) и (0.3.7)).

В § 1 мы выведем некоторые вспомогательные соотношения. В § 2 получим оценки для количества относительных минимумов, а в последнем разделе — для локальных **Φ**-минимумов.

Напомним, что ненулевой узел γ s-мерной решетки Γ называется относительным минимумом, если не существует ненулевого узла $\gamma' \in \Gamma$ такого, что

$$|\gamma'_i| \le |\gamma_i|, \quad i = \overline{1,s},$$

причем хотя бы одно из неравенств является строгим. Через $\mathfrak{M}(\Gamma)$ мы обозначаем множество относительных минимумов решетки Γ.

§ 1. Вспомогательные оценки

Пусть $\Gamma \in \mathcal{L}_{t,s}(\mathbb{R})$, т.е. Γ — s-мерная решетка ранга t. Возьмем любые векторы $\mathbf{P} = (P_1, \dots, P_s) \in \mathbb{R}^s$ и $\mathbf{p} = (p_1, \dots, p_s) \in \mathbb{R}^s$, удовлетворяющие условиям $P_i \ge p_i > 0$, $i = \overline{1,s}$. Определим

$$\mathfrak{M}(\Gamma; \mathbf{P}; \mathbf{p}) = \left\{ \gamma \in \mathfrak{M}(\Gamma) : \quad p_i \le |\gamma_i| \le P_i \quad i = \overline{1,s} \right\}.$$

Целью данного раздела является получение оценки

$$\#\mathfrak{M}(\Gamma; \mathbf{P}; \mathbf{p}) \underset{t,s}{\ll} \ln^{t-1} H + 1, \quad H = \max_{1 \le i \le s} P_i/p_i.$$

Отметим, что непосредственное применение методов работ [2, 28], в которых исследуются *полные* целочисленные решетки, приводит к завышенной оценке

$$\#\mathfrak{M}(\Gamma; \mathbf{P}; \mathbf{p}) \underset{s}{\ll} \ln^{s-1} H + 1.$$

Следующие две леммы доказываются также как и в [2, 28]. В них не учитывается ограничение на ранг решетки.

Лемма 1.1. *Пусть* $\{1,\dots,s\} = I \cup I' \cup \{\nu\}$, *причем множества* I, I', $\{\nu\}$ *попарно непересекаются. Тогда для любого* $(\alpha_1,\dots,\alpha_s) \in \mathbb{R}^s_+$ *количество относительных минимумов* $\gamma \in \Gamma$, *удовлетворяющих неравенствам*

$$\begin{array}{ll} \alpha_i \le |\gamma_i| \le 2\alpha_i & \text{при } i \in I, \\ \alpha_j|\gamma_\nu| \le |\gamma_j| \le 2\alpha_j|\gamma_\nu| & \text{при } j \in I', \\ \gamma_\nu \ne 0, & \end{array} \tag{1.1}$$

не больше, чем 2^s.

Доказательство. Предположим, что утверждение леммы неверно. Тогда найдутся два минимума $\gamma, \eta \in \mathfrak{M}(\Gamma)$, удовлетворяющие (1.1), причем $\gamma_i\eta_i \ge 0$, $i = \overline{1,s}$ (координаты имеют одинаковые знаки). Рассмотрим узел $(\eta-\gamma)$. Пусть, для определенности, $|\gamma_\nu| \le |\eta_\nu|$. Тогда $|\eta_\nu - \gamma_\nu| < |\eta_\nu|$. Кроме того,

$$\begin{aligned} &|\eta_i - \gamma_i| = \Big||\eta_i| - |\gamma_i|\Big| \le 2\alpha_i - \alpha_i = \alpha_i \le |\eta_i| \quad \text{при } i \in I, \\ &|\gamma_j| \le 2\alpha_j|\gamma_\nu| \le 2\alpha_j|\eta_\nu| \le 2|\eta_j| \quad \Longrightarrow \quad |\eta_j - \gamma_j| \le |\eta_j| \quad \text{при } j \in I'. \end{aligned}$$

Значит, узел $(\eta - \gamma)$ противоречит условию $\eta \in \mathfrak{M}(\Gamma)$. □

Будем обозначать $\lceil x \rceil = \min\{n \in \mathbb{Z} : n \ge x\}$ для всех $x \in \mathbb{R}_+$.

Лемма 1.2. *Пусть* $\{1,\dots,s\} = I \cup I' \cup \{\nu\}$, *причем множества* I, I', $\{\nu\}$ *попарно непересекаются. Пусть* $a_i, b_i \in \mathbb{R}_+$, *причем* $a_i < b_i$ *при* $i \in \{1,\dots,s\} \setminus \{\nu\}$. *Тогда количество относительных минимумов* $\gamma \in \Gamma$, *удовлетворяющих неравенствам*

$$\begin{array}{ll} a_i \le |\gamma_i| \le b_i & \text{при } i \in I, \\ a_j|\gamma_\nu| \le |\gamma_j| \le b_j|\gamma_\nu| & \text{при } j \in I', \\ \gamma_\nu \ne 0, & \end{array} \tag{1.2}$$

не больше, чем

$$2^s \prod_{i=\overline{1,s},\ i\ne\nu} \lceil \log_2(b_i/a_i) \rceil.$$

Доказательство. Достаточно заметить, что для любого $\gamma \in \Gamma$, удовлетворяющего (1.2), существуют натуральные $n_i \le \lceil \log_2(b_i/a_i) \rceil$ ($i \in \{1,\dots,s\} \setminus \{\nu\}$) такие, что

$$\begin{aligned} &a_i\, 2^{n_i-1} \le |\gamma_i| \le a_i\, 2^{n_i} \quad \text{при } i \in I, \\ &a_j\, 2^{n_j-1}|\gamma_\nu| \le |\gamma_j| \le a_j\, 2^{n_j}|\gamma_\nu| \quad \text{при } j \in I' \end{aligned}$$

и воспользоваться леммой 1.1. □

Согласно лемме 1.2 для любого $\nu \in \{1,\dots,s\}$

$$\#\mathfrak{M}(\Gamma;\mathbf{P};\mathbf{p}) \le 2^s \prod_{i=\overline{1,s},\ i\ne\nu} (\log_2 P_i/p_i + 1). \tag{1.3}$$

Получим теперь более точную (при больших H) оценку для неполных решеток. Пусть $M = M(\Gamma)$ — базисная матрица Γ. Будем использовать обозначения:

$\mathfrak{I}_k(s)$ — множество всех k-элементных подмножеств $I = \{i_1, \ldots, i_k\}$ из $\{1, \ldots, s\}$,

$M(I)$ ($I \in \mathfrak{I}_k(s)$, $k > 0$) — матрица, составленная из строк M с номерами из I,

$d(I) = d(I, \Gamma) = \det M(I)$ при $I \in \mathfrak{I}_t(s)$,

$I_i = I \setminus \{i\}$ при $I \in \mathfrak{I}_k(s)$, $i \in I$.

Отметим, что величины $d(I, \Gamma)$ не зависят от выбора базисной матрицы.

Пусть $t < s$, $\gamma \in \Gamma$. Через $\tilde{M}$ обозначим матрицу, полученную из M, к которой в качестве последнего столбца дописали γ. Тогда $\operatorname{rang} \tilde{M} \leq t$. Следовательно, $\det \tilde{M}(I) = 0$ для любого $I \in \mathfrak{I}_{t+1}(s)$. Занумеруем элементы из I по возрастанию: $i_1 < i_2 < \ldots < i_{t+1}$. Раскладывая $\det \tilde{M}(I)$ по последнему столбцу получаем формулу

$$\sum_{k=1}^{t+1} (-1)^k \gamma_{i_k} \cdot d(I_{i_k}) = 0 \qquad \text{при } I \in \mathfrak{I}_{t+1}(s), \tag{1.4}$$

из которой вытекает оценка

$$|d(I_k)| \cdot |\gamma_k| \leq \sum_{i \in I_k} |\gamma_i| \cdot |d(I_i)| \qquad \text{при } I \in \mathfrak{I}_{t+1}(s), \quad k \in I. \tag{1.5}$$

Пусть $\Gamma^{(0)}$ — множество узлов $\gamma \in \Gamma$, все координаты которых не равны нулю.

Лемма 1.3. *Пусть $t < s$, $\Gamma^{(0)} \neq \emptyset$, $I \in \mathfrak{I}_{t+1}(s)$, причем $\operatorname{rang} M(I) = t$. Тогда для любого узла $\gamma \in \Gamma^{(0)}$ существуют такие $k, l \in I$, и $\alpha \in \mathbb{R}_+$, что*

$$\alpha |\gamma_l| \leq |\gamma_k| \leq t\alpha |\gamma_l|; \qquad d(I_k) \neq 0,\ d(I_l) \neq 0, \quad k \neq l, \tag{1.6}$$

причем α зависит только от k, l, I и Γ.

Доказательство. Возьмем номера $k, l \in I$, удовлетворяющие условиям

$$k \neq l, \quad |d(I_i)\gamma_i| \leq |d(I_l)\gamma_l| \leq |d(I_k)\gamma_k| \quad \text{при } i \in I \setminus \{k, l\}. \tag{1.7}$$

Так как все координаты γ не равны нулю, то из (1.4), (1.7) вытекает, что

$$d(I_l) \neq 0, \quad d(I_k) \neq 0.$$

Используя неравенство (1.5), получаем

$$\left| \frac{d(I_l)}{d(I_k)} \right| \cdot |\gamma_l| \leq |\gamma_k| \leq t \left| \frac{d(I_l)}{d(I_k)} \right| \cdot |\gamma_l|.$$

Осталось положить $\alpha = |d(I_l)|/|d(I_k)|$. □

Определение 1.1. Пусть $r = s - t$. Будем говорить, что множество $Q \subset \Gamma$ удовлетворяет условию (R), если для некоторого набора номеров k_j, $m_j \in \{1, \ldots, s\}$, $j = \overline{1, r}$, удовлетворяющего условиям

$$\{m_1, \ldots, m_r\} \cap \{k_1, \ldots, k_r\} = \emptyset, \quad k_i \neq k_j \text{ при } i \neq j,$$

существуют такие числа $\beta_j \in \mathbb{R}_+$, $j = \overline{1, r}$, что для любого $\gamma \in Q$

$$\beta_j |\gamma_{m_j}| \leq |\gamma_{k_j}| \leq t^j \beta_j |\gamma_{m_j}|, \quad j = \overline{1, r}. \tag{1.8}$$

Лемма 1.4. *Множество* $\Gamma^{(0)}$ *можно представить в виде объединения не более, чем* $(t(t+1))^{s-t}$ *множеств, удовлетворяющих условию (R).*

Доказательство. Пусть $r = s - t$. Используем математическую индукцию по $r = 0, 1, 2, \ldots$. При $r = 0$ утверждение леммы тривиально.

Индукционный переход от $(r-1)$ к r. Для краткости, положим $T = t(t+1)$. Возьмем любой набор $I \in \mathfrak{I}_{t+1}(s)$ такой, что $\operatorname{rang} M(I) = t$, где M — базисная матрица Γ. По лемме 1.3 множество $\Gamma^{(0)}$ можно представить в виде

$$\Gamma^{(0)} = \bigcup_{i=1}^{T} Q_i$$

так, что для каждого Q_i существуют номера $k = k(i)$, $l = l(i)$ и число $\alpha = \alpha(i) \in \mathbb{R}_+$, удовлетворяющие (1.6) для всех $\gamma \in U_i$. Пусть Γ_i — решетка, составленная из узлов Γ, у которых вычеркнули $k(i)$-ю координату. Так как $d(I_{k(i)}) \neq 0$, то $\Gamma_i \in \mathcal{L}_{t,s-1}(\mathbb{R})$. Значит, по предположению индукции множество $\Gamma_i^{(0)}$ можно представить в виде

$$\Gamma_i^{(0)} = \bigcup_{j=1}^{T^{r-1}} \tilde{Q}_{ij},$$

множества $\tilde{Q}_{ij}$ удовлетворяют условию (R). Следовательно,

$$\Gamma^{(0)} = \bigcup_{i=1}^{T} \bigcup_{j=1}^{T^{r-1}} Q_{ij}, \quad Q_{ij} = \left\{ \gamma \in Q_i : \quad \tilde{\gamma}^{(i)} \in \tilde{Q}_{ij} \right\},$$

узел $\tilde{\gamma}^{(i)}$ получается из γ вычеркиванием $k(i)$-й координаты. Осталось доказать, что каждое множество Q_{ij} удовлетворяет условию (R).

Возьмем любое $Q = Q_{ij}$. Тогда существуют номера k, l, k_j, m_j и числа $\alpha, \beta_j \in \mathbb{R}_+$ $(j = \overline{1, r-1})$ такие, что для любого $\gamma \in Q$ выполняются неравенства (1.6) и (1.8) (при $i, j = \overline{1, r-1}$), причем $k \neq k_j$, $k \neq m_j$ для всех j. Положим $k_r = k$. Осталось подобрать m_r и β_r. Возможны два случая.

1. Если $l \neq k_j$ $(j = \overline{1, r-1})$, то $m_r = l$, $\beta_r = \alpha$.
2. Если $l = k_\nu$, $\nu \in \{1, \ldots, r-1\}$, то

$$\begin{aligned} |\gamma_{k_r}| &= |\gamma_k| \leq t\alpha|\gamma_l| = t\alpha|\gamma_{k_\nu}| \leq t\alpha \cdot t^\nu \beta_\nu |\gamma_{m_\nu}| \leq (\alpha\beta_\nu) t^r |\gamma_{m_\nu}|, \\ |\gamma_{k_r}| &= |\gamma_k| \geq \alpha|\gamma_l| = \alpha|\gamma_{k_\nu}| \geq \alpha\beta_\nu |\gamma_{m_\nu}|. \end{aligned}$$

Следовательно, можно положить $m_r = m_\nu$, $\beta_r = \alpha\beta_{k_\nu}$. □

Лемма 1.5. *Пусть* $\Gamma \in \mathcal{L}_{t,s}(\mathbb{R})$, $\mathbf{P} = (P_1, \ldots, P_s), \mathbf{p} = (p_1, \ldots, p_s) \in \mathbb{R}_+^s$, *причем* $P_i \geq p_i$, $i = \overline{1, s}$. *Тогда справедлива оценка*

$$\#\mathfrak{M}(\Gamma; \mathbf{P}; \mathbf{p}) \leq 2^s \left(t(t+1)\right)^r \prod_{i=1}^{r} \left(i \log_2 t + 2\right) \cdot \log_2^{t-1}(2H) \leq C(t,s) \cdot \log_2^{t-1}(2H),$$

где

$$C(t,s) = 2^s \left(t(t+1)(r \log_2 t + 2)\right)^r, \quad r = s - t, \quad H = \max_{1 \leq i \leq s} P_i/p_i.$$

Доказательство. Пусть Q — любое множество из $\mathfrak{M}(\Gamma;\mathbf{P};\mathbf{p})$, удовлетворяющее условию (R). Так как $\mathfrak{M}(\Gamma;\mathbf{P};\mathbf{p}) \subset \Gamma^{(0)}$, то в силу леммы 1.4 достаточно доказать, что

$$\#\left(Q \cap \mathfrak{M}(\Gamma;\mathbf{P};\mathbf{p})\right) \le 2^s \prod_{i=1}^{r} \left(i \log_2 t + 2\right) \cdot \left(\log_2 H + 1\right)^{t-1}. \tag{1.9}$$

По определению условия (R) существуют номера k_j, $m_j \in \{1,\dots,s\}$ и $\beta_j \in \mathbb{R}_+$ ($j = \overline{1,r}$), удовлетворяющие (1.8). Положим $\nu = m_1$ и определим следующие множества индексов

$$\begin{aligned} I &= \{1,\dots,s\} \setminus \{k_1,\dots,k_r,\nu\}, \\ J &= \{k_i : \quad m_i = \nu, \quad i = \overline{1,r}\}, \\ K &= \{k_i : \quad m_i \ne \nu, \quad i = \overline{1,r}\}. \end{aligned}$$

Тогда $\{1,\dots,s\} = I \cup J \cup K \cup \{\nu\}$.

Возьмем любой $\gamma \in Q \cap \mathfrak{M}(\Gamma;\mathbf{P};\mathbf{p})$. Тогда существуют такие целые n_i, что

$$\begin{aligned} &1 \le n_i \le \log_2 P_i/p_i + 1, \\ &2^{n_i-1} p_i \le |\gamma_i| \le 2^{n_i} p_i \quad \text{при } i \in I. \end{aligned} \tag{1.10}$$

Так как $\{m_2,\dots,m_r\} \subset I$, то из (1.8), (1.10) вытекает

$$\begin{aligned} \beta_i\, 2^{n_{m_i}-1}\, p_{m_i} \le \quad |\gamma_{k_i}| \quad &\le \beta_i\, t^i\, 2^{n_{m_i}}\, p_{m_i} \quad k_i \in K, \\ \beta_i |\gamma_\nu| \le \quad |\gamma_{k_i}| \quad &\le \beta_i\, t^i |\gamma_\nu| \qquad\quad k_i \in J. \end{aligned} \tag{1.11}$$

По лемме 1.2 количество относительных минимумов γ, удовлетворяющих (1.10), (1.11) при заданном наборе n_i, не больше, чем

$$2^s \prod_{i=1}^{r} \left(\log_2 \left(t^i 2\right) + 1 \right) = 2^s \prod_{i=1}^{r} (i \log_2 t + 2).$$

Всевозможных наборов n_i не больше, чем $\left(\log_2 H + 1\right)^{t-1}$. Отсюда вытекает (1.9). □

§ 2. Оценки количества относительных минимумов

Верхняя оценка количества минимумов нецелочисленных решеток

Обоснование оценки (0.3.4) проведем по следующей схеме.

1. Доказываем, что минимумы, имеющие хотя бы одну «достаточно малую» координату, являются минимумами некоторых подрешеток меньшего ранга.
2. Используем лемму 1.5 для оценки количества оставшихся минимумов и применяем математическую индукцию.

Пусть $M = M(\Gamma)$ — базисная матрица решетки $\Gamma \in \mathcal{L}_{t,s}(\mathbb{R})$. Определим

$D(\Gamma)$ — максимум из модулей миноров t-го порядка матрицы M;

$$\lambda(\Gamma) = \min\{|\gamma|_\infty : \ \ \gamma \in \Gamma \setminus \{0\}\};$$

Согласно определениям,

$$D(\Gamma) = \max_{I \in \mathfrak{I}_t(s)} |d(I, \Gamma)|.$$

Напомним, что если $P \in \mathbb{R}_+$, то

$$\mathfrak{M}(\Gamma; P) = \{\gamma \in \mathfrak{M}(\Gamma) : \ \ |\gamma|_\infty \leq P\}.$$

Лемма 2.1. *Пусть* $\Gamma \in \mathcal{L}_{t,s}(\mathbb{R})$, $D = D(\Gamma)$, $\lambda = \lambda(\Gamma)$, $P \in (\lambda, +\infty)$. *Тогда*

$$\#\mathfrak{M}(\Gamma; P) \leq C(t,s) \cdot \log_2^{t-1}\left(\frac{2t!tP^t}{D} + 1\right) + \sum_{i=1}^{s} \#\mathfrak{M}(\tilde{\Gamma}_i; P), \tag{2.1}$$

где $\tilde{\Gamma}_i$ *— некоторые подрешетки* Γ *ранга, меньшего чем* t, *постоянная* $C(t,s)$ *определена в лемме 1.5.*

Доказательство. Для каждого номера $i \in \{1, \ldots, s\}$ определим

$$D_i = \max\left\{|d(I)| : \quad I \in \mathfrak{I}_t(s), \ \ I \ni i\right\}, \qquad P_i = \frac{tPD_i}{D}, \quad p_i = \frac{D_i}{t!P^{t-1}}$$

и представим множество $\mathfrak{M}(\Gamma; P)$ в виде

$$\begin{aligned}
\mathfrak{M}(\Gamma; P) &= \underline{\mathfrak{M}} \cup \overline{\mathfrak{M}}_1 \cup \ldots \cup \overline{\mathfrak{M}}_s, \\
\underline{\mathfrak{M}} &= \left\{\gamma \in \mathfrak{M}(\Gamma; P) : \quad p_i \leq |\gamma_i| \quad i = \overline{1,s}\right\}, \\
\overline{\mathfrak{M}}_j &= \left\{\gamma \in \mathfrak{M}(\Gamma; P) : \quad |\gamma_j| < p_j\right\}, \qquad j = \overline{1,s}.
\end{aligned}$$

Если $k \in \{1, \ldots, s\}$, $D_k = 0$, то из (1.5) вытекает, что $\gamma_k = 0$ для всех $\gamma \in \Gamma$. Поэтому, не умаляя общности, считаем, что $D_i \neq 0$ для всех i.

Докажем, что любые t узлов из $\overline{\mathfrak{M}}_j$ линейно зависимы. Пусть $\gamma^{(1)}, \ldots, \gamma^{(t)} \in \overline{\mathfrak{M}}_j \setminus \{0\}$. Определим матрицу A со столбцами ${\gamma^{(1)}}^T, \ldots, {\gamma^{(t)}}^T$. Возьмем набор $I \in \mathfrak{I}_t(s)$ такой, что $|d(I)| = D_j$ и обозначим через $A(I)$ матрицу, составленную из строк A с номерами из I. Пусть M — базисная матрица решетки Γ. Тогда существует невырожденная целочисленная квадратная матрица S такая, что $M \cdot S = A$. Так как $|\det M(I)| = |d(I)| = D_j$, то

$$|\det A(I)| = |\det S| \cdot |\det M(I)| \geq D_j.$$

С другой стороны, из определения множества $\overline{\mathfrak{M}}_j$ вытекает, что

$$|\det A(I)| < t! \cdot p_j \cdot P^{t-1} = D_j.$$

Получили противоречие. Значит, любые t узлов из $\overline{\mathfrak{M}}_j$ линейно зависимы.

Таким образом, $\overline{\mathfrak{M}}_j \subset \mathfrak{M}(\tilde{\Gamma}_j; P)$, где $\tilde{\Gamma}_j$ — некоторая подрешетка Γ ранга меньшего, чем t. Осталось доказать, что

$$\#\underline{\mathfrak{M}} \leq C(t,s) \cdot \log_2^{t-1}\left(\frac{2t!tP^t}{D} + 1\right). \tag{2.2}$$

Если для некоторого j $p_j > P_j$, то $\underline{\mathfrak{M}} = \emptyset$. Поэтому считаем, что $p_j \le P_j$, $j = \overline{1,s}$.
Пусть $I^* \in \mathfrak{I}_t(s)$, $|d(I^*)| = D$. Из (1.5) вытекает, что для любого $\gamma \in \Gamma$

$$|\gamma_i| \le \frac{D_i}{D} \sum_{j \in I^*} |\gamma_j|, \quad i = \overline{1,s}. \tag{2.3}$$

Если $i \in I^*$ оно тривиально (т.к. тогда $D_i = D$). Если $i \notin I^*$, то для доказательства достаточно в (1.5) выбрать $I = I^* \cup \{i\}$.

Используя (2.3), получаем для любого $\gamma \in \mathfrak{M}(\Gamma; P)$

$$|\gamma_i| \le \frac{D_i}{D} \cdot t \cdot P = P_i \quad i = \overline{1,s}.$$

Следовательно,

$$\underline{\mathfrak{M}} \subset \mathfrak{M}(\Gamma; \mathbf{P}; \mathbf{p}), \quad \mathbf{P} = (P_1, \dots, P_s), \quad \mathbf{p} = (p_1, \dots, p_s).$$

Применяя лемму 1.5 для оценки $\#\mathfrak{M}(\Gamma; \mathbf{P}; \mathbf{p})$ и учитывая, что $P_i/p_i = t!tP^t/D$, получаем (2.2). □

Замечание 2.1. Для полной решетки ($t = s$) неравенство (2.1) можно уточнить:

$$\#\mathfrak{M}(\Gamma; P) \le 2^s \cdot \log_2^{t-1}\left(\frac{2t!P^t}{D}\right) + \sum_{i=1}^{s} \#\mathfrak{M}(\tilde{\Gamma}_i; P).$$

Для этого достаточно положить $P_i = P$ и учесть, что $D_i = D$ для всех i.

Определим

$$N_{t,s}(P) = \sup_{\Gamma \in \mathcal{L}_{t,s}(\mathbb{R}), \lambda(\Gamma)=1} \#\mathfrak{M}(\Gamma; P).$$

Нетрудно проверить следующие формулы

$$\sup_{\Gamma \in \mathcal{L}_{t,s}(\mathbb{R}), \lambda(\Gamma)=\lambda} \#\mathfrak{M}(\Gamma; P) = N_{t,s}(P/\lambda). \tag{2.4}$$

$$N_{t,s}(P) \le N_{t+1,s}(P). \tag{2.5}$$

Пусть $\Gamma \in \mathcal{L}_{t,s}(\mathbb{R})$, $D = D(\Gamma)$, $\lambda = \lambda(\Gamma)$. Возьмем набор индексов $I^* \in \mathfrak{I}_t(s)$ такой, что $|d(I^*)| = D$. Тогда из (1.5) вытекает оценка

$$\forall \gamma \in \Gamma \qquad |\gamma|_\infty \le \sum_{j \in I^*} |\gamma_j|.$$

Согласно теореме Минковского о линейных формах существует ненулевой узел $\gamma \in \Gamma$ такой, что $|\gamma_j| \le D^{1/t}$ для всех $j \in I^*$. Тогда $|\gamma_i| \le tD^{1/t}$ при $i \notin I^*$ и поэтому

$$\left(\frac{\lambda}{t}\right)^t \le D. \tag{2.6}$$

Отметим, что для полной решетки выполняется лучшая оценка: $\lambda^t \le D$.

Теорема 2.1. *Для любого вещественного $P \in (1, +\infty)$ справедлива оценка*

$$N_{t,s}(P) \le \sum_{k=2}^{t} C(k,s) \cdot s^{t-k} \cdot \log_2^{k-1}\left(2 \cdot k! \cdot k^{k+1} \cdot P^k\right) + 2 \cdot s^{t-1},$$

где

$$C(k,s) = 2^s \left(k\left(k+1\right)\left((s-k)\log_2 k + 2\right)\right)^{s-k}.$$

Доказательство. Из леммы 2.1, оценок (2.5), (2.6) и очевидного неравенства $\lambda(\tilde{\Gamma}) \ge \lambda(\Gamma)$ при $\tilde{\Gamma} \subset \Gamma$, вытекает

$$N_{t,s}(P) \le C(t,s) \cdot \log_2^{t-1}\left(2 \cdot t! \cdot t^{t+1} \cdot P^t\right) + s \cdot N_{t-1,s}(P).$$

Осталось заметить, что $N_{1,s} = 2$ и применить математическую индукцию (по t). □

Из теоремы 2.1 и формулы 2.4 вытекает следующий результат.

Следствие 2.1. *Пусть $\Gamma \in \mathcal{L}_{t,s}(\mathbb{R})$, $\lambda = \lambda(\Gamma)$, $P \in (\lambda, +\infty)$. Тогда*

$$\#\mathfrak{M}(\Gamma, P) \le t^{t-1} \cdot C(t,s) \cdot \log_2^{t-1}(P/\lambda) + O_{t,s}\left(\log_2^{t-2}(P/\lambda) + 1\right),$$

где $C(t,s)$ — постоянная, определенная в лемме 1.5 и теореме 2.1.

Нижняя оценка максимального количества минимумов нецелочисленных решеток

Докажем, что существуют решетки $\Gamma \in \mathcal{L}_{t,s}(\mathbb{R})$, удовлетворяющие условию

$$\forall P \in (1, +\infty) \qquad \#\mathfrak{M}(\Gamma, P) \underset{\Gamma}{\gg} \ln^{t-1} P + 1. \tag{2.7}$$

Пусть K — чисто вещественное расширение степени t поля рациональных чисел $\mathbb{Q}$. Обозначим через $\omega_1^{(1)}, \ldots, \omega_t^{(1)}$ — базис, состоящий из целых поля K. Пусть $\omega_1^{(i)}, \ldots, \omega_t^{(i)}$ — сопряженные базисы ($i = \overline{2,t}$). Для каждого

$$\alpha = \sum_{j=1}^{t} \alpha_j \omega_j^{(1)} \in K$$

полагаем

$$x_i(\alpha) = \sum_{j=1}^{t} \alpha_j \omega_j^{(i)} \quad i = \overline{1,t},$$

т.е. $x(\alpha) = (\,x_1(\alpha),\, \ldots,\, x_t(\alpha))$ — геометрическое изображение числа α.

Пусть Γ — t-мерная полная решетка с базисной матрицей

$$\begin{pmatrix} \omega_1^{(1)} & \ldots & \omega_t^{(1)} \\ \vdots & & \vdots \\ \omega_1^{(t)} & \ldots & \omega_t^{(t)} \end{pmatrix},$$

то есть Γ состоит из узлов $x(\alpha)$, где $\alpha \in \Omega$, а Ω — порядок поля K с базисом $\omega_1^{(1)}, \ldots, \omega_t^{(1)}$. Докажем, что для такой решетки выполняется нижняя оценка (2.7).

Любой узел $\gamma \in \Gamma \setminus \{0\}$ имеет ненулевые координаты, причем $\gamma_1 \cdot \ldots \cdot \gamma_t$ — целое число. Следовательно, $|\gamma_1 \cdot \ldots \cdot \gamma_t| \geq 1$, и поэтому

$$E = \{\gamma \in \Gamma : |\gamma_1 \cdot \ldots \cdot \gamma_t| = 1\} \subset \mathfrak{M}(\Gamma).$$

Согласно теореме Дирихле об единицах (см. [5]) существуют числа $e_1, \ldots, e_{t-1} \in \Omega$ (основные единицы кольца Ω) такие, что все элементы α вида

$$\alpha = e_1^{n_1} \cdot \ldots \cdot e_{t-1}^{n_{t-1}} \qquad (n_i \in \mathbb{Z}, \quad i = \overline{1, t-1})$$

попарно различны, причем $x(\alpha) \in E$. Тогда очевидно, что

$$\#\left(E \cap \mathfrak{M}(\Gamma; P)\right) \underset{\Gamma}{\gg} \log_2^{t-1} P.$$

Оценка (2.7) доказана при $s = t$. Для построения неполной решетки из $\mathcal{L}_{t,s}(\mathbb{R})$ ($s > t$), удовлетворяющей (2.7), достаточно ко всем узлам $\gamma \in \Gamma$ дописать координаты $\gamma_{t+1}, \ldots, \gamma_s$, равные нулю.

Верхняя оценка количества минимумов целочисленных решеток

Мы докажем что любой минимум $\gamma \in \mathfrak{M}(\Gamma)$ целочисленной решетки $\Gamma \in \mathcal{L}_{t,s}(\mathbb{Z})$ удовлетворяет неравенству:

$$|\gamma|_\infty \leq t \cdot D(\Gamma) \tag{2.8}$$

и, как следствие теоремы 2.1, получим оценку для максимального числа относительных минимумов целочисленных решеток.

Возьмем любую решетку $\Gamma \in \mathcal{L}_{t,s}(\mathbb{Z})$ с базисом $m^{(1)}, \ldots, m^{(t)}$. Пусть $M = ((m_i^{(j)}))$ — соответствующая базисная матрица. Для $I \in \mathfrak{I}_{t-1}(s)$ и $j \in \{1, \ldots, t\}$ обозначим через $M^{(j)}(I)$ матрицу размера $(t-1) \times (t-1)$, полученную из M удалением j-го столбца и всех строк с номерами, не принадлежащими I. Пусть $\Upsilon(\Gamma)$ — подмножество в Γ, состоящее из узлов $\pm\eta(I)$, где $I \in \mathfrak{I}_{t-1}(s)$,

$$\eta(I) = \sum_{j=1}^{t} \det\left(M^{(j)}(I)\right) m^{(j)}.$$

Согласно свойствам определителя матрицы

$$\eta_i(I) = \begin{cases} 0 & \text{при } i \in I, \\ \pm \det M(I \cup i) & \text{при } i \notin I. \end{cases} \tag{2.9}$$

В частном случае $s = t$ (Γ — полная решетка) множество $\Upsilon(\Gamma)$ состоит из $2s$ узлов $\pm\eta(\bar{i})$ вида $\eta(\bar{i}) = (0, \ldots, 0, D, 0, \ldots, 0)$, т.е. i-я координата вектора $\eta(\bar{i})$ равна $D = \det\Gamma$, а остальные нули.

Лемма 2.2. *Пусть* $\Gamma \in \mathcal{L}_{t,s}(\mathbb{Z})$, $D = D(\Gamma)$ *и* $x \in \mathbb{R}^s$, *причем*

$$\forall \eta \in \Upsilon(\Gamma) \quad \exists j \in \{1, \dots, s\} : \quad |x_j| < |\eta_j|.$$

Тогда существует такой набор $I \in \mathfrak{I}_t(s)$, *что* $d(I) \neq 0$, *причем*

$$\forall i \in I \quad |x_i| \leq |d(I)|.$$

Доказательство. Проведем математическую индукцию по $r = s - t$.

При $r = 0$ утверждение леммы очевидно.

Индукционный переход от $(r-1)$ к r. Пусть I^* — набор из $\mathfrak{I}_t(s)$ для которого $|d(I^*)| = D$. Если $|x_i| \leq D$ для всех $i \in I^*$, то утверждение леммы справедливо (в силу (1.5)). Предположим, что это не так, то есть существует такой $j \in I^*$, что $|x_j| > D$. Тогда

$$|x_j| > |\eta_j| \quad \text{при } \eta \in \Upsilon(\Gamma). \tag{2.10}$$

Пусть $\tilde{\Gamma}$ — решетка в $\mathbb{Z}^{s-1}$, полученная из Γ удалением j-й координаты, а $\tilde{x} \in \mathbb{R}^{s-1}$ — вектор, полученный из x таким же способом. Если ранг $\tilde{\Gamma}$ меньше t, то $d(I) = 0$ для всех наборов $I \in \mathfrak{I}_t(s)$, не содержащих j. Тогда для набора $J^* = I^* \setminus \{j\}$ согласно (1.4)

$$\eta_j(J^*) = \pm D, \quad \eta_i(J^*) = 0 \quad \text{при } i \neq j.$$

Поэтому $|\eta_i(J^*)| \leq |x_i|$ при всех i, что противоречит условию леммы. Следовательно, ранг решетки $\tilde{\Gamma}$ равен t. Заметим, что множество $\Upsilon(\tilde{\Gamma})$ состоит из узлов $\pm\tilde{\eta}(J)$ по всем наборам $J \in \mathfrak{I}_{t-1}(s)$, не содержащим j, где $\tilde{\eta}(J)$ получен из $\eta(I)$ отбрасыванием j-й координаты. Ввиду (2.10), для любого $\tilde{\eta}(J) \in \Omega(\tilde{\Gamma})$ найдется такой номер $i \neq j$, что $|x_i| < |\eta_i|$. Таким образом, решетка $\tilde{\Gamma}$ и вектор $\tilde{x}$ удовлетворяют условиям леммы. Осталось воспользоваться предположением индукции. □

Следствие 2.2. *Относительные минимумы любой целочисленной решетки* $\Gamma \in \mathcal{L}_{t,s}(\mathbb{Z})$ *удовлетворяют оценке (2.8).*

Доказательство. Возьмем любой минимум $\gamma \in \mathfrak{M}(\Gamma)$. Если для некоторого $\eta \in \Upsilon(\Gamma)$ выполняется $|\gamma_i| = |\eta_i|$ для всех i, то оценка (2.8) очевидна. Пусть для любого $\eta \in \Upsilon(\Gamma)$ найдется индекс j для которого $|\eta_j| \neq |\gamma_j|$. Тогда, по определению относительного минимума,

$$\forall \eta \in \Upsilon(\Gamma) \;\; \exists j : \;\; |\gamma_j| < |\eta_j|$$

Значит, вектор $x = \gamma$ удовлетворяет условиям леммы 2.2. Согласно лемме 2.2 существует набор $I_0 \in \mathfrak{I}_t(s)$, для которого $d(I_0) \neq 0$ и для любого $i \in I_0$

$$|\gamma_i| \leq |d(I_0)| \leq D.$$

Если $s = t$, то сразу получаем $|\gamma|_\infty \leq D$. Пусть $s > t$. Используя формулу (1.4), в которой $I = I_0 \cup \{j\}$ приходим к оценкам:

$$|d(I_0)\gamma_j| \leq \sum_{i \in I_0} |\gamma_i| D \leq |d(I_0)| t \cdot D \quad \text{при } j \notin I_0.$$

Следовательно, $|\gamma_j| \leq t \cdot D$ для всех $j \notin I_0$. □

Следствие 2.3. *Пусть* $\Gamma \in \mathcal{L}_{t,s}(\mathbb{Z})$, $D = D(\Gamma) > 1$. *Тогда*

$$\#\mathfrak{M}(\Gamma) \underset{t,s}{\ll} \log_2^{t-1} D.$$

Доказательство. Согласно следствию 2.2, $\mathfrak{M}(\Gamma) = \mathfrak{M}(\Gamma; P)$ при $P = t \cdot D$. Применяя следствие 2.1, получаем требуемую оценку. □

§ 3. Оценки количества локальных минимумов

Пусть $s_0, \ldots, s_r$ — целые числа, причем

$$0 = s_0 < s_1 < \ldots < s_r = s.$$

Положим

$$t_l = s_l - s_{l-1}, \quad l = \overline{1, r}.$$

Пусть функции $\phi_l : \mathbb{R}^{t_l} \to \mathbb{R}$ $(l = \overline{1, r})$ лучевые, непрерывные и кусочно-дифференцируемые. Определим $\mathbf{\Phi} = (\Phi_1, \ldots, \Phi_r) : \mathbb{R}^s \to \mathbb{R}^r$ следующим образом

$$\Phi_1(x) = \phi_1(x_1, \ldots, x_{s_1}), \ldots, \Phi_l(x) = \phi_l(x_{s_{l-1}+1}, \ldots, x_{s_l}), \ldots, \Phi_r(x) = \phi_l(x_{s_{r-1}+1}, \ldots, x_s).$$

Напомним, что ненулевой узел γ решетки $\Gamma \in \mathcal{L}_s(\mathbb{R})$ мы называем локальным $\mathbf{\Phi}$-минимумом, если не существует ненулевого узла $\eta \in \Gamma$ такого, что

$$\Phi_l(\eta) \leq \Phi_l(\gamma), \quad l = \overline{1, r},$$

причем хотя бы одно из неравенств строгое.

Пусть $\mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$ — множество локальных $\mathbf{\Phi}$-минимумов решетки Γ. Основной целью настоящего параграфа является доказательство оценки (0.3.7).

Так как функции ϕ_l непрерывные, лучевые и кусочно-дифференцируемые, то существует такая постоянная $\kappa \geq 1$, что для всех $x, y \in \mathbb{R}^{t_l}$, $l \in \{1, \ldots, r\}$.

$$\kappa^{-1}|x| \leq \phi_l(x) \leq \kappa|x|, \tag{3.1}$$

$$|\phi_l(x) - \phi_l(y)| \leq \kappa|x - y| \tag{3.2}$$

Из (3.2), в частности, следует, что

$$\phi_l(x - y) \leq \phi_l(x) + \kappa \cdot |y|. \tag{3.3}$$

Лемма 3.1. *Возъмем любой* $l \in \{1, \ldots, r\}$ *и положим* $\phi = \phi_l$, $n = t_l$. *Пусть постоянные* α, ϵ *и конус* $K \subset \mathbb{R}^n$ *удовлетворяют условиям*

$$0 < \epsilon < \left(2\kappa^4\right)^{-1}, \quad 0 < \alpha < \sqrt{1 - 2\epsilon + \kappa^{-4}} - 1; \tag{3.4}$$

$$\forall x, y \in K \qquad (x, y) \geq (1 - \epsilon) \cdot |x| \cdot |y|, \tag{3.5}$$

где (x, y) *— скалярное произведение векторов* x, y. *Тогда*

а) если $x, y \in K \setminus \{0\}$, $|x| \leq |y|$, *то* $\phi(x - y) < \phi(y)$;

б) если $x, y \in K \setminus \{0\}$, *причем* $(1+\alpha)^{-1} \cdot |x| \le |y| \le (1+\alpha) \cdot |x|$, *то*

$$\phi(x-y) < \min\{\phi(x), \phi(y)\}.$$

Доказательство. Пусть $x', y' \in K$, $|x'| = |y'| = 1$. Тогда согласно (3.5)

$$|x' - y'| \le \sqrt{2\epsilon}. \tag{3.6}$$

Докажем утверждение а). Используя (3.3), получаем

$$\phi(x-y) = \phi\left(\left(x - y\cdot\frac{|x|}{|y|}\right) + y\left(\frac{|x|}{|y|} - 1\right)\right) \le \left(1 - \frac{|x|}{|y|}\right)\cdot\phi(y) + \kappa\cdot\left|x - y\cdot\frac{|x|}{|y|}\right|. \tag{3.7}$$

Применяя (3.1), (3.6), приходим к оценке

$$\left|x - y\cdot\frac{|x|}{|y|}\right| = |x|\cdot\left|\frac{x}{|x|} - \frac{y}{|y|}\right| \le |x|\cdot\sqrt{2\epsilon} \le \kappa\cdot\sqrt{2\epsilon}\cdot\frac{|x|}{|y|}\cdot\phi(y),$$

подставляя которую в (3.7), заключаем

$$\phi(x-y) \le \phi(y)\cdot\left(1 - \frac{|x|}{|y|}\cdot\left(1 - \kappa^2\cdot\sqrt{2\epsilon}\right)\right) < \phi(y),$$

так как $1 > \kappa^2\cdot\sqrt{2\epsilon}$. Утверждение а) доказано.

Докажем б). Пусть, например, $|x| \le |y|$. Ввиду (3.1) и (3.5),

$$\begin{aligned}\phi(x-y) &\le \kappa\cdot|x-y| \le \kappa\cdot\left(|x|^2 + |y|^2 - 2\cdot(1-\epsilon)\cdot|x|\cdot|y|\right)^{1/2} \le \\ &\le \kappa\cdot|x|\cdot\left(1 + (1+\alpha)^2 - 2(1-\epsilon)\right)^{1/2} = \kappa\cdot|x|\cdot\left(\alpha^2 + 2\alpha + 2\epsilon\right)^{1/2}.\end{aligned}$$

Поскольку

$$|x| \le \kappa\cdot\phi(x), \quad |x| \le |y| \le \kappa\cdot\phi(y), \quad \kappa^2\cdot(\alpha^2 + 2\alpha + 2\epsilon)^{1/2} < 1,$$

то $\phi(x-y) < \min\{\phi(x), \phi(y)\}$. Утверждение б) доказано. □

Замечание 3.1. Условие (3.5) означает, что угол между векторами x и y не больше, чем $\arccos(1-\epsilon)$. Поэтому, для любого $\epsilon \in (0,1)$, пространство $\mathbb{R}^n$ можно разбить на фиксированное (зависящее только от n и ϵ) число конусов K, каждый из которых удовлетворяет условию (3.5).

Пусть

$$\mathfrak{q}_l(x) = \left(\sum_{i\in I_l} x_i^2\right)^{1/2} \quad \text{при } x \in \mathbb{R}^s, \ \ l \in \{1, \dots, r\};$$
$$\lceil x \rceil = \min\{n \in \mathbb{Z} : n \ge x\} \quad \text{при } x \in \mathbb{R}.$$

Возьмем любые векторы $\mathbf{P} = (P_1, \dots, P_{r-1})$, $\mathbf{p} = (p_1, \dots, p_{r-1}) \in \mathbb{R}_+^{r-1}$ такие, что $P_i \ge p_i$. Для любой решетки $\Gamma \in \mathcal{L}_s(\mathbb{R})$ определим

$$\mathfrak{M}_{\mathbf{\Phi}}(\Gamma; \mathbf{P}, \mathbf{p}) = \{\gamma \in \mathfrak{M}_{\mathbf{\Phi}}(\Gamma) : \quad p_l \le \mathfrak{q}_l(\gamma) < P_l, \ l = \overline{1, r-1}\}.$$

Лемма 3.2. *Пусть выполняются следующие условия:*

а) $K = K_1 \times \ldots \times K_r$, *где* K_l — *конус из* $\mathbb{R}^{t_l}$ $(l = \overline{1,r})$, *причем существует положительная постоянная* $\epsilon < (2\kappa^4)^{-1}$ *такая, что*

$$(x,y) \geq (1-\epsilon)\cdot|x|\cdot|y| \quad \text{при } x,y \in K_l,\ \ l = \overline{1,r};$$

б) $\Gamma \in \mathcal{L}_s(\mathbb{R})$, $\mathbf{P},\mathbf{p} \in \mathbb{R}_+^{r-1}$ *и* $P_l > p_l > 0$, $l = \overline{1,r-1}$.

Тогда для любого вещественного α, *удовлетворяющего (3.4), справедлива оценка*

$$\#\left(K \cap \mathfrak{M}_{\mathbf{\Phi}}(\Gamma;\mathbf{P},\mathbf{p})\right) \leq \prod_{l=1}^{r-1} \left\lceil \log_{1+\alpha}(P_l/p_l) \right\rceil .$$

Доказательство. Возьмем любой минимум $\gamma \in K \cap \mathfrak{M}_{\mathbf{\Phi}}(\Gamma;\mathbf{P},\mathbf{p})$. Тогда существует набор $(k_1,\ldots,k_{r-1}) \in \mathbb{N}^{r-1}$ такой, что

$$\begin{aligned} &p_l(1+\alpha)^{k_l-1} \leq \mathfrak{q}_l(\gamma) < p_l\cdot(1+\alpha)^{k_l}, \quad l = \overline{1,r-1}, \\ &1 \leq k_l \leq \left\lceil \log_{1+\alpha}(P_l/p_l) \right\rceil . \end{aligned} \tag{3.8}$$

Докажем, что еще одного локального минимума, удовлетворяющего (3.8) и принадлежащего K, не существует. Действительно, пусть найдется $\eta \in K \cap \mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$ такой, что

$$p_l(1+\alpha)^{k_l-1} \leq \mathfrak{q}_l(\eta) < p_l\cdot(1+\alpha)^{k_l}, \quad l = \overline{1,r-1}.$$

Пусть, например, $\mathfrak{q}_r(\eta) \geq \mathfrak{q}_r(\gamma)$. Тогда, согласно лемме 3.1 а),

$$\phi_r(\eta-\gamma) < \phi_r(\eta).$$

Кроме того, $(1+\alpha)^{-1}\cdot\mathfrak{q}_l(\eta) \leq \mathfrak{q}_l(\gamma) \leq (1+\alpha)\cdot\mathfrak{q}_l(\eta)$, $l = \overline{1,r-1}$. Поэтому по лемме 3.1 б)

$$\phi_l(\eta-\gamma) < \min\{\phi_l(\eta),\phi_l(\gamma)\}, \quad l = \overline{1,r-1}.$$

Значит, узел $(\eta-\gamma)$ противоречит условию $\eta \in \mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$.

Таким образом, существует не более одного локального минимума $\gamma \in K$, удовлетворяющего (3.8), при фиксированном наборе $(k_1,\ldots,k_{r-1})$. Осталось заметить, что количество наборов k оценивается величиной $\prod_{l=1}^{r-1}\left\lceil \log_{1+\alpha}(P_l/p_l)\right\rceil$. □

Теорема 3.1. *Пусть* $\mathbf{P},\mathbf{p} \in \mathbb{R}_+^{r-1}$, *причем* $P_l > p_l > 0$, $l = \overline{1,r-1}$. *Тогда для любой решетки* $\Gamma \in \mathcal{L}_s(\mathbb{R})$ *справедлива оценка*

$$\#\mathfrak{M}_{\mathbf{\Phi}}(\Gamma;\mathbf{P},\mathbf{p}) \underset{\mathbf{\Phi}}{\ll} \prod_{l=1}^{r-1} \lceil \log_2(P_l/p_l) \rceil .$$

Доказательство. В соответствии с замечанием 3.1 пространство $\mathbb{R}^s$ можно разбить на фиксированное (зависящее только от I и κ) число множеств K, каждое из которых удовлетворяет условию а) леммы 3.2. Применяя лемму 3.2 для оценки количества минимумов, попадающих в каждую часть, получаем требуемое неравенство. □

Пусть $\gamma \in \mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$, причем $\mathfrak{q}_l(\gamma) \neq 0$, $l = \overline{1,r}$. Тогда, согласно (3.1) и определению локального минимума, множество

$$U(\gamma) = \left\{x \in \mathbb{R}^s : \ \ \mathfrak{q}_l(x) < \kappa^{-2} \cdot \mathfrak{q}_l(\gamma),\ l = \overline{1,r}\right\}$$

не содержит ненулевых узлов решетки Γ. Поэтому, по теореме Минковского о выпуклом теле, $\operatorname{mes} U(\gamma) \leq 2^s \cdot \det \Gamma$. Так как

$$\operatorname{mes} U(\gamma) = \prod_{l=1}^{r} \left(\kappa^{-2} \cdot \mathfrak{q}_l(\gamma)\right)^{t_l} \cdot \omega_l = \kappa^{-2s} \cdot \prod_{l=1}^{r} \omega_l \cdot (\mathfrak{q}_l(\gamma))^{t_l},$$

где ω_l — объем шара единичного радиуса в $\mathbb{R}^{t_l}$, то

$$\prod_{l=1}^{r} \omega_l \cdot (\mathfrak{q}_l(\gamma))^{t_l} \leq 2^s \cdot \kappa^{2s} \cdot \det \Gamma. \tag{3.9}$$

Следствие 3.1. *Пусть* $\Gamma \in \mathcal{L}_s(\mathbb{Z}; N)$, $N > 1$. *Тогда* $\#\mathfrak{M}_{\mathbf{\Phi}}(\Gamma) \underset{\mathbf{\Phi}}{\ll} \ln^{r-1} N$.

Доказательство. Разобьем множество $\mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$ на две непересекающиеся части:

$$\begin{aligned} \mathfrak{M}'_{\mathbf{\Phi}}(\Gamma) &= \{\gamma \in \mathfrak{M}_{\mathbf{\Phi}}(\Gamma) : \quad \mathfrak{q}_l(\gamma) \neq 0, \ \ l = \overline{1,r}\}, \\ \mathfrak{M}''_{\mathbf{\Phi}}(\Gamma) &= \mathfrak{M}_{\mathbf{\Phi}}(\Gamma) \setminus \mathfrak{M}'_{\mathbf{\Phi}}(\Gamma). \end{aligned}$$

Согласно (3.9) для всех $\gamma \in \mathfrak{M}'(\Gamma)$ выполняется оценка $\mathfrak{q}_l(\gamma) \underset{\mathbf{\Phi}}{\ll} N$, $l = \overline{1,r}$. Поэтому, используя теорему 3.1, в которой $P_l = O_{\mathbf{\Phi}}(N)$, $p_l = 1$, $l = \overline{1,r-1}$, получаем

$$\#\mathfrak{M}'_{\mathbf{\Phi}}(\Gamma) \underset{\mathbf{\Phi}}{\ll} \ln^{r-1} N. \tag{3.10}$$

Осталось оценить $\#\mathfrak{M}''_{\mathbf{\Phi}}(\Gamma)$. Не умаляя общности, рассматриваем минимумы γ, которые для некоторого $k < r$ удовлетворяют условиям:

$$\mathfrak{q}_l(\gamma) \neq 0, \ \ l = \overline{1,k}; \qquad \mathfrak{q}_i(\gamma) = 0, \ \ i = \overline{k+1,r} \tag{3.11}$$

Узел $\gamma' = (\gamma_1, \ldots, \gamma_{s_k})$ является локальным $(\Phi_1, \ldots, \Phi_k)$-минимумом решетки

$$\Gamma' = \{(x_1, \ldots, x_{s_k}) : \ \ (x_1, \ldots, x_{s_k}, 0, \ldots, 0) \in \Gamma\}.$$

Поэтому, согласно (3.10), количество минимумов $\gamma \in \mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$, удовлетворяющих (3.11), не больше, чем $O_{\mathbf{\Phi}}(\ln^{k-1} N' + 1)$, где $N' = \det \Gamma'$. Число N' делит N. Это вытекает из классического результата о существовании у целочисленной решетки базиса треугольного вида (см., например, [54, глава I, следствие 2]). Значит, $N' \leq N$ и, следовательно,

$$\#\mathfrak{M}''_{\mathbf{\Phi}}(\Gamma) \underset{\mathbf{\Phi}}{\ll} \ln^{r-2} N. \tag{3.12}$$

□

Глава II
Асимптотическое распределение целочисленных матриц

§ 1. Формулировка основного результата

Пусть множество $\Omega \subset \mathrm{GL}_s(\mathbb{R})$ удовлетворяет следующим условиям

(А) $\Omega = \left\{(\!(x_{ij})\!) : \quad (x_{i1}, \ldots, x_{is}) \in V_i, \;\; i = \overline{1,s}\right\}$, где $V_1, \ldots, V_s$ — связные конусы из $\mathbb{R}^s$ с липшицевыми границами;

(Б) существует такая постоянная $C > 0$, что для любой матрицы $X = (\!(x_{ij})\!) \in \Omega$

$$\prod_{i=1}^{s} \max_{1 \le j \le s} |x_{ij}| \le C \cdot \det X.$$

Целью настоящей главы является получения асимптотической формулы для количества целочисленных матриц заданного определителя, лежащих в Ω.

Из условия (А) следует, что множество Ω инвариантно относительно левого действия группы $\mathrm{D}_s(\mathbb{R}_+)$, состоящей из диагональных матриц размера $s \times s$ с положительными вещественными на главной диагонали. Рассмотрим $s(s-1)$-мерное многообразие $\mathrm{P}_s(\mathbb{R}) = \mathrm{D}_s(\mathbb{R}_+)\backslash\mathrm{GL}_s(\mathbb{R})$ — проективизацию группы $\mathrm{GL}_s(\mathbb{R})$ относительно левого действия группы $\mathrm{D}_s(\mathbb{R}_+)$.

Пусть $\mathcal{P}(\Omega)$ — образ множества $\Omega \subset \mathrm{GL}_s(\mathbb{R})$ при проективизации $\mathrm{GL}_s(\mathbb{R}) \to \mathrm{P}_s(\mathbb{R})$. Для любых $k = (k_1, \ldots, k_s) \in \{1, \ldots, s\}^s$ и $\theta = (\theta_1, \ldots, \theta_s) \in \{-1, 1\}^s$ определим

$$\begin{aligned} &\mathrm{GL}_s(\mathbb{R}, k, \theta) = \left\{(\!(x_{ij})\!) \in \mathrm{GL}_s(\mathbb{R}) : \quad x_{ik_i} = \theta_i, i = \overline{1,s}\right\}, \\ &\mathrm{P}_s(\mathbb{R}, k, \theta) = \mathcal{P}(\mathrm{GL}_s(\mathbb{R}, k, \theta)). \end{aligned}$$

Тогда $\mathrm{P}_s(\mathbb{R})$ содержится в объединении всех $\mathrm{P}_s(\mathbb{R}, k, \theta)$, причем каждый элемент из $\mathrm{P}_s(\mathbb{R}, k, \theta)$ имеет единственный прообраз при проективизации

$$\mathrm{GL}_s(\mathbb{R}, k, \theta) \to \mathrm{P}_s(\mathbb{R}, k, \theta).$$

Значит, множество всех $\mathrm{P}_s(\mathbb{R}, k, \theta)$ образуют атлас многообразия $\mathrm{P}_s(\mathbb{R})$, а матрицы из $\mathrm{GL}_s(\mathbb{R}, k, \theta)$ являются координатами соответствующих элементов $\mathrm{P}_s(\mathbb{R}, k, \theta)$.

Определим меру $\tilde{\mu} = \tilde{\mu}_{k,\theta}$ на плоскости $\mathrm{GL}_s(\mathbb{R}, k, \theta)$ следующим образом:

$$\tilde{\mu}(W) = \int_W \frac{dX}{|\det X|^s} \quad \text{при } W \subset \mathrm{GL}_s(\mathbb{R}, k, \theta),$$

где dX — дифференциал $s(s-1)$-мерной меры Лебега $s(s-1)$-мерной поверхности $\mathrm{GL}_s(\mathbb{R},k,\theta)$ в точке X (т.е. $dX=\prod_{\substack{1\le i,j\le s,\\ j\ne k_i}} dx_{ij}$). Она порождает меру $\mu=\mu_{k,\theta}$ на карте $\mathrm{P}_s(\mathbb{R},k,\theta)$:

$$\mu(w)=\tilde{\mu}(W)$$

где W — прообраз $w\subset \mathrm{P}_s(\mathbb{R},k,\theta)$ при проективизации $\mathrm{GL}_s(\mathbb{R},k,\theta)\to \mathrm{P}_s(\mathbb{R})$.

Нетрудно проверить, что мера μ не зависит от выбора карты, т.е.

$$\mu_{k,\theta}(w)=\mu_{n,\tau}(w)\quad \text{при } w\subset \mathrm{P}_s(\mathbb{R},k,\theta)\cap \mathrm{P}_s(\mathbb{R},n,\tau).$$

Действительно, пусть, например,

$$\theta=\tau=(1,1,\dots,1),\quad k=(1,1,\dots,1),\quad n=(2,1,\dots,1).$$

Пусть W_k и W_n — прообразы w при проективизациях

$$\mathrm{GL}_s(\mathbb{R},k,\theta)\to \mathrm{P}_s(\mathbb{R})\quad \text{и}\quad \mathrm{GL}_s(\mathbb{R},n,\tau)\to \mathrm{P}_s(\mathbb{R})$$

соответственно. Рассмотрим отображение $X\in \mathrm{GL}_s(\mathbb{R},k,\theta)\to Y\in \mathrm{GL}_s(\mathbb{R},n,\tau)$, действующее по формуле:

$$\begin{aligned} y_{1j}&=\frac{x_{1j}}{x_{12}},\quad j=\overline{1,s},\\ y_{ij}&=x_{ij},\quad i=\overline{2,s},\quad j=\overline{1,s}\end{aligned}$$

(1-ю строку X делим на x_{12}, а остальные не меняем). Тогда

$$\det Y=\frac{\det X}{x_{12}},\quad dY=\frac{dX}{x_{12}^s},\quad \frac{dY}{|\det Y|^s}=\frac{dX}{|\det X|^s}.$$

Значит, $\mu_{k,\theta}(w)=\mu_{n,\tau}(w)$.

Таким образом, мера μ не зависит от выбора карты и поэтому корректно определена на всем многообразии $\mathrm{P}_s(\mathbb{R})$.

Отображение $\mu\cdot\mathcal{P}$ инвариантно относительно правого действия группы $\mathrm{GL}_s(\mathbb{R})$, а именно, если $\Omega\subset \mathrm{GL}_s(\mathbb{R})$, причем $\mathcal{P}(\Omega)$ является μ-измеримым, то для любого $Q\in \mathrm{GL}_s(\mathbb{R})$

$$\mu(\mathcal{P}(\Omega))=\mu(\mathcal{P}(\Omega\cdot Q)).$$

Эта формула легко проверяется, если матрица Q удовлетворяет одному из условий:

1) Q — диагональная матрица;

2) для любого $X\in \mathrm{GL}_s(\mathbb{R})$ матрица $X\cdot Q$ получается из матрицы X изменением нумерации столбцов;

3) для любого $X\in \mathrm{GL}_s(\mathbb{R})$ матрица $X\cdot Q$ получается из матрицы X заменой одного из столбцов матрицы X на его сумму с некоторым другим столбцом.

В общем случае достаточно заметить, что любую невырожденную матрицу можно представить в виде произведения матриц Q вида 1), 2), 3).

Множество $\mathcal{P}(\Omega)$ является μ-измеримым, если Ω измеримо по Лебегу и удовлетворяет условию (Б).

Напомним, что

$$\begin{aligned}\mathcal{R}_s(N) &= \#(\mathrm{M}_s(\mathbb{Z};N)\setminus \mathrm{GL}_s(\mathbb{Z})) = \#\mathcal{L}_s(\mathbb{Z};N),\\ \chi(N) &= 1+\sum_{p\mid N}\frac{\ln p}{p} \qquad \text{(сумма по простым делителям } N).\end{aligned}$$

Основной результат настоящей главы заключается в следующем.

Теорема 1.1. *Пусть множество $\Omega\subset \mathrm{GL}_s(\mathbb{R})$ удовлетворяет условиям (А), (Б). Тогда для любого целого $N>1$ количество целочисленных матриц $M\in\Omega$, удовлетворяющих условию $\det M = N$, равно*

$$\mathcal{R}_s(N)\cdot\left(\nu(\Omega)\cdot\frac{\ln^{s-1}N}{(s-1)!}+O_\Omega\left(\chi(N)\cdot\ln^{s-2}N\right)\right), \tag{1.1}$$

где

$$\nu(\Omega)=\frac{\mu(\mathcal{P}(\Omega))}{\zeta(2)\cdot\zeta(3)\cdot\ldots\zeta(s)}.$$

Замечание 1.1. При $s=2$, используя метод Портера [132], можно получить более точную формулу со степенным понижением в остаточном члене.

Замечание 1.2. Пусть множество $\Omega\subset\mathrm{GL}_s(\mathbb{R})$ удовлетворяет (А) и следующему условию:

$$\text{(Б')}\qquad \exists C>0:\qquad \forall X\in\Omega\quad \prod_{i=1}^{s}\max_{1\le j\le s}|x_{ij}|\le C\cdot|\det X|.$$

(В отличие от (Б) в правой части неравенства стоит $|\det X|$ вместо $\det X$). Тогда количество целочисленных матриц $M\in\Omega$, у которых $|\det M|=N$, также равно (1.1). Действительно, пусть

$$\Omega^+=\{X\in\Omega:\ \det X\ge 0\},\quad \Omega^-=\{X\in\Omega:\ \det X\le 0\}.$$

Множества $\mathcal{P}(\Omega^+)$ и $\mathcal{P}(\Omega^-)$ не пересекаются. Поэтому, применяя теорему 1.1, получаем требуемый результат.

Следствие 1.1. *Пусть множество $\Omega\subset\mathrm{GL}_s(\mathbb{R})$ удовлетворяет условиям (А), (Б'). Пусть $d\in\mathbb{N}$, $(d_2,d_3,\ldots,d_s)\in\mathbb{Z}^{s-1}$. Тогда для любого целого $N>1$ количество целочисленных матриц $M=(\!(m_{ij})\!)$, удовлетворяющих условиям*

$$\begin{aligned}&M\in\Omega,\quad \det M=N,\\ &m_{i1}+\sum_{j=2}^{s}d_j\cdot m_{ij}\equiv 0 \pmod d,\quad i=\overline{1,s},\end{aligned}$$

равно

$$\mathcal{R}_s(N)\cdot\left(\nu(\Omega)\cdot\frac{\ln^{s-1}N}{(s-1)!}+O_{\Omega,d,d_2,\ldots,d_s}\left(\chi(N)\cdot\ln^{s-2}N\right)\right),$$

Доказательство. Определим матрицу G по формуле

$$G = \begin{pmatrix} 1/d & 0 & 0 & \dots & 0 \\ d_2/d & 1 & 0 & \dots & 0 \\ d_3/d & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ d_s/d & 0 & 0 & \dots & 1 \end{pmatrix}$$

Тогда количество искомых матриц равно количеству целочисленных матриц определителя N, лежащих в $\Omega \cdot G = \{X \cdot G : X \in \Omega\}$. Множество $\Omega \cdot G$ удовлетворяет условиям (А), (Б'). Осталось применить теорему 1.1, замечание 1.2 и учесть, что $\mu(\mathcal{P}(\Omega)) = \mu(\mathcal{P}(\Omega \cdot G))$. □

Доказательство теоремы 1.1 мы проведем следующим образом. Очевидно, что

$$\#(\Omega \cap \mathrm{M}_s(\mathbb{Z}; N)) = \sum_{d|N} \sum_{\substack{M \in \mathrm{M}_{s-1,s}(\mathbb{Z}), \\ d(M)=d}} K(M, N),$$

где $d(M)$ — наибольший общий делитель миноров $(s-1)$-го порядка матрицы M, а $K(M, N)$ — количество наборов $(n_1, \dots, n_s) \in \mathbb{Z}^s$ для которых

$$\begin{pmatrix} m_{11} & \dots & m_{1s} \\ \vdots & & \vdots \\ m_{(s-1)1} & \dots & m_{(s-1)s} \\ n_1 & \dots & n_s \end{pmatrix} \in \Omega \cap \mathrm{M}_s(\mathbb{Z}, N).$$

Чтобы вычислить $K(M, N)$ мы должны найти количество узлов некоторой решетки, лежащих в заданном множестве. Эта задача является достаточно простой. Основная проблема заключается в вычислении суммы

$$\sum_{\substack{M \in \mathrm{M}_{s-1,s}(\mathbb{Z}), \\ d(M)=d}} K(M, N).$$

Будем использовать следующие обозначения: если $X \in \mathrm{M}_{t,s}(\mathbb{R})$, $t \le s$, то

$D(X)$ — максимум из модулей миноров t-го порядка матрицы X,
$\mathcal{N}_i(X) = \max\limits_{1 \le j \le s} |x_{ij}|, \quad i = \overline{1, t}.$

Тогда условие (Б) можно записать так

$$\exists C > 0 : \quad \forall X \in \Omega \qquad \prod_{i=1}^{s} \mathcal{N}_i(X) \le C \cdot \det X.$$

Кроме того, если $\Omega \subset \mathrm{GL}_s(\mathbb{R})$, то $\Omega(\mathbb{Z}; N) = \Omega \cap \mathrm{M}_s(\mathbb{Z}; N)$ — множество целочисленных матриц $M \in \Omega$ таких, что $\det M = N$.

§ 2. Вспомогательные результаты

О разложениях целочисленных матриц

Пусть $\mathrm{TM}_s(\mathbb{Z})$ — множество целочисленных нижнетреугольных матриц $T = (\!(t_{ij})\!) \in \mathrm{M}_s(\mathbb{Z})$ таких, что для любого i

$$\begin{array}{ll} 0 < t_{ii}, & \\ 0 \le t_{ij} < t_{ii} & \text{при } j < i, \\ t_{ij} = 0 & \text{при } j > i. \end{array}$$

Теорема 2.1. *Любая целочисленная решетка $\Gamma \in \mathcal{L}_s(\mathbb{Z})$ имеет единственную базисную матрицу $M \in \mathrm{TM}_s(\mathbb{Z})$.*

Доказательство существования см, например, в [54, гл. 1]. Единственность легко проверяется от противного (достаточно рассмотреть разложение векторов одного базиса по другому базису).

Из теоремы 2.1 вытекает следующий результат.

Следствие 2.1. *Любая невырожденная матрица $M \in \mathrm{M}_s(\mathbb{Z})$ единственным образом представима в виде: $M = T \cdot Q$, где $T \in \mathrm{TM}_s(\mathbb{Z})$, $Q \in \mathrm{GL}_s(\mathbb{Z})$.*

Определим функции $\tau_k : \mathbb{N} \to \mathbb{R}_+$, $k = 0, 1, 2, \ldots$ следующим образом

$$\begin{aligned} \tau_0(N) &= 1, \\ \tau_k(N) &= \sum_{d|N} \frac{\tau_{k-1}(d)}{d} \quad \text{при } k \ge 1. \end{aligned} \tag{2.1}$$

Используя индукцию, получаем

$$\tau_k(N) = \sum_{m_1 \cdot \ldots \cdot m_k | N} \frac{1}{m_1^k} \cdot \frac{1}{m_2^{k-1}} \cdot \ldots \cdot \frac{1}{m_k}, \tag{2.2}$$

где суммирование ведется по всем натуральным $m_1, \ldots, m_k$ таким, что $m_1 \cdot \ldots \cdot m_k \mid N$.

Возьмем любое натуральное N. По теореме 2.1,

$$\begin{aligned} \mathcal{R}_s(N) &= \#\mathrm{TM}_s(\mathbb{Z}, N) = \sum_{\substack{m_1, \ldots, m_s \in \mathbb{N}, \\ m_1 \cdot \ldots \cdot m_s = N}} m_2 \cdot m_3^2 \cdot \ldots \cdot m_s^{s-1} = \\ &= \sum_{\substack{m_1, \ldots, m_{s-1} \in \mathbb{N}, \\ m_1 \cdot \ldots \cdot m_{s-1} | N}} \frac{N^{s-1}}{m_1^{s-1} \cdot m_2^{s-2} \cdot \ldots \cdot m_{s-1}} = N^{s-1} \cdot \tau_{s-1}(N). \end{aligned} \tag{2.3}$$

Из (2.2), (2.3) вытекают оценки

$$\tau_{s-1}(N) \asymp \sigma_{-1}(N), \quad \mathcal{R}_s(N) \asymp N^{s-1} \cdot \sigma_{-1}(N). \tag{2.4}$$

Через $d(M)$ будем обозначать наибольший общий делитель миноров t-го порядка матрицы $M \in \mathrm{M}_{t,s}(\mathbb{Z})$, $t < s$.

Лемма 2.1. *Пусть $M \in \mathrm{M}_{t,s}(\mathbb{Z})$, $t < s$. Тогда $d(M) = d(M \cdot Q)$ для любого $Q \in \mathrm{GL}_s(\mathbb{Z})$.*

Для доказательства достаточно заметить, что правое действие любой матрицы из $\mathrm{GL}_s(\mathbb{Z})$ можно представить в виде произведения следующих отображений:

1) изменение нумерации столбцов;

2) изменение знака некоторого столбца;

3) замена одного столбца на его сумму с другим.

Оценки мощности некоторых матричных множеств

Лемма 2.2. *Пусть* $C \in \mathbb{R}_+$, $Y \in \mathrm{GL}_s(\mathbb{R})$, $(P_1, \dots, P_s) \in \mathbb{R}_+^s$. *Тогда количество матриц* $X \in Y \cdot \mathrm{GL}_s(\mathbb{Z})$, *удовлетворяющих условиям*

$$\mathcal{N}_i(X) \le P_i, \quad i = \overline{1,s}, \qquad P_1 \cdot \ldots \cdot P_s \le C \cdot |\det X|, \tag{2.5}$$

не больше, чем $C_1 = (1 + 2 \cdot s! \cdot C)^{s^2-1}$.

Доказательство. Рассмотрим сначала случай, когда Y удовлетворяет следующим дополнительным условиям:

$$\mathcal{N}_i(Y) \le P_i, \;\; i = \overline{1,s}; \quad \prod_{i=1}^{s} P_i \le C \cdot \det Y. \tag{2.6}$$

Пусть $|X|_\infty$ — максимум из модулей элементов матрицы X. Разделим каждую i-ю строку Y на P_i и обозначим полученную матрицу через Y'. Тогда

$$|Y'|_\infty \le 1, \quad C^{-1} \le \det Y'. \tag{2.7}$$

Пусть $f(Y,P)$ — количество матриц $X \in Y \cdot \mathrm{GL}_s(\mathbb{Z})$, удовлетворяющих (2.5). Тогда

$$\begin{aligned} f(Y,P) &= \#\{X \in Y \cdot \mathrm{GL}_s(\mathbb{Z}) : \quad \mathcal{N}_i(X) \le P_i, \;\; i = \overline{1,s}\} = \\ &= \#\{X' \in Y' \cdot \mathrm{GL}_s(\mathbb{Z}) : \quad |X'|_\infty \le 1\} = \#\{Q \in \mathrm{GL}_s(\mathbb{Z}) : \quad |Y' \cdot Q|_\infty \le 1\}. \end{aligned}$$

Если $Q \in \mathrm{GL}_s(\mathbb{Z})$ и $|Y' \cdot Q|_\infty \le 1$, то

$$|Q|_\infty = |Y'^{-1} \cdot Y' \cdot Q|_\infty \le s \cdot |Y'^{-1}|_\infty \cdot |Y' \cdot Q|_\infty \le s \cdot |Y'^{-1}|_\infty \le s \cdot \frac{(s-1)! \cdot |Y'|_\infty^{s-1}}{|\det Y'|}.$$

Учитывая (2.7), получаем $|Q|_\infty \le s! \cdot C$. Количество таких Q не больше, чем $(1 + 2 \cdot C \cdot s!)^{s^2-1}$. Лемма доказана при выполнении условий (2.6).

Пусть (2.6) не выполняется. Возьмем любую $Y_0 \in Y \cdot \mathrm{GL}_s(\mathbb{Z})$, удовлетворяющую (2.6), где Y заменяем на Y_0 (если таких матриц нет, то утверждение леммы тривиально). Тогда $Y \cdot \mathrm{GL}_s(\mathbb{Z}) = Y_0 \cdot \mathrm{GL}_s(\mathbb{Z})$, $\det Y = \det Y_0$. Заменяя Y на Y_0, приходим к случаю (2.6). □

Напомним, что множество $\mathrm{M}_s(\mathbb{Z}, N)$ состоит из целочисленных матриц размера $s \times s$ определителя N. Аналогичным образом, положим

$$\mathrm{TM}_s(\mathbb{Z}; N) = \mathrm{TM}_s(\mathbb{Z}) \cap \mathrm{M}_s(\mathbb{Z}, N)$$

— множество матриц из $\mathrm{TM}_s(\mathbb{Z})$ определителя N.

Следствие 2.2. *Пусть $N \in \mathbb{N}$, $C \in \mathbb{R}_+$, $(P_1, \dots, P_s) \in \mathbb{R}_+^s$, причем $P_1 \cdot \ldots \cdot P_s \le C \cdot N$. Тогда количество матриц $M \in \mathrm{M}_s(\mathbb{Z}, N)$, удовлетворяющих неравенствам*

$$\mathcal{N}_i(M) \le P_i, \quad i = \overline{1, s},$$

не больше, чем $C_1 \cdot \mathcal{R}_s(N)$, где C_1 — постоянная из леммы 2.2.

Доказательство. Используя следствие 2.1 и лемму 2.2, получаем, что искомое число равно

$$\sum_{T \in \mathrm{TM}_s(\mathbb{Z};N)} \#\left\{M \in T \cdot \mathrm{GL}_s(\mathbb{Z}) : \ \mathcal{N}_i(M) \le P_i, \ i = \overline{1, s}\right\} \le \sum_{T \in \mathrm{TM}_s(\mathbb{Z};N)} C_1 = C_1 \cdot \mathcal{R}_s(N).$$

□

Следствие 2.3. *Пусть $N \in \mathbb{N} \cap [2, +\infty)$, $C \in [1, +\infty)$. Тогда количество матриц $M \in \mathrm{M}_s(\mathbb{Z}, N)$, удовлетворяющих условиям:*

$$\prod_{i=1}^{s} \mathcal{N}_i(M) \le C \cdot N,$$
$$\exists n, l \in \{1, \dots, s\} : \quad \frac{1}{C} \cdot \mathcal{N}_l(M) \le \mathcal{N}_n(M) \le C \cdot \mathcal{N}_l(M), \quad n \ne l,$$

не больше, чем $O_{s,C}(\mathcal{R}_s(N) \cdot \ln^{s-2} N)$.

Доказательство. Для любой матрицы M, удовлетворяющей указанным условиям, существует набор $k = (k_1, \dots, k_s) \in \mathbb{N}^s$ такой, что

$$2^{k_i - 1} \le \mathcal{N}_i(M) \le 2^{k_i}, \quad i = \overline{1, s}, \tag{2.8}$$

$$\log_2 N - C' \le \sum_{i=1}^{s} k_i \le \log_2 N + C', \tag{2.9}$$

$$k_l - C'' \le k_n \le k_l + C'', \tag{2.10}$$

где

$$C' = \max\{s!, \log_2 C + s\}, \quad C'' = \log_2 C + 1.$$

Так как $2^{k_1} \cdot \ldots 2^{k_s} \le 2^{C'} \cdot N$, то используя следствие 2.2, мы видим, что количество матриц $M \in \mathrm{M}_s(\mathbb{Z}, N)$, удовлетворяющих (2.8) (при фиксированном наборе k), не больше, чем $O_{s,C}(\mathcal{R}_s(N))$. Осталось заметить, что количество наборов для которых выполняются (2.9), (2.10) оценивается величиной $O_{s,C}(\ln^{s-2} N)$. □

Пусть $d_t(M)$ — наибольший общий делитель миноров t-го порядка, составленных из первых t строк матрицы $M \in \mathrm{M}_s(\mathbb{Z})$.

Следствие 2.4. *Пусть $d, N \in \mathbb{N}$, $C \in [1, +\infty)$, $(P_1, \dots, P_{s-1}) \in [1, +\infty)^{s-1}$. Тогда количество матриц $M \in \mathrm{M}_s(\mathbb{Z}; N)$, удовлетворяющих условиям*

$$\prod_{i=1}^{s} \mathcal{N}_i(M) \le C \cdot N,$$
$$P_i \le \mathcal{N}_i(M) \le 2P_i, \quad i = \overline{1, s-1},$$
$$d_{s-1}(M) = d,$$

не больше, чем $O_{s,C}\left(N^{s-1} \cdot \sigma_{-1}(d) \cdot d^{-1}\right)$.

Доказательство. Положим

$$P_s = \frac{C \cdot N}{2 \cdot (P_1 \cdot \ldots \cdot P_{s-1})}.$$

Тогда для любой M, удовлетворяющей требуемым условиям,

$$\mathcal{N}_i(M) \le 2P_i, \quad i = \overline{1,s}.$$

Последовательно применяя следствие 2.1, леммы 2.1, 2.2, получаем, что искомое число не больше, чем

$$\sum_{\substack{T \in \mathrm{TM}_s(\mathbb{Z};N),\\ d_{s-1}(T)=d}} \# \left\{ M \in T \cdot \mathrm{GL}_s(\mathbb{Z}) : \ \mathcal{N}_i(M) \le 2P_i,\ i = \overline{1,s}, \quad \prod_{i=1}^{s} P_i = \frac{C}{2} |\det M| \right\} \underset{s,C}{\ll}$$
$$\ll \#\{T \in \mathrm{TM}_s(\mathbb{Z};N) : \ d_{s-1}(T) = d\}.$$

Нетрудно заметить, что

$$\#\{T \in \mathrm{TM}_s(\mathbb{Z};N) : \ d_{s-1}(T) = d\} = (N/d)^{s-1} \cdot \#\mathrm{TM}_{s-1}(\mathbb{Z};d).$$

Осталось воспользоваться (2.3) для оценки $\#\mathrm{TM}_{s-1}(\mathbb{Z};d)$. □

Лемма 2.3. *Пусть $t \in \{1,\ldots,s-1\}$, $C \in [1,+\infty)$, $d \in \mathbb{N}$, $(P_1,\ldots,P_s) \in [1,+\infty)^s$. Тогда количество матриц $M \in \mathrm{M}_s(\mathbb{Z})$, удовлетворяющих условиям:*

$$d_t(M) \equiv 0 \pmod d, \tag{2.11}$$

$$\mathcal{N}_i(M) \le P_i,\ i = \overline{1,s}, \qquad \prod_{i=1}^{s} P_i \le C \cdot |\det M|, \tag{2.12}$$

не больше, чем $O_{s,t,C}\left(\dfrac{\sigma_{-1}(d)}{d^{s-t+1}} \cdot (P_1 \cdot \ldots \cdot P_s)^s\right)$.

Доказательство. Если матрица $M \in \mathrm{M}_s(\mathbb{Z})$ удовлетворяет (2.12), то

$$|\det M| \le R = s! \cdot \prod_{i=1}^{s} P_i.$$

Поэтому, используя леммы 2.1, 2.2 и следствие 2.1, мы видим, что количество матриц $M \in \mathrm{M}_s(\mathbb{Z})$, удовлетворяющих (2.11), (2.12), не больше, чем

$$\sum_{\substack{T \in \mathrm{TM}_s(\mathbb{Z}),\ \det T \le R,\\ d_t(T) \equiv 0 \pmod d}} \#\{M \in T \cdot \mathrm{GL}_s(\mathbb{Z}) : \ M \text{ удовлетворяет (2.12)}\} \le C_1 \cdot f_t(R,d),$$

где $f_t(R,d)$ — количество $T \in \mathrm{TM}_s(\mathbb{Z})$ для которых $\det T \le R$ и $d_t(T) \equiv 0 \pmod d$.

Пусть множество $\mathbb{N}^s(R)$ состоит из $m \in \mathbb{N}^s$ таких, что $m_1 \cdot \ldots \cdot m_s \leq R$. Тогда

$$f_t(R,d) = \sum_{\substack{m\in\mathbb{N}^s(R),\\ m_1\cdot\ldots\cdot m_t\equiv 0 \pmod d}} m_2\cdot m_3^2\cdot\ldots\cdot m_s^{s-1} = \sum_{n=1}^{\infty}\sum_{\substack{m\in\mathbb{N}^s(R),\\ m_1\cdot\ldots\cdot m_t=nd}} m_2\cdot m_3^2\cdot\ldots\cdot m_s^{s-1} \underset{s,t}{\ll}$$

$$\underset{s,t}{\ll}\sum_{n=1}^{\infty}\sum_{\substack{m\in\mathbb{N}^t,\\ m_1\cdot\ldots\cdot m_t=nd}} m_2\cdot m_3^2\cdot\ldots\cdot m_t^{t-1}\cdot\left(\frac{R}{m_1\cdot\ldots\cdot m_t}\right)^s =$$

$$= R^s\cdot\sum_{n=1}^{\infty}\sum_{\substack{m\in\mathbb{N}^t,\\ m_1\cdot\ldots\cdot m_t=nd}} \frac{1}{m_1^s}\cdot\frac{1}{m_2^{s-1}}\cdot\ldots\cdot\frac{1}{m_t^{s-t+1}} =$$

$$= R^s\cdot\sum_{n=1}^{\infty}\frac{1}{(n\cdot d)^{s-t+1}}\sum_{\substack{m\in\mathbb{N}^t,\\ m_1\cdot\ldots\cdot m_t=nd}} \frac{1}{m_1^{t-1}}\cdot\frac{1}{m_2^{t-2}}\cdot\ldots\cdot\frac{1}{m_{t-1}} \underset{t}{\ll}$$

$$= \frac{R^s}{d^{s-t+1}}\sum_{n=1}^{\infty}\frac{1}{n^{s-t+1}}\cdot\sigma_{-1}(nd) \ll \frac{R^s}{d^{s-t+1}}\cdot\sigma_{-1}(d) = (s!)^s\cdot(P_1\cdot\ldots\cdot P_s)^s\cdot\frac{\sigma_{-1}(d)}{d^{s-t+1}}.$$

□

Напомним, что если $M \in \mathrm{M}_{t,s}(\mathbb{Z})$ $(t < s)$, то через $d(M)$ и $D(M)$ мы обозначаем соответственно наибольший общий делитель и максимум модулей миноров t-го порядка матрицы M.

Следствие 2.5. *Пусть $t \in \{1,\ldots,s-1\}$, $C \in [1,+\infty)$, $d \in \mathbb{N}$, $(P_1,\ldots,P_t) \in \mathbb{R}_+^t$. Тогда количество матриц $M \in \mathrm{M}_{t,s}(\mathbb{Z})$, удовлетворяющих условиям:*

$$d(M) \equiv 0 \pmod d,$$
$$\mathcal{N}_i(M) \leq P_i,\ i = \overline{1,t}, \qquad \prod_{i=1}^{t} P_i \leq C\cdot D(M),$$

не больше, чем $O_{s,t,c}\left(\dfrac{\sigma_{-1}(d)}{d^{s-t+1}}\cdot(P_1\cdot\ldots\cdot P_t)^s\right)$.

Доказательство. Не умаляя общности рассматриваем только такие матрицы M, что

$$D(M) = \left|\det\begin{pmatrix} m_{11} & \ldots & m_{1t}\\ \vdots & & \vdots\\ m_{t1} & \ldots & m_{tt}\end{pmatrix}\right|.$$

Допишем к M следующие строки (снизу)

$$(\underbrace{0,\ldots,0}_{t},1,0\ldots,0),\quad (\underbrace{0,\ldots,0}_{t+1},1,0\ldots,0),\quad \ldots,(0,\ldots,0,1).$$

Обозначим полученную матрицу через $\tilde{M}$. Тогда $|\det\tilde{M}| = D(M)$ и $\tilde{M}$ удовлетворяет условиям (2.11), (2.12), в которых $P_i = 1$ при $i \geq t+1$. Осталось применить следствие 2.3. □

§ 3. Вычисление некоторых сумм

Пусть $|\nabla f|$ — модуль градиента скалярной функции f.

Лемма 3.1. *Пусть*

а) V *— конус в* $\mathbb{R}^s$ *с липшицевой границей;*

б) $P \in [1, +\infty)$, $V_P = V \cap [-P, P]^s$;

в) $f \in C^1(\overline{V_P})$, *причем существует такая постоянная* $C > 0$, *что для всех* $x \in V_P$

$$0 \le f(x) \le \frac{C}{P^s}, \quad |\nabla f(x)| \le \frac{C}{P^{s+1}};$$

г) $\Gamma \in \mathcal{L}_s(\mathbb{Z}; D)$, *причем* $D \le P$.

Тогда

$$\sum_{\gamma \in V_P \cap \Gamma} f(\gamma) = \frac{1}{D} \int_{V_P} f(x)\, dx + O_V\left(\frac{C}{P}\right).$$

Доказательство. Возьмем такой базис $\{e^{(i)}\}_{i=1}^s$ решетки Γ, что

$$|e^{(i)}|_\infty \le D, \quad i = \overline{1, s}.$$

Этому условию удовлетворяет, например, базис из теоремы 2.1.

Пусть $\Pi = \{t_1 e^{(1)} + \ldots + t_s e^{(s)} : t_i \in [0, 1)\}$ — основной параллелепипед Γ, построенный на векторах $e^{(1)}, \ldots, e^{(s)}$. Для любого узла $\gamma \in \Gamma$ определим

$$\Pi(\gamma) = \Pi + \{\gamma\} = \{x + \gamma : x \in \Pi\}$$

Тогда

$$\forall x, y \in \Pi(\gamma) \qquad |x - y|_\infty \le s \cdot D. \tag{3.1}$$

Пусть

$$\begin{aligned} \Gamma' &= \{\gamma \in \Gamma \cap V_P : \quad \Pi(\Gamma) \subset V_P\}, \\ \Gamma'' &= (\Gamma \cap V_P) \setminus \Gamma', \\ V_P' &= \bigcup_{\gamma \in \Gamma'} \Pi(\gamma). \end{aligned}$$

Сразу отметим, что мера ϵ-окрестности поверхности ∂V_P оценивается величиной $O_V(\epsilon \cdot P^{s-1})$. Используя (3.1), получаем следующие утверждения.

1. Множество $V_P \setminus V_P'$ содержится в $U(sD)$, где $U(sD)$ — окрестность поверхности ∂V_P радиуса $s \cdot D$ (относительно нормы $|\cdot|_\infty$). Поэтому $\operatorname{mes}(V_P \setminus V_P') \underset{V}{\ll} D \cdot P^{s-1}$ и, используя условие в), имеем

$$\begin{aligned} \frac{1}{D} \int_{V_P} f(x)\, dx &= \frac{1}{D} \int_{V_P'} f(x)\, dx + \frac{1}{D} \int_{V_P \setminus V_P'} f(x)\, dx = \\ &= \frac{1}{D} \int_{V_P'} f(x)\, dx + O_V\left(\frac{C}{P}\right). \end{aligned} \tag{3.2}$$

2. Если $\gamma \in \Gamma''$, то $\Pi(\gamma) \subset U(sD)$. Поэтому

$$\#\Gamma'' = \frac{1}{D} \sum_{\gamma \in \Gamma''} \operatorname{mes} \Pi(\gamma) \leq \frac{\operatorname{mes} U(sD)}{D} \underset{V}{\ll} \frac{s \cdot D \cdot P^{s-1}}{D} \underset{s}{\ll} P^{s-1}.$$

Используя условие в), получаем

$$\sum_{\gamma \in \Gamma \cap V_P} f(\gamma) = \sum_{\gamma \in \Gamma'} f(\gamma) + \sum_{\gamma \in \Gamma''} f(\gamma) = \sum_{\gamma \in \Gamma'} f(\gamma) + O_V\left(\frac{C}{P}\right). \tag{3.3}$$

Возьмем любую точку $\gamma \in \Gamma'$. Используя формулу конечных приращений Лагранжа и теорему о среднем для интегралов, получаем

$$\left| \frac{1}{D} \int_{\Pi(\gamma)} f(x)\, dx - f(\gamma) \right| \leq \sup_{x \in \Pi(\gamma)} |\nabla f(x| \cdot \sup_{y \in \Pi(\Gamma)} |x_\gamma - \gamma|.$$

Применяя в) и (3.1), приходим к оценке

$$f(\gamma) = \frac{1}{D} \int_{\Pi(\gamma)} f(x)\, dx + O\left(\frac{C \cdot D}{P^{s+1}}\right).$$

Подставляя последнее соотношение в правую часть (3.3), заключаем

$$\sum_{\gamma \in \Gamma \cap V_P} f(\gamma) = \sum_{\gamma \in \Gamma'} f(\gamma) + O_V\left(\frac{C}{P}\right) = \frac{1}{D} \int_{V'_P} f(x)\, dx + O_V\left(\frac{CD}{P^{s+1}} \cdot \#\Gamma' + \frac{C}{P}\right).$$

Осталось использовать (3.2) и учесть, что

$$\#\Gamma' = \frac{\operatorname{mes} V'(P)}{D} \leq \frac{(2P)^s}{D}.$$

□

Лемма 3.2. *Пусть* $t \in \{1, \ldots, s-1\}$, $M \in \mathrm{M}_{t-1,s}(\mathbb{Z})$, $r = d(M)$. *Возьмем любое натуральное* d, *кратное* r. *Пусть решетка* $\Gamma = \Gamma(M, d)$ *состоит из решений* $n \in \mathbb{Z}^s$ *сравнения*

$$d \left(\begin{pmatrix} m_{11} & \ldots & m_{1s} \\ \vdots & & \vdots \\ m_{(t-1)1} & \ldots & m_{(t-1)s} \\ n_1 & \ldots & n_s \end{pmatrix} \right) \equiv 0 \pmod{d}.$$

Тогда $\det \Gamma = (d/r)^{s-t+1}$.

Доказательство. Используя следствие 2.1 и лемму 2.1, мы всегда можем свести нашу задачу к случаю $m_{ij} = 0$ при $j > i$. Тогда

$$\Gamma = \{(n_1, \ldots, n_s) \in \mathbb{Z}^2 : \quad rn_i \equiv 0 \pmod{d} \text{ при } i \geq t\}$$

и требуемая формула становится очевидной. □

Лемма 3.3. *Пусть $t \in \{1, \dots, s-1\}$ и выполняются следующие условия*

а) матричное множество Θ_t определяется формулой

$$\Theta_t = \{X \in \mathrm{M}_{t,s}(\mathbb{R}) : \quad (x_{i1}, x_{i2}, \dots, x_{is}) \in V_i,\ i = \overline{1,t}\},$$

где V_i — конусы из $\mathbb{R}^s \setminus \{0\}$ с липшицевыми границами, причем существует такая постоянная $C_1 > 0$, что для любого $X \in \Theta_t$

$$\prod_{i=1}^{t} \mathcal{N}_i(X) \le C_1 \cdot D(X);$$

б) $\mathbf{P} = (P_1, \dots, P_t) \in [1, +\infty)^t$, множество $\Theta_t(\mathbf{P})$ определяется формулой

$$\Theta_t(\mathbf{P}) = \{X \in \Theta_t : \ \ P_i \le \mathcal{N}_i(X) < 2P_i,\ i = \overline{1,t}\};$$

в) $f : \Theta_t \to \mathbb{R}_+$, причем $f \in C^1(\overline{\Theta_t(\mathbf{P})})$ и для любых $X \in \Theta_t$, $\mathrm{Diag} \in \mathrm{D}_t(\mathbb{R}_+)$

$$f(\mathrm{Diag} \cdot X) = \frac{f(X)}{(\det \mathrm{Diag})^s}.$$

Тогда для любого натурального d имеет место асимптотическая формула:

$$\sum_{\substack{M \in \Theta_t(\mathbf{P}),\\ d(M)=d}} f(M) = \frac{\tau_{t-1}(d)}{d^{s-t+1}} \left(\prod_{k=s-t+1}^{s} \zeta(k) \right)^{-1} \int_{\Theta(\mathbf{P})} f(X)\, dX + O_{\Theta_t}\left(C_2 \cdot \frac{\ln P_* + \sigma_{-1}(d)}{d \cdot P_*^{1/2}} \right),$$

где

$$P_* = \min_{1 \le i \le t} P_i,$$
$$C_2 = \max\left\{ \max\{f(X), |\nabla f(X)|\} : \ \ X \in \Theta_t,\ \mathcal{N}_i(X) = 1,\ i = \overline{1,t} \right\}.$$

Доказательство. Пусть $S_t(\mathbf{P}, d, f)$ — искомая сумма. Для любого $k \in \{1, \dots, t-1\}$ определим

$$\begin{aligned} \Theta_k &= \{X \in \mathrm{M}_{k,s}(\mathbb{R}) : \quad (x_{i1}, \dots, x_{is}) \in V_i,\ \ i = \overline{1,k}\}, \\ \Theta_k(\mathbf{P}) &= \{X \in \Theta_k : \quad P_i \le \mathcal{N}_i(X) < 2P_i,\ \ i = \overline{1,k}\}. \end{aligned}$$

Из условия а) вытекает, что для любого $Y \in \Theta_k$

$$\prod_{i=1}^{k} \mathcal{N}_i(Y) \underset{t,s}{\ll} D(Y), \tag{3.4}$$

а используя в) и определение C_2 получаем, что для всех $X \in \Theta_t(\mathbf{P})$, $k, j \in \{1, \dots, s\}$

$$f(X) \le \frac{C_2}{(P_1 \cdot \ldots \cdot P_t)^s}, \qquad \left| \frac{\partial f(X)}{x_{kj}} \right| \le \frac{C_2}{P_k \cdot (P_1 \cdot \ldots \cdot P_t)^s}. \tag{3.5}$$

Доказательство проведем, используя математическую индукцию по $t = 1, 2, \ldots$.
База индукции. Пусть $t = 1$. Используя свойства функции Мебиуса, получаем

$$S_1(\mathbf{P}, d, f) = \sum_{\substack{m \in \Theta_1(\mathbf{P}), \\ \text{нод } (m_1, \ldots, m_s) = d}} f(m) = \sum_{n \in N} \mu(n) s(n), \tag{3.6}$$

где

$$s(n) = \sum_{m \in \Theta_1(\mathbf{P}) \cap (nd \cdot \mathbb{Z}^s)} f(m).$$

Согласно (3.5) $f(m) \le C_2/P_1^s$ при $m \in \Theta_1(\mathbf{P})$. Поэтому

$$s(n) \le \frac{C_2}{P_1^s} \cdot \# \left\{ m \in (nd\mathbb{Z}^s) \setminus \{0\} : \ \ |m|_\infty \le 2P_1 \right\} \le \frac{C_2}{P_1^s} \cdot (4P_1/nd)^s \underset{s}{\ll} \frac{C_2}{(nd)^s}.$$

Используя последнее соотношение, оценим сумму по $n > K = P_1^{1/s}/d$:

$$\left| \sum_{n > K} \mu(n) s(n) \right| \le \frac{C_2}{d^s} \sum_{n > K} \frac{1}{n^s} \ll \frac{C_2}{d^s} \cdot \frac{1}{K^{s-1}} = \frac{C_2}{d \cdot P_1^{1-1/s}}. \tag{3.7}$$

Здесь и далее в этому доказательстве постоянные в оценках $\ll$, $O(\ldots)$ могут зависеть только от t, s и Θ_t.

Применяя лемму 3.1, получаем асимптотическую формулу для $s(n)$

$$s(n) = \frac{1}{(nd)^s} \int_{\Theta_1(\mathbf{P})} f(x)\, dx + O\left(\frac{C_2}{P_1} \right),$$

используя которую, вычислим сумму по $n \le K$:

$$\sum_{n \le K} \mu(n) s(n) = \frac{1}{d^s \zeta(s)} \int_{\Theta_1(\mathbf{P})} f(x)\, dx + O\left(\frac{C_2}{P_1} \cdot K + \xi \right),$$
$$\xi = \sum_{n > K} \frac{1}{(nd)^s} \int_{\Theta_1(\mathbf{P})} f(x)\, dx \ll \frac{1}{d^s K^{s-1}} \cdot \frac{C_2}{P_1^s} \cdot \operatorname{mes} \Theta_1(P) \ll \frac{C_2}{d^s K^{s-1}}.$$

Следовательно, имеет место соотношение

$$\sum_{n \le K} \mu(n) s(n) = \frac{1}{d^s \zeta(s)} \int_{\Theta_1(\mathbf{P})} f(x)\, dx + O\left(\frac{C_2}{d \cdot P_1^{1-1/s}} \right),$$

подставляя которое и (3.7) в (3.6), получаем утверждение леммы при $t = 1$.

Индукционный переход от $(t-1)$ к t. Для любых $M' \in \Theta_{t-1}$, $m \in V_t$ определим

$$f(M', m) = f\left(\mathcal{M}(M', m) \right), \quad d(M', m) = d\left(\mathcal{M}(M', m) \right),$$

где

$$\mathcal{M}(M', m) = \begin{pmatrix} m'_{11} & \ldots & m'_{1s} \\ \vdots & & \vdots \\ m'_{(t-1)1} & \ldots & m'_{(t-1)s} \\ m_1 & \ldots & m_s \end{pmatrix}$$

— матрица, полученная из M' к которой в качестве t-й строки дописали m. Определим также

$$V_t(P_t) = \{x \in V_t : \quad P_t \le |x|_\infty \le 2P_t\}.$$

Используя свойства функции Мебиуса, получаем

$$\begin{aligned} S_t(\mathbf{P}, d, f) &= \sum_{r|d} \sum_{\substack{M' \in \Theta_{t-1}(\mathbf{P}),\\ d(M')=r}} \sum_{\substack{m \in V_t(P_t),\\ d(M',m)=d}} f(M', m) = \\ &= \sum_{r|d} \sum_{\substack{M' \in \Theta_{t-1}(\mathbf{P}),\\ d(M')=r}} \sum_{n \in \mathbb{N}} \mu(n) \sum_{\substack{m \in V_t(P_t),\\ d(M',m) \equiv 0 \pmod{nd}}} f(M', m) = S'_t + S''_t, \end{aligned} \tag{3.8}$$

где

$$\begin{aligned} S'_t = S'_t(\mathbf{P}, d, f) &= \sum_{r|d} \sum_{\substack{M' \in \Theta_{t-1}(\mathbf{P}),\\ d(M')=r}} \sum_{n \le K} \mu(n) \sum_{\substack{m \in V_t(P_t),\\ d(M',m) \equiv 0 \pmod{nd}}} f(M', m), \\ S''_t = S''_t(\mathbf{P}, d, f) &= \sum_{r|d} \sum_{\substack{M' \in \Theta_{t-1}(\mathbf{P}),\\ d(M')=r}} \sum_{n > K} \mu(n) \sum_{\substack{m \in V_t(P_t),\\ d(M',m) \equiv 0 \pmod{nd}}} f(M', m), \\ K &= \frac{P_t^{1/(s-t+1)}}{d}, \end{aligned}$$

т.е. S'_t — сумма по $n \le K$, а S''_t — сумма по $n > K$.

Используя первое неравенство из (3.5) и лемму 2.3, оценим S''_t:

$$\begin{aligned} S''_t &\ll \sum_{n>K} \sum_{\substack{M \in \Theta_t(\mathbf{P}),\\ d(M) \equiv 0 \pmod{nd}}} f(M) \ll \\ &\ll \frac{C_2}{(P_1 \cdot \ldots \cdot P_t)^s} \sum_{n>K} \#\{M \in \Theta(\mathbf{P}) : \ d(M) \equiv 0 \pmod{nd}\} \ll \\ &\ll C_2 \cdot \sum_{n>K} \frac{\sigma_{-1}(nd)}{(nd)^{s-t+1}} \ll C_2 \cdot \frac{\ln(Kd)+1}{d^{s-t+1} K^{s-t}} \ll C_2 \cdot \frac{\ln P_t + 1}{d \cdot P_t^{1/2}}. \end{aligned} \tag{3.9}$$

Вычислим S'_t. Согласно лемме 3.2, определитель решетки, составленной из решений $m \in \mathbb{Z}^s$ сравнения $d(M', m) \equiv 0 \pmod{nd}$, равен $(nd/r)^{s-t+1}$. Функция $x \in V_t(P_t) \to f(M', x)$ удовлетворяет условиям леммы 3.1 (в которой $C = C_2/(P_1 \cdot \ldots \cdot P_{t-1})^s$). Поэтому, применяя лемму 3.1, получаем

$$\sum_{\substack{m \in V_t(P_t),\\ d(M',m) \equiv 0 \pmod{nd}}} f(M', m) = \left(\frac{r}{nd}\right)^{s-t+1} \cdot f_0(M') + O\left(\frac{C_2}{P_t \cdot (P_1 \cdot \ldots \cdot P_{t-1})^s}\right),$$

где функция $f_0 : \Theta_{t-1} \to \mathbb{R}_+$ определяется формулой:

$$f_0(X') = \int_{V_t(P_t)} f(X', x)\, dx.$$

Отметим, что согласно первой оценки из (3.5)

$$\forall X' \in \Theta_{t-1}(\mathbf{P}) \qquad f_0(X') \le \frac{C_2 \cdot \operatorname{mes} V_t(P_t)}{(P_1 \cdot \ldots \cdot P_t)^s} \ll \frac{C_2}{(P_1 \cdot \ldots \cdot P_{t-1})^s}.$$

Поэтому

$$\sum_{n\le K}\mu(n)\left(\frac{r}{nd}\right)^{s-t+1}\cdot f_0(M')=\left(\frac{r}{d}\right)^{s-t+1}\frac{f_0(M')}{\zeta(s-t+1)}+O\left(\frac{1}{K^{s-t}}\frac{C_2}{(P_1\cdot\ldots\cdot P_{t-1})^s}\right).$$

Следовательно,

$$\sum_{n\le K}\mu(n)\sum_{\substack{m\in V_t(P_t),\\ d(M',m)\equiv 0 \pmod{nd}}} f(M',m)=\left(\frac{r}{d}\right)^{s-t+1}\cdot\frac{f_0(M')}{\zeta(s-t+1)}+R_0(\mathbf{P},d,r),$$

где

$$\begin{aligned} R_0(\mathbf{P},d,r) &\ll \frac{C_2}{P_t\cdot(P_1\cdot\ldots\cdot P_{t-1})^s}\cdot K+\frac{1}{K^{s-t}}\frac{C_2}{(P_1\cdot\ldots\cdot P_{t-1})^s}= \\ &= \frac{C_2}{(P_1\cdot\ldots\cdot P_{t-1})^s}\cdot\left(\frac{K}{P_t}+\frac{(r/d)^{s-t+1}}{K^{s-t}}\right).\end{aligned}$$

Подставляя полученное соотношение в формулу для S'_t, имеем

$$S'_t=\frac{1}{\zeta(s-t+1)}\sum_{r|d}\left(\frac{r}{d}\right)^{s-t+1}\cdot S_{t-1}(\mathbf{P},r,f_0)+R(\mathbf{P},d),$$

где

$$\begin{aligned} S_{t-1}(\mathbf{P},r,f_0)&=\sum_{\substack{M'\in\Theta_{t-1}(\mathbf{P}),\\ d(M')=r}} f_0(M'),\\ R(\mathbf{P},d)&\ll\sum_{r|d}\#\{M'\in\Theta_{t-1}(\mathbf{P}):d(M')=r\}\cdot R_0(\mathbf{P},d,r).\end{aligned}$$

Оценим $\#\{M'\in\Theta_{t-1}(\mathbf{P}):d(M')=r\}$ с помощью леммы 2.3. Учитывая, что

$$\sum_{r|d}\frac{\sigma_{-1}(r)}{r}\ll\sigma_{-1}(d),$$

получаем

$$R(\mathbf{P},d)\ll C_2\cdot\sum_{r|d}\frac{\sigma_{-1}(r)}{r^{s-t+2}}\cdot\left(\frac{K}{P_t}+\frac{(r/d)^{s-t+1}}{K^{s-t}}\right)\ll C_2\left(\frac{K}{P_t}+\frac{\sigma_{-1}(d)}{d^{s-t+1}K^{s-t}}\right)\ll C_2\frac{\sigma_{-1}(d)}{d\sqrt{P_t}}.$$

Таким образом,

$$S'_t=\frac{1}{\zeta(s-t+1)}\sum_{r|d}\left(\frac{r}{d}\right)^{s-t+1}\cdot S_{t-1}(\mathbf{P},r,f_0)+O\left(C_2\frac{\sigma_{-1}(d)}{d\sqrt{P_t}}\right).$$

Учитывая (3.9), (3.8), заключаем

$$S_t(\mathbf{P},d,f)=\frac{1}{\zeta(s-t+1)}\sum_{r|d}\left(\frac{r}{d}\right)^{s-t+1}\cdot S_{t-1}(\mathbf{P},r,f_0)+O\left(C_2\frac{\sigma_{-1}(d)+\ln P_t}{d\sqrt{P_t}}\right). \quad (3.10)$$

Согласно предположению индукции,

$$S_{t-1}(\mathbf{P},r,f_0)=\frac{\tau_{t-2}(r)}{r^{s-t+2}}\left(\prod_{k=s-t+2}^{s}\zeta(k)\right)^{-1}\int_{\Theta_{t-1}(\mathbf{P})}f_0(X')\,dX'+O\left(C_2\cdot\frac{\sigma_{-1}(r)+\ln P_*}{r\cdot P_*^{1/2}}\right).$$

Подставляя последнее соотношение в (3.10), учитывая, что

$$\int_{\Theta_{t-1}(\mathbf{P})}f_0(X')\,dX'=\int_{\Theta_t(\mathbf{P})}f(X)\,dX,$$
$$\sum_{r|d}\left(\frac{r}{d}\right)^{s-t+1}\cdot\frac{\tau_{t-2}(r)}{r^{s-t+2}}=\frac{\tau_{t-1}(d)}{d^{s-t+1}},$$
$$\sum_{r|d}\left(\frac{r}{d}\right)^{s-t+1}\cdot\frac{1}{r}\ll\frac{1}{d},\qquad\sum_{r|d}\left(\frac{r}{d}\right)^{s-t+1}\cdot\frac{\sigma_{-1}(r)}{r}\ll\frac{\sigma_{-1}(d)}{d},$$

приходим к требуемой формуле. □

§ 4. Доказательство теоремы 1.1

Для любой $\Gamma\in\mathcal{L}_s(\mathbb{R})$ определим

$$\upsilon(\Gamma)=\min\left(\max_{1\le i\le s}\left|a^{(i)}\right|_\infty\right),$$

где минимум берется по всем базисам $\{a^{(i)}\}_{i=1}^s$ решетки Γ. Из хорошо известных результатов о последовательных минимумах (см., например, [54, глава 8]) вытекает, что для любой линейно-независимой системы $\{b^{(i)}\}_{i=1}^s\subset\Gamma$

$$\upsilon(\Gamma)\le C_0\cdot\max_{1\le i\le s}\left|b^{(i)}\right|_\infty,\tag{4.1}$$

где положительная постоянная C_0 зависит только от s.

Если $\epsilon\in\mathbb{R}_+$, а S — гиперповерхность из $\mathbb{R}^s$, то полагаем

$$U(S,\epsilon)=\{x\in\mathbb{R}^s:\quad\inf_{y\in S}|x-y|_\infty\le\epsilon\}$$

— замыкание ϵ-окрестности S относительно нормы $|\cdot|_\infty$.

Лемма 4.1. *Пусть $\Gamma\in\mathcal{L}_s(\mathbb{Z},D)$, $x_0\in\mathbb{R}^s$, $\upsilon=\upsilon(\Gamma)$. Возьмем любое ограниченное измеримое по Лебегу множество G из $\mathbb{R}^s$. Тогда*

$$\left|\#\left(G\cap(\Gamma+x_0)\right)-\frac{1}{D}\mathrm{mes}\,G\right|\ \le\ \frac{1}{D}\mathrm{mes}\,U(\partial G,s\upsilon),\tag{4.2}$$

$$\left|\#\left(G\cap(\Gamma+x_0)\right)-\frac{1}{D}\mathrm{mes}\,G\right|\ \le\ \#((\Gamma+x_0)\cap U(\partial G,s\upsilon)).\tag{4.3}$$

Доказательство. Не умаляя общности считаем, что $x_0 = 0$.

Пусть $\{a^{(i)}\}_{i=1}^s$ — такой базис Γ, что

$$\max_{1\le i\le s} \left|a^{(i)}\right|_\infty = \upsilon(\Gamma).$$

Пусть $\Pi = \{t_1 a^{(1)} + \ldots + t_s a^{(s)} : t_i \in [0,1)\}$ — основной параллелепипед Γ, построенный на векторах $a^{(i)}$. Для любого узла $\gamma \in \Gamma$ определим

$$\Pi(\gamma) = \Pi(\Gamma) + \gamma = \{\gamma + y : y \in \Pi(\Gamma)\}.$$

Отметим, что $\Pi(\gamma) \cap \Gamma = \{\gamma\}$. Кроме того,

$$\forall x, y \in \Pi(\gamma) \qquad |x - y|_\infty \le s \cdot \upsilon.$$

Пусть G_* — объединение всех $\Pi(\gamma)$, которые содержатся в G, а G^* — пересекаются с G, т.е.

$$G_* = \bigcup_{\gamma\in\Gamma:\ \Pi(\gamma)\subset G} \Pi(\gamma), \quad G^* = \bigcup_{\gamma\in\Gamma:\ \Pi(\gamma)\cap G\ne\emptyset} \Pi(\gamma).$$

Тогда

$$G_* \subset G \subset G^* \subset (G \cup U(\partial G, s\upsilon)).$$

Так как

$$\frac{\operatorname{mes} G_*}{D} = \#(\Gamma \cap G_*), \quad \frac{\operatorname{mes} G^*}{D} = \#(\Gamma \cap G^*), \quad \frac{\operatorname{mes}(G^* \setminus G_*)}{D} = \#(\Gamma \cap (G^* \setminus G_*)),$$

то

$$\begin{aligned} |D^{-1}\operatorname{mes} G - \#(G \cap \Gamma)| &= |D^{-1}\operatorname{mes}(G \setminus G_*) - \#(\Gamma \cap (G \setminus G_*))| \le \\ &\le D^{-1}\operatorname{mes}(G^* \setminus G_*) = \#(\Gamma \cap (G^* \setminus G_*)). \end{aligned}$$

Осталось заметить, что $(G^* \setminus G_*) \subset U(\partial G, s\upsilon)$. □

Лемма 4.2. *Пусть множество $\Omega \subset \mathrm{GL}_s(\mathbb{R})$ удовлетворяет условиям (А), (Б). Пусть d — делитель натурального N, а $\mathbf{P} = (P_1, \ldots, P_{s-1}) \in [1, +\infty)^{s-1}$. Положим*

$$\hat{P} = \prod_{i=1}^{s-1} P_i, \quad P^* = \max_{1\le i\le s-1} P_i, \quad P_* = \min_{1\le i\le s-1} P_i, \quad C_* = C_0 \cdot 2^s \cdot (C \cdot s! \cdot s)^2,$$

где C_0 — постоянная из оценки (4.1). Предположим, что

$$\hat{P} \cdot P^* \le \frac{N}{C_*}. \tag{4.4}$$

Тогда количество целочисленных матриц $M \in \Omega$, удовлетворяющих условиям:

$$\begin{gathered} \det M = N, \\ d_{s-1}(M) = d, \\ P_i \le \mathcal{N}_i(M) < 2P_i, \quad i = \overline{1, s-1}, \end{gathered}$$

равно

$$\ln^{s-1} 2 \cdot \nu(\Omega) \cdot \frac{\tau_{s-1}(d)}{d} \cdot N^{s-1} + O_\Omega\left(\frac{\ln P_* + \sigma_{-1}(d)}{\sqrt{P_*}} \cdot N^{s-1} + \frac{\sigma_{-1}(d)}{d} \cdot P^* \cdot \hat{P} \cdot N^{s-2}\right),$$

где $\nu(\Omega)$ — постоянная из теоремы 1.1.

Доказательство. Пусть

$$\Theta = \left\{ X \in \mathrm{M}_{s-1,s}(\mathbb{R}) : \quad (x_{i1}, \ldots, x_{is}) \in V_i, \;\; i = \overline{1, s-1} \right\},$$
$$\Theta(\mathbf{P}) = \left\{ X \in \Theta : \quad P_i \le \mathcal{N}_i(X) < 2P_i, \;\; i = \overline{1, s-1} \right\}.$$

Для любой целочисленной матрицы $M \in \Theta$ определим

$$K(M, N) = \#\left\{ m \in \mathbb{Z}^s : \;\; \mathcal{M}(M, m) \in \Omega(\mathbb{Z}, N) \right\}.$$

Напомним, что $\mathcal{M}(M, m)$ — это матрица размера $s \times s$, полученная из M, к которой дописали m в качестве s-й строки, т.е.

$$\mathcal{M}(M, m) = \begin{pmatrix} m_{11} & \ldots & m_{1s} \\ \vdots & & \vdots \\ m_{(s-1)s} & \ldots & m_{(s-1)s} \\ m_1 & \ldots & m_s \end{pmatrix}$$

Тогда искомое число равно

$$\sum_{\substack{M \in \Theta(\mathbf{P}), \\ d(M) = d}} K(M, N).$$

Вычисление этой суммы проведем по следующей схеме.

1. Получим асимптотическую формулу для $K(M, N)$.
2. Вычислим $\sum K(M, N)$, используя лемму 3.3.

Сразу отметим, что

$$\forall X \in \Theta \qquad \mathcal{N}(X) \le C \cdot s \cdot D(X), \tag{4.5}$$

т.к. в противном случае нарушается условие (Б).

Для любого вещественного $R \ge 1$ определим функцию $f_R : \Theta \to \mathbb{R}_+$ по формуле:

$$f_R(X) = \frac{\mathrm{mes}_{\,s-1}(\pi_R(X) \cap V_s)}{\sqrt{A_1^2(X) + A_2^2(X) + \ldots + A_s^2(X)}},$$

где $\mathrm{mes}_{\,s-1}$ — $(s-1)$-мерная мера Лебега на плоскости $\pi_R(X) \subset \mathbb{R}^s$, состоящей из решений $(x_1, \ldots, x_s)$ уравнения

$$\sum_{j=1}^{s} A_j(X) \cdot x_j = R,$$

а $A_j(X) = (-1)^{s+j} D_j(X)$, $D_j(X)$ — определитель матрицы, полученной из X вычеркиванием j-го столбца. Справедливы следующие свойства функции f_R:

$$f_R(X) = R^{s-1} \cdot f_1(X), \tag{4.6}$$
$$f_1(\mathrm{Diag} \cdot X) = \frac{f_1(X)}{(\det \mathrm{Diag})^s}, \tag{4.7}$$
$$f_1 \in C^\infty(\overline{\Theta(P)}). \tag{4.8}$$

где $X \in \Theta$, $\mathrm{Diag} \in \mathrm{D}_{s-1}(\mathbb{R}_+)$. Для доказательства (4.6) достаточно заметить, что V_s — конус и сделать в интеграле

$$\mathrm{mes}_{\,s-1}(\pi_R(X) \cap V_s) = \int_{\pi_R(X)\cap V_s} dx$$

замену $x = R \cdot y$. Для доказательства (4.7) достаточно учесть, что $A_j(\mathrm{Diag} \cdot X) = \det \mathrm{Diag} \cdot A_j(X)$, поэтому $f_1(\mathrm{Diag} \cdot X) = f_R(X)/(\det \mathrm{Diag}\,)$, где $R = 1/(\det \mathrm{Diag}\,)$, и воспользоваться (4.6). Сооотношение (4.8) очевидно.

Возьмем любую целочисленную $M \in \Theta(\mathbf{P})$, у которой $d(M) = d$. Докажем, что

$$K(M,N) = d \cdot N^{s-1} \cdot f_1(M) + O\left(d \cdot N^{s-2} \cdot \frac{P^*}{\hat{P}^{s-1}}\right). \tag{4.9}$$

Здесь и далее в этом доказательстве постоянные в оценках $\ll$ и $O(\ldots)$ могут зависеть только от Ω. Для краткости, определим для любой $X \in \mathrm{M}_{t,s}(\mathbb{R})$

$$\mathcal{N}(X) = \prod_{i=1}^{t} \mathcal{N}_i(X).$$

Рассмотрим сначала случай, когда выполняются два дополнительные условия

$$\begin{gathered} \mathcal{N}(M) \le C \cdot s \cdot |A_s|; \\ \forall x \in V_s \quad |x|_\infty \le C \cdot s! \cdot |x_s|. \end{gathered} \tag{4.10}$$

Здесь и далее $A_j = A_j(M)$. Так как множество V_s связное и не содержит 0, то функция $x \in V_s \to x_s$ знакопостоянная. Не умаляя общности, будем считать, что $x_s > 0$ для всех $x \in V_s$.

Величина $K(M,N)$ равна количеству целочисленных точек в $V_s \cap \pi_N(M)$. Так как d делит N, то существует целочисленная точка $n \in \pi_N(M)$. Тогда

$$K(M,N) = \#(\mathbb{Z}^s \cap \pi_N(M) \cap V_s) = \#(V' \cap (\Gamma' + n')),$$

где $V' = V'(M,N)$ — проекция множества $V_s \cap \pi_N(M)$ на плоскость $\{x \in \mathbb{R}^s : x_s = 0\}$, $n' = (n_1, \ldots, n_{s-1})$, а Γ' — решетка, составленная из решений $(\gamma'_1, \ldots, \gamma'_{s-1}) \in \mathbb{Z}^{s-1}$ сравнения

$$A_1\gamma'_1 + \ldots + A_{s-1}\gamma'_{s-1} \equiv 0 \pmod{A_s}.$$

Как хорошо известно, $\det \Gamma' = |A_s|/d$. Поэтому, используя лемму 4.1, получаем

$$K(M,N) = d \cdot \frac{\mathrm{mes}\, V'}{|A_s|} + O_s\left(d \cdot \frac{\mathrm{mes}\, U(\partial V', \upsilon)}{|A_s|}\right), \tag{4.11}$$

где $\upsilon = \upsilon(\Gamma')$. Сразу отметим, что

$$\frac{\mathrm{mes}\, V'}{|A_s|} = f_N(M) = N^{s-1} \cdot f_1(M) \tag{4.12}$$

Осталось оценить остаточный член соотношения (4.11). Для этого сделаем замену

$$x'_i = \frac{x_i}{x_s}, \quad i = \overline{1, s-1}, \tag{4.13}$$

где

$$x_s = \frac{1}{A_s}\left(N - \sum_{j=1}^{s-1} A_j x_j\right).$$

Преобразование $(x_1, \dots, x_{s-1}) \to (x'_1, \dots, x'_{s-1})$ отображает V' на W_s, где W_s такое множество из $\mathbb{R}^{s-1}$, что

$$\{(x_1, \dots, x_{s-1}, 1) \in V_s\} = \{(x'_1, \dots, x'_{s-1}, 1) : (x'_1, \dots, x'_{s-1}) \in W_s\},$$

т.е. W_s — это проекция сечения конуса V_s плоскостью $\{x \in \mathbb{R}^s : x_s = 1\}$ на плоскость $\{x \in \mathbb{R}^s : x_s = 0\}$. Согласно (4.10) множество W_s является ограниченным.

Выясним, что является образом $U(\partial V', \upsilon)$ при отображении $x \to x'$.

Строки матрицы M образуют линейно-независимую систему из Γ'. Поэтому, согласно (4.1) и условию $M \in \Theta(\mathbf{P})$,

$$\upsilon \le C_0 \cdot \max_{1\le i\le s} \mathcal{N}_i(M) \le C_0 \cdot (2 \cdot P^*).$$

Возьмем любую точку $(y_1, \dots, y_{s-1}) \in U(\partial V', \upsilon)$. Тогда найдется такая точка $(x_1, \dots, x_{s-1}) \in \partial V'$, что

$$|x_i - y_i| \le \upsilon \le C_0 \cdot (2 \cdot P^*), \quad i = \overline{1, s-1}. \tag{4.14}$$

Так как $M \in \Theta(\mathbf{P})$, то

$$D(M) = \max_{1\le j\le s} |A_j| \le (s-1)! \prod_{i=1}^{s-1} \mathcal{N}_i(M) \le (s-1)! \cdot 2^{s-1} \cdot \hat{P}. \tag{4.15}$$

Определим

$$x_s = \frac{1}{A_s}\left(N - \sum_{j=1}^{s-1} A_j x_j\right), \quad y_s = \frac{1}{A_s}\left(N - \sum_{j=1}^{s-1} A_j y_j\right).$$

Тогда $(x_1, \dots, x_s) \in \pi_N(M)$ и, используя (4.10), (4.14), (4.15), (4.4), получаем

$$N \le s! \cdot \mathcal{N}(M) \cdot |x|_\infty \le s! \cdot (2^{s-1}\hat{P}) \cdot (C \cdot s \cdot x_s) \quad \Longrightarrow \quad x_s \ge \frac{N}{C \cdot s \cdot s! \cdot 2^{s-1} \cdot \hat{P}},$$

$$|x_s - y_s| \le \sum_{i=1}^{s-1} \frac{|A_i|}{|A_s|} \cdot |x_i - y_i| \le (s-1) \cdot \frac{(s-1)! \cdot \mathcal{N}(M)}{\mathcal{N}(M)/(C \cdot s)} \cdot \upsilon \le C \cdot s! \cdot (s-1) \cdot 2 \cdot C_0 \cdot P^*,$$

$$|y_s| \ge x_s - |x_s - y_s| \ge \frac{N}{C \cdot s \cdot s! \cdot 2^{s-1} \cdot \hat{P}} - C \cdot s! \cdot (s-1) \cdot 2 \cdot C_0 \cdot P^* \gg \frac{N}{\hat{P}},$$

$$\left|\frac{x_i}{x_s} - \frac{y_i}{y_s}\right| \le \frac{|x_i - y_i|}{|y_s|} + \frac{|x_s - y_s|}{x_s|y_s|} \cdot |x_i| \ll \frac{P^*\hat{P}}{N}.$$

Согласно последней оценке, преобразование переменных (4.13) переводит множество $U(\partial V', \upsilon)$ в $U(\partial W_s, \mu)$, где $\mu \ll P^*\hat{P}/N$. Кроме того,

$$dx_1 \cdot dx_{s-1} = N^{s-1} \cdot |A_s| \cdot \frac{dx'_1 \dots dx'_{s-1}}{|\det \mathcal{M}(M, x')|^s}, \tag{4.16}$$

$$\mathcal{M}(M, x') = \begin{pmatrix} m_{11} & \dots & m_{1(s-1)} & m_{1s} \\ \vdots & & \vdots & \vdots \\ m_{(s-1)1} & \dots & m_{(s-1)(s-1)} & m_{(s-1)s} \\ x'_1 & \dots & x'_{s-1} & 1 \end{pmatrix}.$$

Матрица $\mathcal{M}(M, x')$ принадлежит Ω (в силу условий (А)). Поэтому, согласно (Б),

$$|\det \mathcal{M}(M, x')| \geq \mathcal{N}(M)/C \gg \hat{P}.$$

Значит,

$$\operatorname{mes} U(\partial V', \upsilon) \leq \int_{U(\partial W_s, \mu)} N^{s-1} \cdot |A_s| \cdot \frac{dx'_1 \dots dx'_{s-1}}{|\det \mathcal{M}(M, x')|^s} \ll$$
$$\ll \frac{N^{s-1}}{\hat{P}^s} \cdot |A_s| \cdot \operatorname{mes} U(\partial W_s, \mu) \ll \frac{N^{s-1}}{\hat{P}^s} \cdot |A_s| \cdot \mu \ll \frac{N^{s-1}}{\hat{P}^s} |A_s| \cdot \frac{P^* \cdot \hat{P}}{N} = N^{s-2} \frac{P^*}{\hat{P}^{s-1}} \cdot |A_s|.$$

Подставляя последнюю оценку и равенство (4.12) в (4.11), получаем (4.9).

Формула (4.9) доказана при выполнении условий (4.10). Рассмотрим теперь общий случай. Согласно (Б),

$$\forall x \in V_s \quad |x|_\infty \cdot \mathcal{N}(M) \leq C \cdot \sum_{i=1}^{s} x_i \cdot A_i,$$

где $A_i = A_i(X)$. Поэтому

$$\forall x \in V_s \quad \exists l \in \{1, \dots, s\} : \qquad |x|_\infty \leq C \cdot s! \cdot |x_l|, \;\; \mathcal{N}(M) \leq C \cdot s \cdot |A_l|.$$

Значит, мы можем разбить множество V_s на не более, чем s конусов (зависящих только от Ω), каждый из которых, после изменения нумерации координат, удовлетворяет условиям (4.10). Соотношение (4.9) полностью доказано.

Используя (4.9), получаем

$$\sum_{\substack{M \in \Theta(\mathbf{P}), \\ d(M) = d}} K(M, N) = d \cdot N^{s-1} \cdot \sum_{\substack{M \in \Theta(\mathbf{P}), \\ d(M) = d}} f_1(M) + O\left(d \cdot N^{s-2} \cdot \frac{P^*}{\hat{P}^{s-1}} \cdot \sum_{\substack{M \in \Theta(\mathbf{P}), \\ d(M) = d}} 1 \right),$$

Согласно следствию 2.5,

$$\sum_{\substack{M \in \Theta(\mathbf{P}), \\ d(M) = d}} 1 \ll \hat{P}^s \cdot \frac{\sigma_{-1}(d)}{d^2}.$$

Значит,

$$\sum_{\substack{M \in \Theta(\mathbf{P}), \\ d(M) = d}} K(M, N) = d \cdot N^{s-1} \cdot \sum_{\substack{M \in \Theta(\mathbf{P}), \\ d(M) = d}} f_1(M) + O\left(\frac{\sigma_{-1}(d)}{d} \cdot P^* \cdot \hat{P} \cdot N^{s-2} \right). \qquad (4.17)$$

Согласно (А), (Б), (4.6), (4.7), (4.8), (4.5), множество $\Theta_t = \Theta$ и функция $f = f_1$ удовлетворяет условиям леммы 3.3. Применяя ее, получаем следующую асимптотическую формулу для $\sum f_1(M)$:

$$d \sum_{\substack{M \in \Theta(\mathbf{P}), \\ d(M) = d}} f_1(M) = \frac{\tau_{s-1(d)}}{d^{s-t}} \cdot \frac{1}{\zeta(2) \cdot \ldots \cdot \zeta(s)} \cdot \int_{\Theta(\mathbf{P})} f_1(X)\, dX + O\left(\frac{\ln P_* + \sigma_{-1}(d)}{\sqrt{P_*}} \cdot N^{s-1} \right). \qquad (4.18)$$

Осталось доказать, что

$$\int_{\Theta(\mathbf{P})} f_1(X)\,dX = (\ln 2)^{s-1}\cdot\mu(\mathcal{P}(\Omega)). \tag{4.19}$$

Рассмотрим случай, когда существуют номера $k_1,\ldots,k_s\in\{1,\ldots,s\}$ такие, что

$$\forall X\in\Omega\quad \mathcal{N}_i(X)=|x_{ik_i}|,\ \ i=\overline{1,s}. \tag{4.20}$$

Пусть, например,

$$k_1=k_2=\ldots=k_s=s.$$

Так как множество Ω связное, то функции $X\in\Omega\to x_{is}$ знакопостоянные. Пусть $x_{is}>0$, $i=\overline{1,s}$. Тогда каждое V_i можно представить в виде:

$$V_i=\{t(x'_1,\ldots,x'_{s-1},1):\quad (x'_1,\ldots,x'_{s-1})\in W_i,\ \ t\in\mathbb{R}_+\}$$

где W_i — некоторое ограниченное множество из $\mathbb{R}^{s-1}$. Согласно (4.12),

$$f_1(X)=\frac{1}{|A_s|N^{s-1}}\int_{V'}dx.$$

Сделаем в этом интеграле замену переменных (4.13). Учитывая (4.16), получаем

$$f_1(X)=\int_{W_s}\frac{dx'_1\ldots dx'_{s-1}}{|\det\mathcal{M}(X,x')|^s},\quad \mathcal{M}(X,x')=\begin{pmatrix} x_{11} & \ldots & x_{1(s-1)} & x_{1s}\\ \vdots & & \vdots & \vdots\\ x_{(s-1)1} & \ldots & x_{(s-1)(s-1)} & x_{(s-1)s}\\ x'_1 & \ldots & x'_{s-1} & 1\end{pmatrix}.$$

Теперь в интеграле

$$\int_{\Theta(\mathbf{P})} f_1(X)\,dX$$

сделаем замену

$$x_{is}=t_i,\quad x_{ij}=t_i\cdot x_{ij'},\ \ i,j=\overline{1,s-1}.$$

Тогда

$$\prod_{\substack{1\le i\le s-1,\\ 1\le j\le s}} dx_{ij}=\left(\prod_{l=1}^{s-1}t_l^{s-1}\,dt_l\right)\cdot\prod_{i,j=1}^{s}dx'_{ij},$$

$$f_1(X)=\frac{1}{t_1^s\cdot\ldots\cdot t_{s-1}^s}\int_{W_s}\frac{dx'_1\ldots dx'_{s-1}}{|\det X'|^s},\quad X'=\begin{pmatrix} x'_{11} & \ldots & x'_{1(s-1)} & 1\\ \vdots & & \vdots & \vdots\\ x'_1 & \ldots & x'_{s-1} & 1\end{pmatrix}.$$

$$\int_{\Theta(\mathbf{P})} f_1(X)\,dX=\left(\prod_{l=1}^{s-1}\int_{P_l}^{2P_l}\frac{dt_l}{t_l}\right)\cdot\int_{W_1\times\ldots\times W_s}\frac{dX'}{|\det X'|^s}=\ln^{s-2}2\cdot\mu(\mathcal{P}(\Omega)).$$

Формула (4.19) доказана при выполнении условий (4.20) с $k_i=s$. Для других вариантов выбора k_i доказательство проводится точно таким же образом. В общем случае множество Ω достаточно разбить на фиксированное число попарно непересекающихся частей, каждая из которых удовлетворяет (А), (Б), (4.20). Соотношение (4.19) полностью доказано.

Подставляя (4.19) в (4.18), а (4.18) в (4.17), получаем утверждение леммы. □

Лемма 4.3. *Для любого натурального N имеет место оценка*

$$\sum_{d|N} \frac{\sigma_{-1}(d)}{d} \cdot \ln d \le c \cdot \sigma_{-1}(N) \cdot \chi(N) \qquad (c = 4 \cdot \zeta(2)). \tag{4.21}$$

Доказательство. Пусть $\Lambda(r)$ — функция Мангольдта, т.е.

$$\Lambda(r) = \begin{cases} \ln p, & \text{если } r = p^\alpha, \ \ p \text{ — простое,} \\ 0, & \text{в противном случае.} \end{cases}$$

Используя формулу $\ln d = \sum_{r|d} \Lambda(r)$, получаем

$$\begin{aligned} \sum_{d|N} \frac{\sigma_{-1}(d)}{d} \cdot \ln d &= \sum_{r|N} \Lambda(r) \sum_{\substack{d|N, \\ d \equiv 0 \pmod r}} \frac{\sigma_{-1}(d)}{d} = \\ &= \sum_{r|N} \Lambda(r) \sum_{d'r|N} \frac{\sigma_{-1}(d'r)}{d'r} \le \sum_{r|N} \frac{\Lambda(r) \cdot \sigma_{-1}(r)}{r} \cdot \sum_{d|N} \frac{\sigma_{-1}(d)}{d}. \end{aligned}$$

Для завершения доказательства осталось заметить, что

$$\begin{aligned} &\sum_{d|N} \frac{\sigma_{-1}(d)}{d} = \sum_{r \cdot r'|N} \frac{1}{r^2 r'} \le \zeta(2) \cdot \sigma_{-1}(N), \\ &\sum_{r|N} \frac{\Lambda(r) \cdot \sigma_{-1}(r)}{r} \le \sum_{r|N} \frac{\Lambda(r) \cdot 2}{r} \le 4 \sum_{p|N} \frac{\ln p}{p} = 4(\chi(N) - 1). \end{aligned}$$

В последней сумме p — простые делители N. □

Замечание 4.1. Для любого натурального $L \ge s - 1$ имеют место соотношения

$$\begin{aligned} &\#\{k' \in \mathbb{N}^{s-1} : |k'|_\infty + |k'|_1 \le L\} = \#\{k \in \mathbb{N}^s : \ \ |k|_1 = L, \ |k|_\infty = k_s\} = \\ &= \frac{1}{s} \#\{k \in \mathbb{N}^s : \ \ |k|_1 = L\} + O_s(L^{s-2}) = \frac{L^{s-1}}{s!} + O_s(L^{s-2}). \end{aligned}$$

Доказательство теоремы 1.1. Для любого $l \in \{1, \dots, s\}$ определим

$$\Omega_l = \left\{ X \in \Omega : \quad \mathcal{N}_l(X) = \max_{1 \le i \le s} \mathcal{N}_i(X) \right\}.$$

Согласно следствию 2.3, количество матриц $M \in \Omega(\mathbb{Z}; N)$ с $\mathcal{N}_l(M) = \mathcal{N}_m(M)$ $(l \ne m)$, не больше, чем $O(\mathcal{R}_s(N) \cdot \ln^{s-2} N)$. Здесь и далее в этом доказательстве постоянные в оценках $\ll$ и $O(\dots)$ могут зависеть только от Ω. Поэтому

$$\#\Omega(\mathbb{Z}; N) = \sum_{l=1}^{s} \Omega_l(\mathbb{Z}; N) + O(\mathcal{R}_s(N) \cdot \ln^{s-2} N). \tag{4.22}$$

Осталось доказать, что для любого l

$$\#\Omega_l(\mathbb{Z}; N) = \mathcal{R}_s(N) \cdot \left(\nu(\Omega) \cdot \frac{\ln^{s-1} N}{s!} + O(\chi(N) \cdot \ln^{s-2} N) \right). \tag{4.23}$$

Не умаляя общности рассмотрим случай $l = s$. Пусть $C_1 = \max\{C_*, s!\}$, где C_* — постоянная из леммы 4.2. Определим множества

$$K(N) = \left\{k \in \mathbb{N}^{s-1} : |k|_\infty + |k|_1 \le \log_2(N/C_1)\right\},$$
$$\omega_k(N) = \left\{M \in \Omega(\mathbb{Z}; N) : \quad 2^{k_i-1} \le \mathcal{N}_i(M) < 2^{k_i},\ i = \overline{1, s-1}\right\}, \quad k \in K(N),$$
$$\omega(N) = \bigcup_{k \in K(N)} \omega_k(N).$$

Сразу отметим следующие свойства.

1. Если $k \in K(N)$, то параметры $P_i = 2^{k_i-1}$ удовлетворяют условиям леммы 4.2. Поэтому мы можем использовать лемму 4.2 для вычисления количества целочисленных матриц $M \in \omega_k(N)$, удовлетворяющих условию $d_{s-1}(M) = d$.

2. Если $M \in \Omega(\mathbb{Z}; N)$, но $M \notin \omega(N)$, то

$$\left(\max_{1 \le j \le s-1} \mathcal{N}_j(M)\right) \cdot \prod_{i=1}^{s-1} \mathcal{N}_i(M) \gg N. \tag{4.24}$$

   Для доказательства достаточно определить натуральные $k_1, \ldots, k_{s-1}$ из условий $2^{k_i-1} \le \mathcal{N}_i(M) < 2^{k_i}$ и учесть, что $|k|_\infty + |k|_1 > \log_2(N/C_1)$.

3. Согласно (Б) и определению детерминанта матрицы,

$$\forall M \in \Omega(\mathbb{Z}; N) \qquad \frac{1}{C} \prod_{i=1}^{s} \mathcal{N}_i(M) \le N \le s! \cdot \prod_{i=1}^{s} \mathcal{N}_i(M). \tag{4.25}$$

Перейдем к вычислению $\#\Omega_s(\mathbb{Z}; N)$. Докажем сначала, что

$$\omega(N) \subset \Omega_s(\mathbb{Z}; N). \tag{4.26}$$

Возьмем любую $M \in \omega(N)$. Тогда $M \in \omega_k(N)$ с некоторым $k \in K(N)$. Согласно (4.25),

$$\left(\max_{1 \le j \le s-1} \mathcal{N}_j(M)\right) \cdot \prod_{i=1}^{s-1} \mathcal{N}_i(M) \le 2^{|k|_\infty + |k|_1} \le \frac{N}{C_1} \le \frac{s!}{C_1} \cdot \prod_{i=1}^{s} \mathcal{N}_i(M) \le \prod_{i=1}^{s} \mathcal{N}_i(M).$$

Значит, $\max_{1 \le j \le s-1} \mathcal{N}_j(M) \le \mathcal{N}_s(M)$, т.е. $M \in \Omega_s(\mathbb{Z}; N)$. Соотношение (4.26) доказано.

Оценим теперь мощность множества $\Omega_s(\mathbb{Z}; N) \backslash \omega(N)$. Возьмем любую $M \in \Omega_s(\mathbb{Z}; N)$ такую, что $M \notin \omega(N)$. Так как $M \in \Omega_s(\mathbb{Z}; N)$, то

$$\max_{1 \le j \le s-1} \mathcal{N}_j(M) \le \mathcal{N}_s(M).$$

и, используя (4.24), (4.25), получаем

$$\left(\max_{1 \le j \le s-1} \mathcal{N}_j(M)\right) \cdot \prod_{i=1}^{s-1} \mathcal{N}_i(M) \gg \prod_{i=1}^{s} \mathcal{N}_i(M) \implies \max_{1 \le j \le s-1} \mathcal{N}_j(M) \gg \mathcal{N}_s(M).$$

Значит, $\max_{1\le j\le s-1}\mathcal{N}_j(M)\asymp\mathcal{N}_s(M)$. Согласно следствию 2.3, количество таких матриц оценивается величиной $O(\mathcal{R}_s(N)\cdot\ln^{s-2}N)$. Учитывая (4.26), приходим к оценке

$$\#\Omega_s(\mathbb{Z};N)=\#\omega(N)+O(\mathcal{R}_s(N)\cdot\ln^{s-2}N). \tag{4.27}$$

Осталось вычислить $\#\omega(N)$.

Возьмем натуральное d. Разобьем $K(N)$ на две непересекающиеся части:

$$K'(N,d)=\{k\in K(N):k_*\ge 2\log_2 d\},\qquad K''(N,d)=\{k\in K(N):k_*<2\log_2 d\}$$

Здесь и далее

$$k_*=\min_{1\le i\le s-1}k_i.$$

Положим

$$\omega_{k,d}(N)=\{M\in\omega_k(N):d_{s-1}(M)=d\}.$$

Сразу отметим, что

$$\#K(N)=\frac{\log_2^{s-1}N}{s!}+O\left(\ln^{s-2}N\right)\quad(\text{по замечанию 4.1, } L=\log_2(N/C_1)),$$

$$\#K''(N,d)\ll(\ln N)^{s-2}\cdot\ln(2d), \tag{4.28}$$

$$\#K'(N,d)=\#K(N)-\#K''(N,d)=\frac{\log_2^{s-1}N}{s!}+O\left((\ln N)^{s-2}\cdot\ln 2d\right). \tag{4.29}$$

Так как $\#\omega_k(N)=\sum_{d|N}\#\omega_k(N,d)$, то

$$\#\omega(N)=\sum_{d|N}\sum_{k\in K(N)}\#\omega_{k,d}(N)=\sum_{d|N}\Big(S'(N,d)+S''(N,d)\Big), \tag{4.30}$$

где

$$S'(N,d)=\sum_{k\in K'(N,d)}\#\omega_{k,d}(N),\quad S''(N,d)=\sum_{k\in K''(N,d)}\#\omega_{k,d}(N).$$

Согласно следствию 2.4, $\#\omega_{k,d}(N)\ll N^{s-1}\cdot\sigma_{-1}(d)\cdot d^{-1}$. Учитывая (4.28), получаем

$$S''(N,d)\ll N^{s-1}\frac{\sigma_{-1}(d)}{d}\sum_{k\in K''(N,d)}1\ll N^{s-1}\cdot\frac{\sigma_{-1}(d)}{d}\cdot(\ln N)^{s-2}\cdot\ln d. \tag{4.31}$$

Вычислим $S'(N,d)$. Согласно лемме 4.2 (в которой $P_i=2^{k_i-1}$),

$$\begin{aligned}\#\omega_{k,d}(N) &= \ln^{s-1}2\cdot\nu(\Omega)\cdot\frac{\tau_{s-1}(d)}{d}\cdot N^{s-1}+\\ &\quad+O_\Omega\left(\frac{k_*+\sigma_{-1}(d)}{2^{k_*/2}}\cdot N^{s-1}+\frac{\sigma_{-1}(d)}{d}\cdot 2^{|k|_\infty}\cdot 2^{|k|_1}\cdot N^{s-2}\right).\end{aligned}$$

Следовательно,

$$\begin{aligned}\sum_{k\in K'(N,d)}\#\omega_{k,d} &= N^{s-1}\cdot\frac{\tau_{s-1}(d)}{d}\cdot\ln^{s-1}2\cdot\nu(\Omega)\cdot\#K'(N,d)+R(N,d),\\ R(N,d) &\ll \sum_{k\in K'(N,d)}\left(\frac{k_*+\sigma_{-1}(d)}{2^{k_*/2}}\cdot N^{s-1}+\frac{\sigma_{-1}(d)}{d}\cdot 2^{|k|_\infty+|k_1|}N^{s-2}\right)\ll\\ &\ll \frac{\log_2(2d)+\sigma_{-1}(d)}{2^{\log_2 d}}\cdot N^{s-1}\cdot\ln^{s-2}N+\frac{\sigma_{-1}(d)}{d}\cdot N^{s-1}\cdot\ln^{s-2}N\ll\\ &\ll \frac{\ln(2d)}{d}\cdot N^{s-1}\cdot\ln^{s-2}N.\end{aligned}$$

Используя (4.29), заключаем

$$S'(N,d)=\sum_{k\in K'(N,d)}\#\omega_{k,d}(N)=N^{s-1}\frac{\tau_{s-1}(d)}{d}\frac{\ln^{s-1}N}{s!}\cdot\nu(\Omega)+O\left(N^{s-1}\cdot\frac{\ln(2d)}{d}\cdot\ln^{s-2}N\right).$$

Подставим последнее соотношение и (4.31) в (4.30). Используя (2.3) для суммирования главного члена и (2.4), (4.21) для оценки остатка, получаем формулу

$$\#\omega(N)=\mathcal{R}_s(N)\cdot\left(\nu(\Omega)\cdot\frac{\ln^{s-1}N}{s!}+O(\chi(N)\cdot\ln^{s-2}N)\right).$$

Подставляя ее в (4.27), приходим к (4.23) (при $s=l$). Из (4.23) и (4.27) вытекает утверждение теоремы 1.1. □

Глава III
Среднее количество относительных минимумов

Напомним, что $\mathfrak{M}(\Gamma)$ — множество относительных минимумов решетки Γ, а

$$E(N,s) = \frac{1}{\mathcal{R}_s(N)} \cdot \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z};N)} \#\mathfrak{M}(\Gamma)$$

— среднее число относительных минимумов полных целочисленных s-мерных решеток определителя N. Здесь и далее $N \in \mathbb{N}$, $N > 1$.

Целью настоящей главы является доказательство асимптотической формулы

$$E(N,s) = \mathcal{C}(s) \cdot \ln^{s-1} N + O_s\left(\chi(N) \cdot \ln^{s-2} N\right),$$

где $\mathcal{C}(s)$ — положительная постоянная, зависящая только от размерности, а

$$\chi(N) = 1 + \sum_{p|N} \frac{\ln p}{p} \quad \text{(сумма по простым делителям } N\text{)}.$$

При вычислении $E(N,s)$ можно пренебречь минимумами, имеющими хотя бы одну нулевую координату (их количество оценивается остаточным членом). Поэтому, в силу симметрии, достаточно рассмотреть минимумы с положительными координатами.

Пусть множество $\mathcal{U}_s$ состоит из пар (Γ, a), где $\Gamma \in \mathcal{L}_s(\mathbb{R})$ и a — относительный минимум Γ с положительными координатами. Определим также

$$\mathcal{U}_s(N) = \{(\Gamma, a) \in \mathcal{U}_s : \quad \Gamma \in \mathcal{L}_s(\mathbb{Z}, N)\}.$$

Тогда

$$\sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z};N)} \#(\mathbb{R}^s_+ \cap \mathfrak{M}(\Gamma)) = \#\mathcal{U}_s(N).$$

Из оценки (I.3.12) вытекает, что у любой решетки $\Gamma \in \mathcal{L}_s(\mathbb{Z}, N)$ количество относительных минимумов, имеющих хотя бы одну нулевую координату, оценивается величиной $O_s(\ln^{s-2} N)$. Поэтому (в силу симметрии)

$$E(N,s) = \frac{2^s}{\mathcal{R}_s(N)} \cdot \#\mathcal{U}_s(N) + O_s\left(\ln^{s-2} N\right). \tag{0.1}$$

Вычисление $\#\mathcal{U}_s(N)$ будет проводиться следующим образом. Мы построим отображение Φ, которое каждой паре $(\Gamma, a) \in \mathcal{U}_s$ ставит в соответствие базисную матрицу решетки Γ. Причем, если $\Omega_{\mathfrak{M},s}$ состоит из базисных матриц, полученных таким способом (т.е. $\Omega_{\mathfrak{M},s}$ — образ Φ), а $\Omega'_{\mathfrak{M},s}$ — внутренность $\Omega_{\mathfrak{M},s}$, то Φ взаимно однозначно переводит некоторое подмножество $\mathcal{U}'_s \subset \mathcal{U}_s$ на $\Omega'_{\mathfrak{M},s}$. Поэтому

$$\#\Omega'_{\mathfrak{M},s}(\mathbb{Z}, N) = \#\mathcal{U}'_s(N) \leq \#\mathcal{U}_s(N) \leq \#\Omega_{\mathfrak{M},s}(\mathbb{Z}, N).$$

Здесь и далее, если $\Omega \subset \mathrm{GL}_s(\mathbb{R})$, то $\Omega(\mathbb{Z}; N)$ — множество целочисленных матриц из Ω определителя N. Следовательно,

$$\#\mathcal{U}_s(N) = \#\Omega_{\mathfrak{M},s}(\mathbb{Z}, N) + O\left(\#(\partial\Omega_{\mathfrak{M},s}(\mathbb{Z}, N))\right),$$

где $\partial\Omega_{\mathfrak{M},s}$ — граница $\Omega_{\mathfrak{M},s}$. Для вычисления $\#\Omega_{\mathfrak{M},s}(\mathbb{Z}, N)$ и оценки $\#\partial\Omega_{\mathfrak{M},s}(\mathbb{Z}, N)$ будем использовать теорему 1.1.

Чтобы проиллюстрировать идею доказательства мы сначала рассмотрим случай $s = 2$. В § 2 мы выведем требуемую формулу при $s = 3$ и в § 3 — для случая произвольного s. К сожалению, постоянная $\mathcal{C}(s)$ не выражается через известные при $s \geq 3$. В § 4 доказываются оценки

$$\frac{1}{(s-1)!} \leq \mathcal{C}(s) \leq \frac{2^s}{(s-1)!},$$

позволяющие судить о поведении $\mathcal{C}(s)$ при $s \to +\infty$.

Отметим, что используемый в § 2 метод дополнения минимума до базиса не обобщается на случай $s \geq 4$. Однако он позволяет получить более наглядное описание константы $\mathcal{C}(3)$, чем то, которое вытекает из результатов § 3.

§ 1. Двумерный случай

Этот раздел содержит известные результаты и приводится для полноты изложения.

Определение 1.1. Пусть $\Gamma \in \mathcal{L}_s(\mathbb{R})$. Множество $\{a^{(1)}, \ldots, a^{(s)}\} \subset \mathfrak{M}(\Gamma)$ будем называть *минимальной системой*, если не существует ненулевого $\gamma \in \Gamma$ такого, что

$$|\gamma_i| < \max\left\{|a_i^{(1)}|, \ldots, |a_i^{(s)}|\right\}, \quad i = \overline{1, s}.$$

Минимальную систему, образующую базис, называем *минимальным базисом*.

Минимальные системы впервые были изучены в работах Г.Ф. Вороного [20] и Г. Минковского [124] (см., также [126]) в связи с методами построения единиц в числовых полях. Ими были исследованы различные свойства минимальных систем двух и трехмерных решеток общего положения (в трехмерном случае без доказательства). Доказательство, обсуждение и переизложение оригинальных результатов см. в [18, 95, 97, 130] Некоторые свойства минимальных систем произвольных решеток изучены в [26, 72].

Мы будем использовать базисы, которые являются «почти» минимальными.

Возьмем любую пару $(\Gamma, a) \in \mathcal{U}_2$. Выберем узел $b = (\pm b_1, b_2) \in \Gamma$ из следующих условий

$$\begin{array}{l} \{a, b\} \text{ — базис } \Gamma, \\ 0 \le b_1 \le a_1, \\ 0 \le b_2 \to \min. \end{array} \tag{1.1}$$

Справедливы следующие очевидные свойства.

1. $a_2 \le b_2$ (т.к. $a \in \mathfrak{M}(\Gamma)$).

2. $b = (-b_1, b_2)$, $b_1 > 0$ (иначе $(b - a)$ противоречит выбору b).

Таким образом каждой паре $(\Gamma, a) \in \mathcal{U}_2$ поставлена в соответствие (возможно не единственная) базисная матрица $M = \begin{pmatrix} a_1 & -b_1 \\ a_2 & b_2 \end{pmatrix} \in \Omega$, где

$$\Omega = \left\{ \begin{pmatrix} x_1 & -y_1 \\ x_2 & y_2 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) : \quad 0 < y_1 \le x_1, \quad 0 < x_2 \le y_2 \right\}.$$

Очевидно, что разным парам из $\mathcal{U}_2$ соответствуют разные матрицы из Ω. Кроме того, если $(\Gamma, a) \in \mathcal{U}_2(N)$, то $M \in \mathrm{M}_2(\mathbb{Z}, N)$. Значит, справедлива оценка

$$\#\mathcal{U}_2(N) \le \#\Omega(\mathbb{Z}, N). \tag{1.2}$$

Пусть Ω' — внутренность Ω. Возьмем любую матрицу $M = \begin{pmatrix} a_1 & -b_1 \\ a_2 & b_2 \end{pmatrix} \in \Omega'$. Тогда $0 < b_1 < a_1$, $0 < a_2 < b_2$. Пусть $\Gamma = \Gamma(a, b)$ — решетка, порожденная a, b. Нетрудно проверить, что $a \in \mathfrak{M}(\Gamma)$, а b является единственным узлом, удовлетворяющим (1.1). То есть существует взаимно однозначное соответствие между Ω' и некоторым подмножеством $\mathcal{U}_2$. Значит, $\#\Omega'(\mathbb{Z}, N) \le \#\mathcal{U}_2(N)$ и учитывая (1.2), получаем

$$\#\mathcal{U}_2(N) = \#\Omega(\mathbb{Z}, N) + O(\#\partial\Omega(\mathbb{Z}, N)), \tag{1.3}$$

где $\partial\Omega$ — граница Ω.

Множество Ω удовлетворяет условиям теоремы 1.1, согласно которой

$$\begin{array}{l} \#\Omega(\mathbb{Z}, N) = \mathcal{R}_2(N) \cdot \left(\dfrac{\mu(\mathcal{P}(\Omega))}{\zeta(2)} + O_\Omega(\chi(N)) \right), \\ \#\partial\Omega(\mathbb{Z}, N) = O_\Omega(\mathcal{R}_2(N) \cdot \chi(N)). \end{array} \tag{1.4}$$

Нетрудно вычислить, что

$$\mu(\mathcal{P}(\Omega)) = \int_0^1 \int_0^1 \frac{dxdy}{(1 + xy)^2} = \ln 2.$$

Поэтому из (0.1), (1.3), (1.4) следует асимптотическая формула

$$E(N, 2) = \mathcal{C}(2) \cdot \ln N + O(\chi(N)), \quad \mathcal{C}(2) = \frac{4 \cdot \ln 2}{\zeta(2)}.$$

§ 2. Трехмерный случай

Содержание этого раздела излагается по следующему плану:

1) доказываем, что любой относительный минимум трехмерной решетки можно дополнить до базиса специального вида (лемма 2.2);

2) доказываем, что «почти всегда» это дополнение является единственным (следствие 2.1);

3) доказываем асимптотическую формулу (0.1) при $s = 3$ (теорема 2.1) .

Замечание 2.1. Пусть $\Gamma \in \mathcal{L}_s(\mathbb{R})$. По теореме Минковского о линейных формах для любых $\epsilon > 0$ и $k \in \{1, \dots, s\}$ существует такой узел $\gamma \in \Gamma \setminus \{0\}$, что $|\gamma_i| \le \epsilon$ при $i \ne k$.

Возьмем любую пару $(\Gamma, a) \in \mathcal{U}_3$. Дополним узел a до базиса решетки Γ узлами b, c следующим образом.

Согласно замечанию 2.1, найдется такой ненулевой узел $b \in \Gamma$, что $|b_i| < a_i$, $i = 1, 3$. Выберем узел $b = (\pm b_1, b_2, \pm b_3)$ из условий

$$\begin{array}{l} b \in \Gamma \setminus \{0, \pm a\}, \\ 0 \le b_i \le a_i, \quad i = 1, 3, \\ 0 \le b_2 \to \min . \end{array} \tag{2.1}$$

Тогда $a_2 \le b_2$ (иначе $a \notin \mathfrak{M}(\Gamma)$). Следовательно, a, b линейно независимые. Кроме того, хотя бы одна из координат b отрицательная (иначе $(b-a)$ противоречит выбору b). Значит, возможны следующие три варианта комбинации знаков у координат b:

$$b = (-b_1, b_2, -b_3), \quad b_1, b_2, b_3 > 0; \tag{2.2}$$

$$b = (-b_1, b_2, b_3), \quad b_1, b_2 > 0, \quad b_3 \ge 0; \tag{2.3}$$

$$b = (b_1, b_2, -b_3), \quad b_2, b_3 > 0, \quad b_1 \ge 0; \tag{2.4}$$

В силу симметрии будем рассматривать только первый и второй случай.

Лемма 2.1. *Пусть b удовлетворяет (2.1), причем b имеет вид (2.2) или (2.3). Тогда существует узел $c = (c_1, c_2, c_3) \in \Gamma$ такой, что $\{a, b, c\}$ — базис Γ и $|c_1| \le a_1$, $|c_2| < b_2$.*

Доказательство. Из выбора b и условия $a \in \mathfrak{M}(\Gamma)$ вытекает, что треугольник с вершинами в точках $0, a, b$ не содержит ненулевых узлов Γ, кроме a и b. Значит, a, b можно дополнить до базиса некоторым узлом c. Далее, c всегда можно выбрать так, что $|c_1| \le a_1$. Пусть вторая координата вектора c неотрицательная и наименьшая среди всех возможных, т.е. $0 \le c_2 \le |c_2'|$ для любого c', удовлетворяющего условиям: $\{a, b, c'\}$ — базис Γ, $|c_1'| \le a_1$. Предположим, что $c_2 \ge b_2$. Тогда, рассматривая узлы

$$\begin{array}{l} (c - b) \text{ при } c_1 \le 0, \\ (c - a) \text{ при } c_1 \ge 0, \end{array}$$

получаем противоречие с выбором c. Значит, $c_2 < b_2$. □

Пусть b удовлетворяет (2.2) либо (2.3). Согласно лемме 2.1, существует (возможно не единственный) узел $c = (\pm c_1, \pm c_2, c_3)$ такой, что

$$\begin{array}{l} \{a, b, c\} \text{ — базис } \Gamma; \\ 0 \le c_1 \le a_1, \;\; 0 \le c_2 < b_2; \\ 0 \le c_3 \to \min. \end{array} \tag{2.5}$$

Исследуем свойства базиса $\{a, b, c\}$. Определим следующие множества:

$$\begin{aligned} \Omega_1 &= \left\{ \begin{pmatrix} a_1 & -b_1 & -c_1 \\ a_2 & b_2 & -c_2 \\ a_3 & -b_3 & c_3 \end{pmatrix} : \quad a_1 < b_1 + c_1, \right\}, \\ \Omega_2 &= \left\{ \begin{pmatrix} a_1 & -b_1 & -c_1 \\ a_2 & b_2 & c_2 \\ a_3 & -b_3 & c_3 \end{pmatrix} : \begin{array}{c} c_1 \ge b_1 \\ \text{либо} \\ a_2 \ge c_2 \end{array} \right\}, \\ \Omega_3 &= \left\{ \begin{pmatrix} a_1 & -b_1 & -c_1 \\ a_2 & b_2 & -c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} \right\}, \\ \Omega_4 &= \left\{ \begin{pmatrix} a_1 & -b_1 & c_1 \\ a_2 & b_2 & -c_2 \\ a_3 & b_3 & c_3 \end{pmatrix} : \begin{array}{c} b_1 \ge c_1 \\ b_2 \le a_2 + c_2 \end{array} \right\}, \end{aligned}$$

где a_1, b_2, c_3 — положительные, а остальные a_i, b_i, c_i — неотрицательные вещественные, причем

$$a_1 \ge \max\{b_1, c_1\}, \quad b_2 \ge \max\{a_2, c_2\}, \quad c_3 > a_3 \ge b_3,$$

Лемма 2.2. *Возьмем любой узел b, удовлетворяющий (2.1). Пусть выполняются (2.2) или (2.3). Тогда существует c, удовлетворяющий (2.5), причем*

$$M \in \begin{cases} \Omega_1 \cup \Omega_2, & \text{если } b \text{ имеет вид (2.2)}, \\ \Omega_3 \cup \Omega_4, & \text{если } b \text{ имеет вид (2.3)}. \end{cases}$$

где $M = M(a, b, c)$ — матрица со столбцами a, b, c.

Доказательство. Пусть c — *любой* узел, удовлетворяющий (2.5). Как уже отмечалось ранее $b_2 \ge a_2$. Кроме того, $a_3 < c_3$ (иначе c противоречит выбору b) и хотя бы одна координата c отрицательная (иначе $(c - a)$ противоречит выбору c). Таким образом, достаточно рассмотреть следующие случаи:

1.1.	$b = (-b_1, b_2, -b_3)$,	$c = (-c_1, -c_2, c_3)$,	$b_1, b_3 > 0$,	$c_1, c_2 > 0$.
1.2.	$b = (-b_1, b_2, -b_3)$,	$c = (c_1, -c_2, c_3)$,	$b_1, b_3 > 0$,	$c_2 > 0$.
1.3.	$b = (-b_1, b_2, -b_3)$,	$c = (-c_1, c_2, c_3)$,	$b_1, b_3 > 0$,	$c_1 > 0$.
2.1.	$b = (-b_1, b_2, b_3)$,	$c = (-c_1, -c_2, c_3)$.	$b_1 > 0$,	$c_1, c_2 > 0$.
2.2.	$b = (-b_1, b_2, b_3)$,	$c = (c_1, -c_2, c_3)$,	$b_1 > 0$,	$c_2 > 0$.
2.3.	$b = (-b_1, b_2, b_3)$,	$c = (-c_1, c_2, c_3)$,	$b_1 > 0$,	$c_1 > 0$.

Здесь и ниже b_i, c_i — неотрицательные вещественные, причем $b_2, c_3 > 0$.

1.1. Пусть

$$M = \begin{pmatrix} a_1 & -b_1 & -c_1 \\ a_2 & b_2 & -c_2 \\ a_3 & -b_3 & c_3 \end{pmatrix}, \quad c_2, b_3 > 0.$$

Если $b_1 + c_1 \le a_1$, то узел $c' = (b + c)$ удовлетворяет условиям:

$$|c'_1| = b_1 + c_1 \le a_1, \quad |c'_2| = b_2 - c_2 < b_2, \quad c'_3 = c_3 - b_3 < c_3.$$

Это противоречит выбору c. Значит $b_1 + c_1 > a_1$ и $M \in \Omega_1$.

1.2. Пусть $b = (-b_1, b_2, -b_3)$, $c = (c_1, -c_2, c_3)$, причем $b_3, c_2 > 0$. Тогда узел $(b + c)$ противоречит выбору c, т.е. этот случай невозможен.

1.3. Пусть

$$M = \begin{pmatrix} a_1 & -b_1 & -c_1 \\ a_2 & b_2 & c_2 \\ a_3 & -b_3 & c_3 \end{pmatrix}, \quad b_1, b_3, c_1 > 0.$$

Если $a_2 \ge c_2$ либо $c_1 \ge b_1$, то $M \in \Omega_2$. Пусть

$$a_2 < c_2, \quad c_1 < b_1.$$

Рассмотрим узел $c' = (c'_1, c'_2, c'_3) = c - b - a$. Имеем

$$\begin{aligned} c'_1 &= -(a_1 + c_1 - b_1), \quad |c'_1| < a_1, \\ c_2 &= -(b_2 + a_2 - c_2), \quad |c'_2| < b_2, \\ c'_3 &= +(c_3 + b_3 - a_3), \quad |c'_3| \le c_3. \end{aligned}$$

Значит, $c'_3 = c_3$, т.е. $b_3 = a_3$. Тогда узел c' также удовлетворяет (2.5) и $M(a, b, c') \in \partial\Omega_1$.

2.1. В этом случае $M \in \Omega_3$.

2.2. Пусть

$$M = \begin{pmatrix} a_1 & -b_1 & c_1 \\ a_2 & b_2 & -c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}, \quad b_1, c_2 > 0.$$

Если $b_2 > a_2 + c_2$, то узел $(c - a)$ противоречит выбору c. Поэтому

$$b_2 \le a_2 + c_2.$$

Если $b_1 \ge c_1$, то $M \in \Omega_4$. Пусть

$$b_1 < c_1.$$

Тогда

$$a_2 < b_2,$$

(иначе b противоречит условию $a \in \mathfrak{M}(\Gamma)$). Рассмотрим узел $c' = (c'_1, c'_2, c'_3) = -a + b + c$. Тогда

$$\begin{aligned} c'_1 &= -(a_1 + b_1 - c_1), \quad |c'_1| < a_1, \\ c_2 &= -(a_2 + c_2 - b_2), \quad |c'_2| < b_2, \\ c'_3 &= +(c_3 + b_3 - a_3), \quad |c'_3| \le c_3. \end{aligned}$$

Тогда $|c'_3| = c_3$ (иначе c' противоречит выбору c), т.е. $b_3 = a_3$. Следовательно, узел c' также удовлетворяет (2.5) и $M(a, b, c') \in \partial\Omega_3$.

2.3. Пусть

$$M = M(a, b, c) = \begin{pmatrix} a_1 & -b_1 & -c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}, \quad b_1, c_1 > 0.$$

Если $c_2 = 0$, то $M \in \Omega_3$. Пусть

$$c_2 > 0.$$

Если $b_3 > 0$, то узел $(c-b)$ противоречит выбору c. Значит, $b_3 = 0$. Тогда узел $c' = c-b$ также удовлетворяет (2.5), причем

$$M(a,b,c') \in \begin{cases} \partial\Omega_3, & b_1 \le c_1, \\ \partial\Omega_4 & b_1 > c_1. \end{cases}$$

□

Рассмотрим теперь вопрос: в каких случаях узел a *единственным* образом дополняется до базиса указанным выше способом (т.е. когда узлы b, c однозначно определяются условиями (2.1), (2.5))?

Пусть Ω_i' — внутренность множества Ω_i, то есть для матриц из Ω_i' все неравенства, входящие в определение Ω_i, являются строгими. Очевидно, что $\Omega_i' \cap \Omega_j' = \emptyset$ при $i \ne j$.

Лемма 2.3. *Пусть $M = M(a,b,c) \in \cup_{i=1}^4 \Omega_i'$, решетка Γ порождена векторами a, b, c. Тогда не существует такого узла $\gamma \in \Gamma \setminus \{0, \pm a, \pm b, \pm c\}$, что*

$$|\gamma_1| \le a_1, \quad |\gamma_2| \le b_2, \quad |\gamma_3| \le c_3.$$

Доказательство. Пусть

$$\gamma = (m'a + n'b + k'c) \in \Gamma \setminus \{0, \pm a, \pm b, \pm c\}.$$

Нужно доказать, что $|\gamma_1| > b_1$ либо $|\gamma_2| > b_2$, либо $|\gamma_3| > c_3$. Целые m', n', k' будем называть коэффициентами. Не умаляя общности считаем, что первая ненулевая координата вектора (m', n', k') является положительной. Случай, когда два коэффициента равны нулю является тривиальным. Всюду ниже m, n, k — натуральные.

Пусть ровно один из коэффициентов равен нулю. Тогда

если $(m', n', k') = (m, n, 0)$, то $|\gamma_2| = ma_2 + nb_2 > b_2$;

если $(m', n', k') = (m, -n, 0)$, то $|\gamma_1| = ma_1 + nb_1 > a_1$;

если $(m', n', k') = (m, 0, k)$, то $|\gamma_3| = ma_3 + kc_3 > c_3$;

если $(m', n', k') = (m, 0, -k)$, то

$$\begin{array}{ll} |\gamma_1| = ma_1 + kc_1 > a_1 & \text{при } M \in \Omega_1' \cup \Omega_2' \cup \Omega_3'; \\ |\gamma_2| = ma_2 + kc_2 \ge a_2 + c_2 > b_2 & \text{при } M \in \Omega_4'; \end{array}$$

если $(m', n', k') = (0, n, k)$, то

$$\begin{array}{lll} |\gamma_1| = nb_1 + kc_1 \ge b_1 + c_1 > a_1 & \text{при} & M \in \Omega_1'; \\ |\gamma_2| = nb_2 + kc_2 > b_2 & \text{при} & M \in \Omega_2'; \\ |\gamma_3| = nb_3 + kc_3 > c_3 & \text{при} & M \in \Omega_3' \cup \Omega_4' \end{array}$$

если $(m', n', k') = (0, n, -k)$, то

$$\begin{array}{ll} |\gamma_3| = nb_3 + kc_3 > c_3 & \text{при } M \in \Omega'_1 \cup \Omega'_2; \\ |\gamma_2| = nb_2 + kc_2 > b_2 & \text{при } M \in \Omega'_3 \cup \Omega'_4. \end{array}$$

Пусть теперь все коэффициенты ненулевые. Возможны четыре случая.

1. Пусть $(m', n', k') = (m, n, k)$. Тогда, если $M \in \Omega'_1$, то

$$\begin{array}{ll} |\gamma_3| = ma_3 - nb_3 + kc_3 \geq |kc_3 - (n-1)b_3| > c_3 & \text{при } k \geq n, \\ |\gamma_2| = ma_2 + nb_2 - kc_2 > b_2 & \text{при } k < n. \end{array}$$

Если $M \in \Omega'_2$, то $|\gamma_2| = ma_2 + nb_2 + kc_2 > b_2$.
Если $M \in \Omega'_3 \cup \Omega'_4$, то $|\gamma_3| = ma_3 + nb_3 + kc_3 > c_3$.

2. Пусть $(m', n', k') = (m, -n, -k)$. Тогда, если $M \in \Omega'_1 \cup \Omega'_2 \cup \Omega'_3$, то

$$|\gamma_1| = ma_1 + nb_1 + kc_1 > a_1.$$

Если $M \in \Omega'_4$, то

$$\begin{array}{ll} |\gamma_1| = ma_1 + nb_1 - kc_1 > a_1 & \text{при } m > k \text{ либо } n \geq k, \\ |\gamma_3| = -ma_3 + nb_3 + kc_3 > c_3 & \text{при } m < k, \\ |\gamma_2| = ma_2 - nb_2 + mc_2 > b_2 & \text{при } k = m > n. \end{array}$$

3. Пусть $(m', n', k') = (m, -n, k)$. Тогда, если $M \in \Omega'_1 \cup \Omega'_2$, то

$$|\gamma_3| = ma_3 + nb_3 + kc_3 > c_3.$$

Если $M \in \Omega'_3$, то

$$\begin{array}{ll} |\gamma_2| = -ma_2 + nb_2 + kc_2 > b_2 & \text{при } n > m, \\ |\gamma_3| = ma_3 - nb_3 + kc_3 > c_3 & \text{при } n \leq m. \end{array}$$

Если $M \in \Omega'_4$, то $|\gamma_1| = ma_1 + nb_1 + kc_1 > a_1$.

4. Пусть $(m', n', k') = (m, n, -k)$. Тогда, если $M \in \Omega'_1 \cup \Omega'_3 \cup \Omega'_4$, то

$$|\gamma_2| = ma_2 + nb_2 + kc_2 > b_2.$$

Если $M \in \Omega'_2$, то

$$\begin{array}{ll} |\gamma_1| = ma_1 - nb_1 + kc_1 > a_1 & \text{при } m > n, \\ |\gamma_2| = ma_2 + nb_2 - kc_2 > b_2 & \text{при } n > k, \\ |\gamma_3| = -ma_3 + nb_3 + kc_3 > c_3 & \text{при } k > m, \\ |\gamma_1| > a_1 \text{ либо } |\gamma_2| > b_2 & \text{при } k = m = n. \end{array}$$

□

Из леммы очевидным образом вытекает следующий результат.

Следствие 2.1. *Пусть* $M(a, b, c) \in \cup_{i=1}^{4} \Omega'_i$, *решетка* Γ *порождена векторами* a, b, c. *Тогда*

а) b и c являются единственными узлами Γ, удовлетворяющими условиям (2.1) и (2.5) соответственно;

б) система $\{a, b, c\}$ является минимальной.

Мера μ и оператор проективизации $\mathcal{P} : \mathrm{GL}_s(\mathbb{R}) \to \mathrm{P}_s(\mathbb{R})$ определены в § II.1.

Теорема 2.1. *Для любого целого $N > 1$ среднее количество относительных минимумов трехмерных решеток равно*

$$E(N, 3) = \mathcal{C}(3) \cdot \ln^2 N + O(\chi(N) \cdot \ln N),$$

где

$$\mathcal{C}(3) = \frac{4}{\zeta(2)\zeta(3)} \cdot \Big(\mu(\mathcal{P}(\Omega_1)) + \mu(\mathcal{P}(\Omega_2)) + 2 \cdot \mu(\mathcal{P}(\Omega_3)) + 2 \cdot \mu(\mathcal{P}(\Omega_4)) \Big).$$

Доказательство. Будем использовать соотношение (0.1). Множество $\mathcal{U}_3(N)$ разобьем на три (пересекающиеся) части:

$$\begin{aligned} U^{(1)} &= \{(\Gamma, a) \in \mathcal{U}_3(N) : \text{ существует } b, \text{ удовлетворяющий (2.1) и (2.2)}\}, \\ U^{(2)} &= \{(\Gamma, a) \in \mathcal{U}_3(N) : \text{ существует } b, \text{ удовлетворяющий (2.1) и (2.3)}\}, \\ U^{(3)} &= \{(\Gamma, a) \in \mathcal{U}_3(N) : \text{ существует } b, \text{ удовлетворяющий (2.1) и (2.4)}\}. \end{aligned}$$

В силу симметрии,

$$\#U^{(2)} = \#U^{(3)}. \tag{2.6}$$

Кроме того,

$$\#U^{(1)} = \#\Omega_1(\mathbb{Z}, N) + \#\Omega_2(\mathbb{Z}, N) + O(\xi(N)), \tag{2.7}$$
$$\#U^{(2)} = \#\Omega_3(\mathbb{Z}, N) + \#\Omega_4(\mathbb{Z}, N) + O(\xi(N)), \tag{2.8}$$
$$\#(U_i \cap U_j) = O(\xi(N)) \text{ при } i \neq j, \tag{2.9}$$

где

$$\xi(N) = \sum_{i=1}^{4} \#\partial\Omega_i(\mathbb{Z}, N).$$

Докажем (2.7). Пусть $(\Gamma, a) \in U^{(1)}$. Согласно лемме 2.2 узел a можно дополнить до базиса (a, b, c) так, что $M = M(a, b, c) \in \Omega_1 \cup \Omega_2$. Матрицы из $\Omega_1 \cup \Omega_2$ имеют положительный определитель. Следовательно, $M \in \mathrm{M}_3(\mathbb{Z}; N)$. Таким образом, каждой паре $(\Gamma, a) \in U^{(1)}$ мы можем поставить в соответствие (хотя бы одну) целочисленную матрицу из $\Omega_1 \cup \Omega_2$ определителя N. Очевидно, что разным парам из $U^{(1)}$ соответствуют разные матрицы. Значит,

$$\#U^{(1)} \leq \# \Big((\Omega_1 \cup \Omega_2)(\mathbb{Z}; N) \Big) \leq \#\Omega_1(\mathbb{Z}; N) + \#\Omega_2(\mathbb{Z}; N) + \xi(N). \tag{2.10}$$

Возьмем любую целочисленную матрицу $M = M(a, b, c) \in \Omega_1' \cup \Omega_2'$ с $\det M = N$. Рассмотрим решетку Γ с базисом a, b, c. Согласно следствию 2.1, b и c являются

единственными узлами Γ, удовлетворяющими условиям (2.1) и (2.5). Кроме того, $(\Gamma, a) \in U^{(1)}$. Значит, существует взаимно однозначное соответствие между $\Omega_1'(\mathbb{Z}; N) \cup \Omega_2'(\mathbb{Z}; N)$ и некоторым подмножеством $U^{(1)}$. Поэтому

$$\#\Omega_1'(\mathbb{Z}; N) + \#\Omega_2'(\mathbb{Z}; N) \leq \#U^{(1)}. \tag{2.11}$$

Из (2.10), (2.11) вытекает (2.7). Соотношение (2.8) доказывается аналогично.

Для обоснования (2.9) достаточно заметить следующее. Если $(\Gamma, a) \in U^{(i)} \cap U^{(j)}$, то существует, как минимум, два узла b, удовлетворяющих (2.1). Значит, матрица $M(a, b, c)$ не может лежать в $\cup_{i=1}^{4} \Omega_i'$ (иначе противоречие со следствием 2.1), т.е. $M(a, b, c)$ принадлежит объединению границ множеств Ω_i. Повторяя рассуждения, использованные при доказательстве (2.10), получаем (2.9).

Из (2.6), (2.7), (2.8), (2.9) вытекает асимптотическая формула

$$\#\mathcal{U}_3(N) = \#\Omega_1(\mathbb{Z}, N) + \#\Omega_2(\mathbb{Z}, N) + 2 \cdot \#\Omega_3(\mathbb{Z}, N) + 2 \cdot \#\Omega_4(\mathbb{Z}, N) + O(\xi(N)). \tag{2.12}$$

Если $M(a, b, c)$ принадлежит некоторому Ω_i', то система $\{a, b, c\}$ является минимальной по следствию 2.1. Поэтому, согласно теореме Минковского о линейных формах,

$$a_1 \cdot b_2 \cdot c_3 < \det M(a, b, c).$$

Значит, множество $\Omega = \Omega_i$ удовлетворяет условию (Б) главы II. Выполнение (А) очевидно. Поэтому мы можем применить теорему 1.1. Ввиду $\mu(\mathcal{P}(\partial\Omega_i)) = 0$, получаем

$$\#\Omega_i(\mathbb{Z}, N) = \frac{\mathcal{R}_3(N)}{\zeta(2) \cdot \zeta(3)} \cdot \left(\frac{\mu(\mathcal{P}(\Omega_i))}{2} \cdot \ln^2 N + O_{\Omega_i}\left(\chi(N) \cdot \ln N\right) \right),$$
$$\xi(N) \ll \mathcal{R}_3(N) \cdot \chi(N) \cdot \ln N,$$

Осталось подставить последние соотношения в (2.12), (0.1). □

Замечание 2.2. По-видимому, постоянная $\mathcal{C}(3)$ не выражается через известные. Приближенные вычисления дали следующий результат:

$$\mu(\mathcal{P}(\Omega_1)) \approx 0.0442, \quad \mu(\mathcal{P}(\Omega_2)) \approx 0.0922,$$
$$\mu(\mathcal{P}(\Omega_3)) \approx 0.1119, \quad \mu(\mathcal{P}(\Omega_4)) \approx 0.0268,$$
$$\mathcal{C}(3) \approx 0.8335.$$

Отметим, что

$$\mathcal{C}(2) = \frac{4 \ln 2}{\zeta(2)} \approx 1.6855.$$

§ 3. Случай произвольной размерности

Введем следующее отношение упорядоченности на $\mathbb{R}^s$ (лексикографическое). Пусть $x, y \in \mathbb{R}^s$. Пишем $x \prec y$, если существует такой номер $k \in \{1, \ldots, s\}$, что $x_i = y_i$, $i = \overline{1, k-1}$ и $x_k < y_k$.

Пусть M — некоторое подмножество $\mathbb{R}^s$. Будем говорить, что $x \in M$ является $\prec$-наименьшим вектором M, если $x \prec y$ для любого другого $y \in M$. Любое конечное множество имеет единственный $\prec$-наименьший вектор.

Возьмем любую пару $(\Gamma, a) \in \mathcal{U}_s$. Выберем ненулевые узлы $b^{(1)}, \dots, b^{(s)}$ решетки Γ следующим образом.

1 шаг. Полагаем $b^{(1)} = a$.

2 шаг. Определим множество $H_2 = H_2(\Gamma; b^{(1)})$, состоящее из ненулевых $\gamma \in \Gamma$, удовлетворяющих условиям:

$$|\gamma_1| \le \frac{b_1^{(1)}}{s!}; \qquad |\gamma_i| \le a_i, \;\; i > 2.$$

Оно непусто согласно замечанию 2.1. Выберем узел $b^{(2)}$ из условий:

$$b^{(2)} \in H_2, \qquad 0 \le b_2^{(2)} = \min_{\gamma \in H_2} |\gamma_2|.$$

Если таких узлов несколько, то в качестве $b^{(2)}$ выбираем $\prec$-наименьший. Отметим, что

$$a_2 < b_2^{(2)}. \tag{3.1}$$

Действительно, в противном случае

$$|b_1^{(2)}| < a_1, \quad |b_i^{(2)}| \le a_i, \;\; i = \overline{2, s}.$$

Это противоречит условию $a \in \mathfrak{M}(\Gamma)$.

k-й шаг. Пусть $b^{(1)}, \dots, b^{(k-1)}$ выбраны. Через $H_k = H_k(\Gamma; b^{(1)}, \dots, b^{(k-1)})$ обозначаем множество, состоящее из таких ненулевых $\gamma \in \Gamma$, что

$$\begin{aligned} |\gamma_j| &\le \frac{b_j^{(j)}}{s!} \quad \text{при} \quad j < k, \\ |\gamma_j| &\le a_j \quad \text{при} \quad j > k. \end{aligned}$$

Оно непусто согласно замечанию 2.1. Узел $b^{(k)}$ выбираем из условий:

$$b^{(k)} \in H_k, \qquad 0 \le b_k^{(k)} = \min_{\gamma \in H_k} |\gamma_k|.$$

Если таких узлов несколько, то в качестве $b^{(k)}$ выбираем $\prec$-наименьший. Отметим, что

$$a_k < b_k^{(k)}, \quad k = \overline{3, s}, \tag{3.2}$$

так как в противном случае $b^{(k)} \in H_{k-1}$, однако $b_{k-1}^{(k)} < b_{k-1}^{(k-1)}$, что противоречит выбору $b^{(k-1)}$.

Набор $\{b^{(j)}\}_{j=1}^s$ будем называть $\mathfrak{M}$-*подходящей системой* для пары (Γ, a). Подчеркнем, что для любой пары $(\Gamma, a) \in \mathcal{U}_s$ существует *единственная* $\mathfrak{M}$-подходящая система.

Лемма 3.1. *Пусть $\{b^{(j)}\}_{j=1}^s$ — $\mathfrak{M}$-подходящая система для пары $(\Gamma, a) \in \mathcal{U}_s$. Тогда*

а) для любого $k \in \{1, \dots, s\}$ справедливы оценки:

$$\begin{aligned} \left|b_k^{(j)}\right| &< b_k^{(k)}, \quad j < k, \\ \left|b_k^{(j)}\right| &\le \frac{b_k^{(k)}}{s!}, \quad j > k; \end{aligned} \tag{3.3}$$

б) система $b^{(1)}, \dots, b^{(s)}$ линейно-независимая, причем

$$\det(\|b_i^{(j)}\|) > \frac{1}{s!} \prod_{i=1}^{s} b_i^{(i)}; \tag{3.4}$$

в) справедлива оценка:

$$\prod_{i=1}^{s} b_i^{(i)} < C_1 \cdot \det \Gamma, \quad C_1 = (s!)^{s-1}. \tag{3.5}$$

Доказательство. Докажем а). Так как $b^{(j)} \in H_j$, то

$$|b_k^{(j)}| \le a_k \text{ при } j < k; \quad |b_k^{(j)}| \le \frac{b_k^{(k)}}{s!} \text{ при } j > k.$$

Учитывая (3.1), (3.2), получаем (3.3).

Докажем б). В силу (3.3) для любой нетождественной перестановки $(k_1, \dots, k_s)$ из $\{1, \dots, s\}$ выполняется оценка

$$\prod_{j=1}^{s} \left| b_{k_j}^{(j)} \right| < \frac{1}{s!} \prod_{i=1}^{s} b_i^{(i)}.$$

Поэтому

$$\det(\|b_i^{(j)}\|) > \prod_{i=1}^{s} b_i^{(i)} - (s! - 1) \cdot \frac{1}{s!} \prod_{i=1}^{s} b_i^{(i)} = \frac{1}{s!} \prod_{i=1}^{s} b_i^{(i)}.$$

Докажем в). Если (3.5) не выполняется, то по теореме Минковского о линейных формах [54, глава III, § 2, теорема III] существует такой ненулевой узел $\gamma \in \Gamma$, что

$$|\gamma_i| \le \frac{b_i^{(i)}}{s!}, \quad i = \overline{1, s-1}; \qquad |\gamma_s| < b_s^{(s)}.$$

Но тогда $\gamma \in H_s(\Gamma; b^{(1)}, \dots, b^{(s-1)})$, причем $|\gamma_s| < b_s^{(s)}$. Это противоречит выбору $b^{(s)}$. □

Пусть $b^{(1)}, \dots, b^{(s)}$ — $\mathfrak{M}$-подходящая система для пары $(\Gamma, a) \in \mathcal{U}_s$. Хорошо известно (см., например, [54, глава I, следствие 2]), что существует единственный базис $a^{(1)}, \dots, a^{(s)}$ решетки Γ такой, что

$$\begin{aligned} b^{(1)} &= v_{11} a^{(1)}, \\ b^{(2)} &= v_{12} a^{(1)} + v_{22} a^{(2)}, \\ &\vdots \\ b^{(s)} &= v_{1s} a^{(1)} + v_{2s} a^{(2)} + \dots + v_{ss} a^{(s)}, \end{aligned}$$

то есть

$$b^{(j)} = \sum_{i=1}^{j} v_{ij} a^{(i)}, \quad j = \overline{1, s} \tag{3.6}$$

причем неотрицательные целые v_{ij} удовлетворяют условиям:

$$0 \le v_{ij} < v_{jj} \text{ при } i < j. \tag{3.7}$$

Так как $b^{(1)} = a \in \mathfrak{M}(\Gamma)$, то $v_{11} = 1$, то есть $a^{(1)} = b^{(1)} = a$.

Систему $a^{(1)}, a^{(2)}, \dots, a^{(s)}$ будем называть $\mathfrak{M}$-*подходящим базисом*, а соответствующую матрицу $A = (\!(a_i^{(j)})\!)$ (со столбцами ${a^{(1)}}^T, \dots, {a^{(s)}}^T$) — $\mathfrak{M}$-*подходящей базисной матрицей* для пары (Γ, a).

Для любой пары $(\Gamma, a) \in \mathcal{U}_s$ существует *единственный* $\mathfrak{M}$-подходящий базис.

Пусть V — верхнетреугольная матрица размера $s \times s$, у которой (i,j)-элемент равен v_{ij} при $i \le j$ и равен нулю при $i > j$. Пусть $B = (\!(b_i^{(j)})\!)$. Тогда (3.6) можно записать в виде

$$B = A \cdot V. \tag{3.8}$$

Лемма 3.2. *Пусть* $\{a^{(j)}\}_{j=1}^s$ — $\mathfrak{M}$-*подходящий базис, а* $\{b^{(j)}\}_{j=1}^s$ — $\mathfrak{M}$-*подходящая система для пары* $(\Gamma, a) \in \mathcal{U}_s$. *Тогда*

$$\det A > 0; \tag{3.9}$$

$$\prod_{i=1}^{s} v_{ii} < C_1 \cdot s! = (s!)^s. \tag{3.10}$$

$$\left|a_k^{(j)}\right| \le 2^{j-1} \cdot b_k^{(k)}, \quad k, j = \overline{1, s}; \tag{3.11}$$

$$\prod_{i=1}^{s} \max_{1 \le j \le s} \left|a_i^{(j)}\right| < C_2 \cdot \det \Gamma, \quad C_2 = 2^{s(s-1)} \cdot C_1. \tag{3.12}$$

Доказательство. Используя (3.4), (3.7), получаем $\det B > 0$, $\det V > 0$. Поэтому (3.9) вытекает из (3.8). Кроме того,

$$\prod_{i=1}^{s} v_{ii} = \det V = \frac{\det B}{\det A} < \frac{s! \cdot \prod_{i=1}^{s} b_i^{(i)}}{\det A}.$$

Ввиду (3.5) и равенства $\det A = \det \Gamma$, приходим к (3.10).

Для доказательства (3.11) достаточно учесть, что для любого j

$$\left|a_k^{(j)}\right| \le \frac{1}{v_{jj}} \left|b_k^{(j)}\right| + \sum_{i=1}^{j-1} \frac{v_{ij}}{v_{jj}} \left|a_k^{(i)}\right| \le \left|b_k^{(k)}\right| + \sum_{i=1}^{j-1} \left|a_k^{(i)}\right|.$$

и применить математическую индукцию. Оценка (3.12) следует из (3.5), (3.11). □

Нам понадобится следующий вспомогательный результат.

Лемма 3.3. *Пусть* C', C'' — *некоторые положительные постоянные,* $\Gamma \in \mathcal{L}_s(\mathbb{R})$. *Пусть* $x^{(1)}, \dots, x^{(s)}$ — *такой базис решетки* Γ, *что*

$$\prod_{i=1}^{s} \max_{1 \le j \le s} \left|x_i^{(j)}\right| \le C' \cdot \det \Gamma,$$

Тогда любой узел $\gamma \in \Gamma$, удовлетворяющий неравенствам

$$|\gamma_i| \le C'' \cdot \max_{1\le j\le s} \left|x_i^{(j)}\right|, \quad i = \overline{1,s},$$

представим в виде $\gamma = n_1 x^{(1)} + \ldots + n_s x^{(s)}$, где $|n_j| \le C' \cdot C'' \cdot s!$, $j = \overline{1,s}$.

Доказательство. Используя формулы Крамера, получаем

$$n_j = \frac{D_j}{D}, \quad j = \overline{1,s},$$

где $D = \det X$, $X = (\!(x_i^{(j)})\!)$, а D_j — определитель матрицы, полученной из X, заменой j-го столбца на γ^T. Осталось заметить, что

$$|D| = \det \Gamma,$$
$$|D_j| \le C'' \cdot s! \cdot \prod_{i=1}^{s} \max_{1\le k\le s} \left|x_i^{(k)}\right| \le C' \cdot C'' \cdot s! \cdot \det \Gamma.$$

□

Пусть $\Omega_{\mathfrak{M},s}$ — множество, состоящее из всех $\mathfrak{M}$-подходящих базисных матриц для пар $(\Gamma, a) \in \mathcal{U}_s$. Рассмотрим свойства $\Omega_{\mathfrak{M},s}$.

Многогранным углом в пространстве $\mathbb{R}^s$ с вершиной в точке 0 будем называть множество решений $x \in \mathbb{R}^s$ некоторой конечной системы линейных однородных неравенств, т.е. множество, состоящее из $x \in \mathbb{R}^s$, удовлетворяющих соотношениям вида:

$$\sum_{i=1}^{s} \alpha_i^{(k)} x_i \le 0, \;\; k = \overline{1,L_1}; \qquad \sum_{i=1}^{s} \beta_i^{(k)} x_i < 0, \;\; k = \overline{1,L_2},$$

где L_1, L_2 — неотрицательные целые, а $\alpha_i^{(k)}, \beta_i^{(k)} \in \mathbb{R}$.

Определим отображение Φ, которое каждой невырожденной матрице $A = (\!(a_i^{(j)})\!)$ ставит в соответствие пару (Γ, a), где $a = a^{(1)}$, а Γ — решетка с базисом $\{a^{(j)}\}_{j=1}^{s}$ (т.е. столбцы A образуют базис Γ). Тогда множество $\Omega_{\mathfrak{M},s}$ состоит из матриц A таких, что $\Phi(A) = (\Gamma, a) \in \mathcal{U}_s$, причем матрица A является $\mathfrak{M}$-подходящей для пары (Γ, a).

Теорема 3.1. *Справедливы следующие свойства:*

а) Φ взаимно однозначно отображает $\Omega_{\mathfrak{M},s}$ на $\mathcal{U}_s$;

б) для любой матрицы $A = (\!(a_i^{(j)})\!) \in \Omega_{\mathfrak{M},s}$ имеет место оценка:

$$\prod_{i=1}^{s} \max_{1\le j\le s} |a_i^{(j)}| \le C_2 \cdot \det A.$$

в) $\Omega_{\mathfrak{M},s}$ является объединением фиксированного числа множеств вида

$$\left\{ (\!(a_i^{(j)})\!) : \quad (a_i^{(1)}, \ldots, a_i^{(s)}) \in K_i, \; i = \overline{1,s} \right\},$$

где K_i — многогранные углы из $\mathbb{R}^s$ с вершинами в точке 0.

Доказательство. Утверждение а) вытекает из определений, а б) эквивалентно (3.12).

Осталось доказать в). Будем говорить, что матричное множество Ω удовлетворяет в), если выполняется условие в), в котором $\Omega_{\mathfrak{M},s}$ заменяем на Ω.

Определим множество $\mathrm{GL}_s'(\mathbb{R})$, состоящее из матриц $X \in \mathrm{GL}_s(\mathbb{R})$, у которых элементы первого столбца положительные.

Возьмем любую $A = (\!(a_i^{(j)})\!) \in \mathrm{GL}_s'(\mathbb{R})$. Пусть $(\Gamma, a) = \Phi(A)$. Тогда $A \in \Omega_{\mathfrak{M},s}$, если и только если $a \in \mathfrak{M}(\Gamma)$ и существует $\mathfrak{M}$-подходящая система (для пары (Γ, a)), которая определяется формулами (3.6), где v_{ij} — целые числа, удовлетворяющие (3.7).

Согласно леммам 3.1, 3.2, $\mathfrak{M}$-подходящая система должна удовлетворять оценкам (3.3), а целые v_{ij} — (3.10). Кроме того, $v_{11} = 1$. Пусть множество $\mathcal{V}$ состоит из наборов целочисленных коэффициентов $V = (v_{11}, v_{12}, \ldots, v_{ss})$ для которых выполняются (3.7), (3.10), причем $v_{11} = 1$. Тогда $\Omega_{\mathfrak{M},s}$ можно представить в виде:

$$\Omega_{\mathfrak{M},s} = \bigcup_{V \in \mathcal{V}} \Omega_V,$$

где Ω_V состоит из матриц $A = (\!(a_i^{(j)})\!) \in \mathrm{GL}_s'(\mathbb{R})$, удовлетворяющих следующим условиям (в которых $b^{(j)}$ определяются (3.6), а $(\Gamma, a) = \Phi(A)$):

1) выполняются оценки (3.3) для $b^{(j)}$;

2) $a \in \mathfrak{M}(\Gamma)$; система $\{b^{(j)}\}_{j=1}^s$ является $\mathfrak{M}$-подходящей для пары (Γ, a).

Подчеркнем, что коэффициенты v_{ij} в (3.6) однозначно определяются по V.

Так как множество $\mathcal{V}$ конечное, то осталось доказать, что каждое Ω_V удовлетворяет в).

Пусть $V \in \mathcal{V}$. Определим $\tilde{\Omega}_V$ — множество матриц из $\mathrm{GL}_s'(\mathbb{R})$ для которых выполняется условие 1). Очевидно, что $\tilde{\Omega}_V$ удовлетворяет в). Рассмотрим некоторые свойства множества $\tilde{\Omega}_V$.

Возьмем любую матрицу $A = (\!(a_i^{(j)})\!) \in \tilde{\Omega}_V$. Пусть $B = (\!(b_i^{(j)})\!)$. Тогда

$$\det B > \frac{1}{s!} \prod_{i=1}^{s} b_i^{(i)} \qquad \text{(согласно (3.3))},$$

$$\det B = \det A \cdot \prod_{i=1}^{s} v_{ii} < (s!)^s \cdot \det A \qquad \text{(согласно (3.10))},$$

$$|a_i^{(j)}| \le 2^{j-1} \cdot b_i^{(i)}, \quad i, j = \overline{1, s} \qquad \text{(согласно (3.6), (3.7), (3.3))},$$

и поэтому

$$\prod_{i=1}^{s} \max_{1 \le j \le s} |a_i^{(j)}| \le 2^{s(s-1)} \prod_{i=1}^{s} b_i^{(i)} \le 2^{s(s-1)} \cdot s! \cdot \det B \le C_3 \cdot \det A, \tag{3.13}$$

где $C_3 = (s!)^{s+1} \cdot 2^{s(s-1)}$. Кроме того, используя (3.6), (3.7), (3.10), имеем

$$b_i^{(i)} \underset{s}{\ll} \max_{1 \le j \le s} |a_i^{(j)}|, \quad i = \overline{1, s}. \tag{3.14}$$

Положим $(\Gamma, a) = \Phi(A)$ и определим множества

$$H_k(A) = \left\{ \gamma \in \Gamma \setminus \{0\} : \quad |\gamma_i| \le \frac{b^{(i)}}{s!}, \ \ i = \overline{1, k-1}, \quad |\gamma_i| \le a_i, \ \ i = \overline{k+1, s} \right\}, \quad k = \overline{2, s}.$$

Матрица A не принадлежит Ω_V, если и только если не выполняется условие 2), то есть существует узел $\gamma \in \Gamma \setminus \{0\}$, удовлетворяющий одному из следующих двух условий:

i) $|\gamma_i| \le a_i$, $i = \overline{1,s}$, причем хотя бы одно из неравенств строгое;

ii) существует такой номер $k \in \{2,\dots,s\}$, что $\gamma \in H_k(A)$ и либо $|\gamma_k| < b_k^{(k)}$, либо $\gamma_k = b_k^{(k)}$, $\gamma \prec b^{(k)}$.

Условие i) означает, что $a \notin \mathfrak{M}(\Gamma)$, а ii) — $\{b^{(j)}\}_{j=1}^s$ не является $\mathfrak{M}$-подходящей системой. Используя (3.14), получаем, что в обоих случаях

$$|\gamma_i| \underset{s}{\ll} \max_{1\le j\le s} |a_i^{(j)}|, \quad i = \overline{1,s}.$$

Применяя лемму 3.3 (с учетом (3.13)), мы видим, что любой $\gamma \in \Gamma$, удовлетворяющий i) или ii), представим в виде

$$\gamma = \sum_{j=1}^{s} n_j a^{(j)}, \quad |n_j| \le C_4,$$

где C_4 — некоторая постоянная, зависящая только от s. Значит,

$$\tilde{\Omega}_V \setminus \Omega_V = \bigcup_{n\in\mathcal{N}_s} U_{V,n}, \quad \mathcal{N}_s = \{n \in \mathbb{Z}^s \setminus \{0\} : \quad \max_{1\le i\le s} |n_i| \le C_4\},$$

где $U_{V,n}$ ($n = (n_1,\dots,n_s)$) состоит из матриц $A \in \Omega_V$ таких, что выполняется i) или ii), в которых $\gamma = n_1 a^{(1)} + \ldots + n_s a^{(s)}$. Каждое из множеств $U_{V,n}$ удовлетворяет в). Значит, это условие выполняется и для $\tilde{\Omega}_V \setminus \Omega_V$. Следовательно, Ω_V также удовлетворяет в). □

Пусть $\Omega_{\mathfrak{M},s}(\mathbb{Z};N)$ — множество целочисленных матриц $M \in \Omega_{\mathfrak{M},s}$, у которых $\det M = N$. Тогда

$$A \in \Omega_{\mathfrak{M},s}(\mathbb{Z};N) \quad \Longleftrightarrow \quad \Phi(A) \in \mathcal{U}_s(N).$$

Поэтому, используя теорему 3.1 а), получаем

$$\#\mathcal{U}_s(N) = \#\Omega_{\mathfrak{M},s}(\mathbb{Z};N). \tag{3.15}$$

Замечание 3.1. Пусть Γ — s-мерная решетка. Из утверждения а) теоремы 3.1 вытекает, что множество относительных минимумов Γ с положительными координатами совпадает с множеством первых столбцов матриц $A \in \Omega_{\mathfrak{M},s} \cap M(\Gamma)$, где $M(\Gamma)$ — множество всех базисных матриц Γ.

Оператор проективизации $\mathcal{P}$ и мера μ определены в § II.1.

Теорема 3.2. *Для любых целых $s, N \ge 2$ справедлива следующая асимптотическая формула для среднего количества относительных минимумов:*

$$E(N,s) = \mathcal{C}(s)\cdot \ln^{s-1} N + O_s(\chi(N)\cdot \ln^{s-2} N),$$

где

$$\mathcal{C}(s) = \frac{2^s}{(s-1)!}\cdot \frac{\mu(\mathcal{P}(\Omega_{\mathfrak{M},s}))}{\zeta(2)\cdot\ldots\cdot\zeta(s)}.$$

Доказательство. Используя (0.1) и (3.15), получаем

$$E(N,s)=\frac{2^s}{\mathcal{R}_s(N)}\cdot\#\mathcal{U}_s(N)+O_s(\ln^{s-2}N)=\frac{2^s}{\mathcal{R}_s(N)}\cdot\#\Omega_{\mathfrak{M},s}(\mathbb{Z};N)+O_s(\ln^{s-2}N).$$

Осталось заметить, что множество $\Omega_{\mathfrak{M},s}$ удовлетворяет условиям (А), (Б) главы II (см. теорему 3.1) и применять теорему II.1.1 для вычисления $\#\Omega_{\mathfrak{M},s}(\mathbb{Z};N)$. □

§ 4. Оценки постоянной $\mathcal{C}(s)$

Теорема 4.1. *Для любого простого N и целого $s\geq 2$ справедливы оценки*

$$\frac{1}{(s-1)!}+O_s\left(\frac{1}{\ln N}\right)\leqslant\frac{E(N,s)}{\ln^{s-1}N}\leqslant\frac{2^s}{(s-1)!}+O_s\left(\frac{1}{\ln N}\right)$$

Доказательство. Пусть $\mathfrak{M}_+(\Gamma)$ — множество относительных минимумов решетки Γ с положительными координатами. Определим множество $L_s(N)$, состоящее из решеток $\Gamma(a)$ вида

$$\Gamma(a)=\left\{\gamma\in\mathbb{Z}^s:\ \sum_{i=1}^{s-1}a_i\gamma_i\equiv\gamma_s\pmod N\right\},$$

где

$$a=(a_1,\ldots,a_{s-1})\in\mathbb{Z}^{s-1}(N)=(\mathbb{Z}\cap[1,N])^{s-1}$$

Так как N простое, то согласно формулам (II.2.3),

$$\#\mathcal{L}_s(\mathbb{Z},N)=N^{s-1}+N^{s-2}+\ldots+1=N^{s-1}+O_s(N^{s-2}).$$

Кроме того, $\#L_s(N)=N^{s-1}$. У любой решетки из $\mathcal{L}_s(\mathbb{Z};N)$ количество относительных минимумов оценивается величиной $O_s(\ln^{s-1}N)$. Поэтому, используя (0.1), заключаем

$$E\,(N,s)=\frac{2^s}{N^{s-1}}\sum_{\Gamma\in L_s(N)}\#\mathfrak{M}_+(\Gamma)+O_s\left(\ln^{s-2}N\right).$$

Очевидно, что

$$\sum_{\Gamma\in L_s(N)}\#\mathfrak{M}_+(\Gamma)=\sum_{\gamma\in\mathbb{N}^s}f_s(N,\gamma),$$

где $f_s(N,\gamma)$ — количество решеток $\Gamma\in L_s(N)$ таких, что $\gamma\in\mathfrak{M}(\Gamma)$. Поэтому достаточно доказать следующие оценки:

$$\frac{\ln^{s-1}N}{2^s\cdot(s-1)!}+O_s(\ln^{s-2}N)\leq\frac{1}{N^{s-1}}\sum_{\gamma\in\mathbb{N}^s}f_s(N,\gamma)\leq\frac{\ln^{s-1}N}{(s-1)!}+O_s(\ln^{s-2}N),\qquad(4.1)$$

Для любых $\gamma,\eta\in\mathbb{Z}^s$ определим

$T_s(N,\gamma)$ — количество решеток $\Gamma\in L_s(N)$ таких, что $\gamma\in\Gamma$;

$T_s(N,\gamma,\eta)$ — количество решеток $\Gamma\in L_s(N)$ таких, что $\gamma,\eta\in\Gamma$.

Другими словами, $T_s(N,\gamma)$ совпадает с количеством решений $a \in \mathbb{Z}^{s-1}(N)$ сравнения

$$a_1\gamma_1 + \ldots + a_{s-1}\gamma_{s-1} \equiv \gamma_s \pmod N,$$

а $T_s(N,\gamma,\eta)$ равно количеству решений $a \in \mathbb{Z}^{s-1}(N)$ системы сравнений

$$\begin{cases} a_1\gamma_1 + \ldots + a_{s-1}\gamma_{s-1} \equiv \gamma_s \pmod N, \\ a_1\eta_1 + \ldots + a_{s-1}\eta_{s-1} \equiv \eta_s \pmod N. \end{cases}$$

Так как N — простое, то

$$T_s(N,\gamma) = N^{s-2}, \qquad T_s(N,\gamma,\eta) = N^{s-3}. \tag{4.2}$$

Для любого натурального m и вещественного $R \geq 2$ определим множество

$$K_m(R) = \{x \in \mathbb{N}^m : \quad x_1 \cdot \ldots \cdot x_m \leq R\}.$$

Нетрудно проверить, что

$$\sum_{\gamma \in K_m(N)} \frac{1}{\gamma_1 \cdot \ldots \cdot \gamma_m} = \frac{\ln^m R}{m!} + O_m\left(\ln^{m-1} R\right).$$

Следовательно,

$$\sum_{\gamma \in K_s(R)} 1 = R \cdot \frac{\ln^{s-1} R}{(s-1)!} + O_s\left(R \cdot \ln^{s-2} R\right), \tag{4.3}$$

$$\sum_{\gamma \in K_s(R)} \gamma_1 \cdot \ldots \cdot \gamma_s = \frac{R^2}{2} \cdot \frac{\ln^{s-1} R}{(s-1)!} + O_s\left(R^2 \cdot \ln^{s-2} R\right). \tag{4.4}$$

Докажем второе неравенство из (4.1). Если $\Gamma \in \mathcal{L}_s(\mathbb{Z}, N)$, $\gamma \in \mathfrak{M}_+(\Gamma)$, то $\gamma \in K_s(N)$ по теореме Минковского о линейных формах. Поэтому, используя (4.2), (4.3), получаем

$$\sum_{\gamma \in \mathbb{N}^s} f_s(N,\gamma) \leq \sum_{\gamma \in K_s(N)} T_s(N,\gamma) = \sum_{\gamma \in K_s(N)} N^{s-2} = N^{s-1} \cdot \frac{\ln^{s-1} N}{(s-1)!} + O_s(\ln^{s-2} N).$$

Второе неравенство из (4.1) доказано.

Осталось доказать первую оценку из (4.1). Пусть $\Gamma \in \mathcal{L}_s(\mathbb{Z}, N)$, $\gamma \in \Gamma$. Положим

$$\Pi(\gamma) = \left\{\eta \in \mathbb{Z}^s \setminus \{0, \pm\gamma\} : \quad |\eta_i| \leqslant |\gamma_i|,\ i = \overline{1,s}; \quad 0 \leq \gamma_s\right\}.$$

Если $\gamma \notin \mathfrak{M}(\Gamma)$, то множество $\Pi(\gamma)$ содержит хотя бы один узел решетки Γ. Поэтому

$$f_s(N,\gamma) \geq T_s(N,\gamma) - \sum_{\eta \in \Pi(\gamma)} T_s(N,\gamma,\eta).$$

Ввиду (4.2), имеем

$$f_s(N,\gamma) \geq N^{s-2} - N^{s-3} \cdot \#\Pi(\gamma) \geq N^{s-2} - N^{s-3} \cdot \gamma_s \cdot \prod_{i=1}^{s-1}(2\gamma_i + 1).$$

Возьмем любую постоянную $\epsilon \in (0,1)$. Согласно (4.3), (4.4),

$$\sum_{\gamma \in K_s(\epsilon N)} N^{s-2} = N^{s-1}\left(\epsilon \cdot \frac{\ln^{s-1} N}{(s-1)!} + O_{s,\epsilon}\left(\ln^{s-2} N\right)\right),$$

$$\sum_{\gamma \in K_s(\epsilon N)} \left(N^{s-3} \cdot \gamma_s \cdot \prod_{i=1}^{s-1}(2\gamma_i + 1)\right) = N^{s-1}\left(2^{s-1}\frac{\epsilon^2}{2}\frac{\ln^{s-1} N}{(s-1)!} + O_{s,\epsilon}(\ln^{s-2} N)\right).$$

Следовательно,

$$\begin{aligned}\sum_{\gamma \in \mathbb{N}^s} f_s(N,\gamma) \;&\geq\; \sum_{\gamma \in K_s(\epsilon N)} f_s(N,\gamma) \geq \sum_{\gamma \in K_s(\epsilon N)} \left(N^{s-2} - N^{s-3} \cdot \gamma_s \cdot \prod_{i=1}^{s-1}(2\gamma_i + 1)\right) = \\ &= \; N^{s-1} \cdot \frac{\ln^{s-1} N}{(s-1)!}\left(\epsilon - \epsilon^2 \cdot 2^{s-2}\right) + O_{s,\epsilon}(N^{s-1}\ln^{s-1} N).\end{aligned}$$

Выбирая $\epsilon = 1/2^{s-1}$, получаем первое неравенство из (4.1). □

Следствие 4.1. *Для любого целого $s \geq 2$ справедлива оценка*

$$\frac{1}{(s-1)!} \leq \mathcal{C}(s) \leq \frac{2^s}{(s-1)!}.$$

Доказательство. Пусть $\{p_k\}$ — последовательность простых чисел, занумерованных по возрастанию. По определению,

$$\mathcal{C}(s) = \lim_{N\to\infty} \frac{E(N,s)}{\ln^{s-1} N} = \lim_{k\to\infty} \frac{E(p_k,s)}{\ln^{s-1} p_k}.$$

Осталось применить теорему 4.1. □

Глава IV
Статистические свойства многогранников Клейна

Напомним обозначения и определения. Пусть Γ — решетка из $\mathcal{L}_s(\mathbb{R})$, а $\mathcal{T}$ — целочисленно-линейный тип многогранников из $\mathbb{R}^{s-1}$. Тогда

$\mathcal{V}(\Gamma)$ — множество вершин полиэдров Клейна решетки Γ;

$\mathcal{F}(\Gamma)$ — множество компактных гиперграней полиэдров Клейна решетки Γ;

$\mathcal{F}(\Gamma, \mathcal{T})$ — множество граней из $\mathcal{F}(\Gamma)$ типа $\mathcal{T}$ (грань $F \in \mathcal{F}(\Gamma)$ принадлежит типу $\mathcal{T}$, если для любой базисной матрицы M решетки Γ многогранник $M^{-1} \cdot F$ имеет целочисленно-линейный тип $\mathcal{T}$);

TF_3 — множество допустимых типов компактных гиперграней многогранников Клейна трехмерных решеток, т.е. $\forall \mathcal{T} \in TF_3 \quad \exists \Gamma \in \mathcal{L}_3(\mathbb{R}) : \quad \mathcal{F}(\Gamma, \mathcal{T}) \neq \emptyset$.

Кроме того,

$$E_{\mathcal{T}}(N, s) = \frac{1}{\mathcal{R}_s(N)} \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z}, N)} \#\mathcal{F}(\Gamma, \mathcal{T}), \qquad E_{\mathcal{V}}(N, s) = \frac{1}{\mathcal{R}_s(N)} \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z}, N)} \#\mathcal{V}(\Gamma)$$

— среднее число граней типа $\mathcal{T}$ и вершин многогранников Клейна целочисленных s-мерных решеток определителя N.

В настоящей главы мы докажем следующие асимптотические формулы

$$E_{\mathcal{T}}(N, 3) = C_{\mathcal{T}} \cdot \ln^2 N + O_{\mathcal{T}}(\chi(N) \cdot \ln N), \tag{0.1}$$

$$E_{\mathcal{V}}(N, 3) = C_{\mathcal{V}} \cdot \ln^2 N + O(\chi(N) \cdot \ln N), \qquad N > 1, \tag{0.2}$$

где $\mathcal{T} \in TF_3$, $C_{\mathcal{T}}$ — положительная постоянная, зависящая только от $\mathcal{T}$, а $C_{\mathcal{V}}$ — абсолютная положительная постоянная. Также мы получим двусторонние оценки для $E_{\mathcal{V}}(N; s)$ в случае произвольной размерности s.

§ 1. Оценки количества элементов многогранников Клейна

Оценки количества вершин многомерных полиэдров Клейна

Пусть $N \in \mathbb{N}$, $N > 1$. В этом разделе мы докажем следующую нижнюю оценку для среднего числа вершин многогранников Клейна:

$$E_{\mathcal{V}}(N, s) \underset{s}{\gg} \ln^{s-1} N. \tag{1.1}$$

Так как любая вершина многогранника Клейна является относительным минимумом (см. [13, 24]), то для любой целочисленной решетки Γ

$$\#\mathcal{V}(\Gamma) \leq \#\mathfrak{M}(\Gamma)$$

Поэтому из неравенства (1.1) и известных оценок (0.3.2) для максимального количества относительных минимумов следуют следующие двусторонние оценки для среднего и максимального числа вершин многогранников Клейна решеток из $\mathcal{L}_s(\mathbb{Z}; N)$:

$$E_{\mathcal{V}}(N, s) \underset{s}{\asymp} \ln^{s-1} N, \qquad \max_{\Gamma \in \mathcal{L}_s(\mathbb{Z};N)} \#\mathcal{V}(\Gamma) \underset{s}{\asymp} \ln^{s-1} N. \tag{1.2}$$

Доказательство соотношения (1.1) основано на идеях [1].

Лемма 1.1. *Для любого $x = (x_1, \ldots, x_s) \in \mathbb{Z}^s \setminus \{0\}$ существует целочисленная унимодулярная матрица $S \in \mathrm{GL}_s(\mathbb{Z})$ такая, что*

$$S \cdot x = (r, 0, 0, \ldots, 0),$$

где $r =$ нод $(x_1, \ldots, x_s)$.

Доказательство вытекает, например, из следствия II.2.1.

Пусть $x \in \mathbb{Z}^s$, $r =$ нод $(x_1, \ldots, x_s)$. Определим

$$T_s(N, x) = \#\left\{\Gamma \in \mathcal{L}_s(\mathbb{Z}; N) : \quad x \in \Gamma\right\}$$

— количество решеток из $\mathcal{L}_s(\mathbb{Z}; N)$, содержащих узел x. Согласно лемме 1.1, $T_s(N, x)$ равно количеству решеток $\Gamma \in \mathcal{L}_s(\mathbb{Z}; N)$, которые содержат узел $(r, 0, \ldots, 0)$. Применяя теорему II.2.1, получаем формулу

$$T_s(N, x) = \sum_{\substack{d_1 | r, \\ d_1 \cdot \ldots \cdot d_s = N}} d_1^{s-1} \cdot d_2^{s-2} \cdot \ldots \cdot d_{s-1}, \tag{1.3}$$

где суммирование ведется по всем $(d_1, \ldots, d_s) \in \mathbb{N}^s$ таким, что $d_1 | r$ и $d_1 \cdot \ldots \cdot d_s = N$. (Если использовать обозначения теоремы 2.1, то $d_i = m_{ii}$).

Следствие 1.1. *Пусть $a = (a_1, \ldots, a_s) \in [1, +\infty)^s$. Тогда*

$$\sum_{|x_i| \leq a_i, i=\overline{1,s}} T_s(N, x) \leq 3^s \cdot \zeta(s) \cdot (a_1 \cdot \ldots \cdot a_s) \cdot \frac{\mathcal{R}_s(N)}{N},$$

где суммирование ведется по всем таким $(x_1, \ldots, x_s) \in \mathbb{Z}^s$, что $|x_i| \leq a_i$.

Доказательство. Пусть $\hat{a} = a_1 \cdot \ldots \cdot a_s$. Для любого $x \in \mathbb{Z}^s$ определим

$$r(x) = \text{нод } (x_1, \ldots, x_s).$$

Используя (1.3), получаем

$$\sum_{|x_i| \le a_i, i=\overline{1,s}} T_s(N,x) = \sum_{|x_i| \le a_i, i=\overline{1,s}} \sum_{\substack{d_1 | r(x), \\ d_1 \cdot \ldots \cdot d_s = N}} d_1^{s-1} \cdot d_2^{s-2} \cdot \ldots \cdot d_{s-1} =$$

$$= \sum_{r=1}^{\min\{a_1,\ldots,a_s\}} \left(\sum_{\substack{|x_i| \le a_i, \\ \text{нод } (x_1,\ldots,x_s)=r}} \sum_{\substack{d_1 | r, \\ d_1 \cdot \ldots \cdot d_s = N}} d_1^{s-1} \cdot d_2^{s-2} \cdot \ldots \cdot d_{s-1} \right) \le$$

$$\le \sum_{r=1}^{\min\{a_1,\ldots,a_s\}} \left(\prod_{i=1}^{s} \left(\frac{2a_i}{r} + 1 \right) \sum_{\substack{d_1 | r, \\ d_1 \cdot \ldots \cdot d_s = N}} d_1^{s-1} \cdot d_2^{s-2} \cdot \ldots \cdot d_{s-1} \right) \le$$

$$\le \sum_{r=1}^{\min\{a_1,\ldots,a_s\}} \left(\frac{3^s \cdot \hat{a}}{r^s} \sum_{\substack{d_1 | r, \\ d_1 \cdot \ldots \cdot d_s = N}} d_1^{s-1} \cdot d_2^{s-2} \cdot \ldots \cdot d_{s-1} \right) =$$

$$= 3^s \cdot \hat{a} \sum_{d_1 \cdot \ldots \cdot d_s = N} \left(d_1^{s-1} \cdot d_2^{s-2} \cdot \ldots \cdot d_{s-1} \sum_{\substack{1 \le r \le \min\{a_1,\ldots,a_s\}, \\ r \equiv 0 \pmod{d_1}}} \frac{1}{r^s} \right) \le$$

$$\le 3^s \cdot \hat{a} \sum_{d_1 \cdot \ldots \cdot d_s = N} d_1^{s-1} \cdot d_2^{s-2} \cdot \ldots \cdot d_{s-1} \sum_{r'=1}^{\infty} \frac{1}{d_1^s \cdot r'^s} =$$

$$= 3^s \cdot \hat{a} \cdot \zeta(s) \sum_{d_1 \cdot \ldots \cdot d_s = N} \frac{d_2^{s-1} \cdot d_3^{s-2} \cdot \ldots \cdot d_s}{N} = 3^s \cdot \hat{a} \cdot \zeta(s) \cdot \frac{R_s(N)}{N}.$$

□

Для любого натурального t определим множество

$$\mathbb{Z}_t^s = \left\{ n \in \mathbb{Z}_+^s : \ \ n_1 + \ldots + n_s = t \right\}.$$

Кроме того, если $\lambda, \xi \in (1, \infty)$, $k \in \mathbb{Z}_+^s$, то

$$\mathcal{P}_{\lambda,\xi}(k) = \left\{ x \in \mathbb{R}^s : \quad |x_1| \le \xi \cdot \lambda^{k_1}, \ \ |x_j| \le \lambda^{k_j}, j = \overline{2,s} \right\}.$$
$$\mathcal{S}_{t,\lambda,\xi} = \bigcup_{k \in \mathbb{Z}_t^s} \mathcal{P}_{\lambda,\xi}(k).$$

Лемма 1.2. *Пусть X – конечное множество из $\mathbb{R}^s$. Тогда для любых $t \in \mathbb{N}$, $\lambda, \xi \in (1, \infty)$ справедлива оценка*

$$\#(X \cap \mathcal{S}_{t,\lambda,\xi}) \ge \sum_{k \in \mathbb{Z}_t^s} \#\left(X \cap P_{\lambda,\xi}(k)\right) - \sum_{l=1}^{s-1} C_{s-1}^l \sum_{k \in \mathbb{Z}_{t-l}^s} \#(X \cap P_{\lambda,\xi}(k)),$$

где $C_{s-1}^l = (s-1)!/(l!(s-1-l)!)$ — биномиальный коэффициент.

Лемма является тривиальным следствием из [1, лемма 2].

Теорема 1.1. *Пусть каждой решетке $\Gamma \in \mathcal{L}_s(\mathbb{Z}; N)$ поставлено в соответствие конечное множество $X(\Gamma) \subset \Gamma \setminus \{0\}$, причем существует такая положительная постоянная $c > 0$, что из условий*

$$y \in \mathbb{R}_+^s, \quad y_1 \cdot \ldots \cdot y_s \geq c \cdot N,$$

вытекает

$$\forall \Gamma \in \mathcal{L}_s(\mathbb{Z}; N) \quad \exists \gamma \in X(\Gamma): \qquad |\gamma_i| \leq y_i, \quad i = \overline{1, s}.$$

Тогда справедлива оценка

$$\frac{1}{\mathcal{R}_s(N)} \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z};N)} \# X(\Gamma) \underset{s,c}{\gg} \ln^{s-1} N.$$

Доказательство. Пусть $c_s = 3^s \cdot \zeta(s) \cdot c$. Возьмем любую постоянную λ такую, что

$$1 + c_s \cdot \left(1 - \left(1 + \frac{1}{\lambda}\right)^{s-1}\right) > 0, \qquad \lambda > 1. \tag{1.4}$$

Подчеркнем, что λ зависит только от c и s. Положим

$$t = [\log_\lambda N], \quad \xi = \frac{cN}{\lambda^t}.$$

Не умаляя общности, считаем, что $t \geq 1$ (т.е. $N \geq \lambda$). Тогда для любого $k \in \mathbb{Z}_t^s$

$$\begin{array}{l} \xi \cdot \lambda^{k_1} \cdot \lambda^{k_2} \cdot \ldots \cdot \lambda^{k_s} = c \cdot N, \\ \max\left\{\xi \cdot \lambda^{k_1},\ \lambda^{k_2}, \ldots, \lambda^{k_s}\right\} \geq 1. \end{array} \tag{1.5}$$

Используя лемму 1.2, получаем

$$\sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z};N)} \# X(\Gamma) \geq \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z};N)} \# \left(X(\Gamma) \cap \mathcal{S}_{t,\lambda,\xi}\right) \geq Q_s'(N) - Q_s''(N),$$

где

$$\begin{aligned} Q_s'(N) &= \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z};N)} \sum_{k \in \mathbb{Z}_t^s} \# \left(X(\Gamma) \cap P_{\lambda,\xi}(k)\right), \\ Q_s''(N) &= \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z};N)} \sum_{l=1}^{s-1} C_{s-1}^l \sum_{k \in \mathbb{Z}_{t-l}^s} \# \left(X(\Gamma) \cap P_{\lambda,\xi}(k)\right). \end{aligned}$$

Из (1.5) и условий теоремы вытекает, что для любых $k \in \mathbb{Z}_t^s$, $\Gamma \in \mathcal{L}_s(\mathbb{Z}; N)$ найдется такой узел $\gamma \in X(\Gamma)$, что

$$|\gamma_1| \leq \xi \cdot \lambda^{k_1}, \quad |\gamma_j| \leq \lambda^{k_j}, \quad j = \overline{2, s}.$$

Поэтому

$$Q_s'(N) \geq \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z};N)} \sum_{k \in \mathbb{Z}_t^s} 1 = \mathcal{R}_s(N) \cdot \# \mathbb{Z}_t^s = \mathcal{R}_s(N) \cdot C_{t+s-1}^{s-1} \geq \frac{t^{s-1}}{(s-1)!} \cdot \mathcal{R}_s(N)$$

Используя следствие 1.1 и соотношения (1.5), получаем

$$\begin{aligned} Q''_s(N) &\le \sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};N)} \sum_{l=1}^{s-1} C_{s-1}^l \sum_{k\in\mathbb{Z}^s_{t-l}} \#\left(\Gamma\cap P_{\lambda,\xi}(k)\right) \le \\ &\le \sum_{l=1}^{s-1} C_{s-1}^l \sum_{k\in\mathbb{Z}^s_{t-l}} 3^s\cdot\zeta(s)\cdot\frac{\mathcal{R}_s(N)}{N}\cdot\xi\cdot\lambda^{k_1}\cdot\lambda^{k_2}\cdot\ldots\cdot\lambda^{k_s} = \\ &= c_s\cdot\sum_{l=1}^{s-1} C_{s-1}^l \sum_{k\in\mathbb{Z}^s_{t-l}} \frac{\mathcal{R}_s(N)}{\lambda^l} = \\ &= c_s\cdot\mathcal{R}_s(N)\cdot\sum_{l=1}^{s-1} C_{s-1}^l\cdot\frac{C_{t+s-l-1}^{s-1}}{\lambda^l} \le \\ &\le c_s\cdot\mathcal{R}_s(N)\cdot\frac{(t+s)^{s-1}}{(s-1)!}\cdot\sum_{l=1}^{s-1} C_{s-1}^l\frac{1}{\lambda^l} = \\ &= c_s\cdot\mathcal{R}_s(N)\cdot\frac{(t+s)^{s-1}}{(s-1)!}\cdot\left(\left(1+\frac{1}{\lambda}\right)^{s-1}-1\right). \end{aligned}$$

Из последнего соотношения и асимптотической формулы

$$(t+s)^{s-1} = t^{s-1} + O_s(t^{s-2}),$$

вытекает, что

$$Q''_s(N) \le \frac{\mathcal{R}_s(N)}{(s-1)!}\cdot c_s\cdot t^{s-1}\left(\left(1+\frac{1}{\lambda}\right)^{s-1}-1\right) + O_{s,\lambda}\left(\mathcal{R}_s(N)\cdot t^{s-2}\right).$$

Следовательно,

$$\begin{aligned} \sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};N)} \#X(\Gamma) &\ge Q'_s(N) - Q''_s(N) \ge \\ &\ge \frac{R_s(N)\cdot t^{s-1}}{(s-1)!}\left(1+c_s-c_s\left(1+\frac{1}{\lambda}\right)^{s-1}\right) + O_{s,\lambda}\left(R_s(N)\cdot t^{s-2}\right). \end{aligned}$$

Учитывая условие (1.4) и определение t, получаем утверждение теоремы. □

Согласно теореме Минковского о линейных формах, множество относительных минимумов $X(\Gamma) = \mathfrak{M}(\Gamma)$ удовлетворяет условиям теоремы 1.1, где $c = 1$. Докажем, что множество вершин $X(\Gamma) = \mathcal{V}(\Gamma)$ также удовлетворяет условиям теоремы 1.1.

Лемма 1.3. *Пусть $\Gamma\in\mathcal{L}_s(\mathbb{R})$. Тогда для любого ненулевого узла γ решетки Γ найдется такая вершина $v\in\mathcal{V}(\Gamma)$, что*

$$|v_i| \le s\cdot|\gamma_i|, \quad i = \overline{1,s}.$$

Доказательство. Не умаляя общности считаем, что $\gamma \in [0,+\infty)^s$. Пусть x – точка пересечения отрезка $[0,\gamma]$ и границы полиэдра Клейна решетки Γ. Согласно теореме Каратеодори (см., например, [30]) точку x можно представить в виде

$$x = \sum_{i=1}^{s} \lambda_i v^{(i)},$$

где

$$\lambda_i \in [0,1], \quad v^{(i)} \in \mathcal{V}(\Gamma) \cap [0,+\infty)^s, \quad i = \overline{1,s}; \qquad \sum_{i=1}^{s} \lambda_i = 1.$$

Пусть $\lambda_k = \max\{\lambda_1, \ldots, \lambda_s\}$. Тогда $\lambda_k \geq 1/s$, и поэтому

$$x_i \geq \lambda_k \cdot v_i^{(k)} \geq \frac{1}{s} v_i^{(k)}, \quad i = \overline{1,s}.$$

Вершина $v = v^{(k)}$ удовлетворяет требуемым условиям. □

Следствие 1.2. *Пусть $\Gamma \in \mathcal{L}_s(\mathbb{Z}; N)$. Тогда для любой точки $y \in \mathbb{R}^s_+$, удовлетворяющей условию*

$$y_1 \cdot \ldots \cdot y_s \geq s^s \cdot N,$$

существует такая вершина $v \in \mathcal{V}(\Gamma)$, что

$$|v_i| \leq y_i, \quad i = \overline{1,s}.$$

Доказательство. Согласно теореме Минковского о линейных формах найдется ненулевой узел $\gamma \in \Gamma$ такой, что

$$|\gamma_i| \leq \frac{1}{s} \cdot y_i, \quad i = \overline{1,s}.$$

Осталось воспользоваться леммой 1.3. □

Согласно следствию 1.2 множество вершин $X(\Gamma) = \mathcal{V}(\Gamma)$ удовлетворяет условиям теоремы 1.1, в которых $c = s^s$. Поэтому имеет место следующий результат.

Следствие 1.3. *Для любого целого $N > 1$ выполняется оценка (1.1).*

Оценки количества элементов трехмерных полиэдров Клейна

Возьмем любую трехмерную целочисленную решетку $\Gamma \in \mathcal{L}_3(\mathbb{Z})$. В силу симметрии, ограничимся рассмотрение многогранника Клейна $K_+(\Gamma)$, лежащего в угле $[0,+\infty)^3$. Пусть $f_k(\Gamma)$ — количество k-мерных граней $K_+(\Gamma)$ (т.е. f_0 — количество вершин, f_1 — ребер и f_2 — гиперграней).

Так как решетка Γ целочисленная, то все вершины $K_+(\Gamma)$ лежат внутри симплекса

$$S = \{x \in [0,+\infty)^3 : x_1 + x_2 + x_3 \leq D\},$$

где D — некоторое достаточно большое число (например, $D > \det\Gamma$). Рассмотрим множество $K' = S \cap K_+(\Gamma)$. Оно является выпуклым трехмерным многогранником,

т.е. K' — выпуклая оболочка конечного числа точек. Пусть f'_k — количество k-мерных граней K'. Хорошо известны следующие оценки (см., например, [68])

$$\frac{3f'_0}{2} \le f'_1 \le 3f'_0 - 6, \qquad \frac{f'_0}{2} + 2 \le f'_2 \le 2f'_0 - 4. \tag{1.6}$$

Многогранник K' содержит все компактные грани полиэдра Клейна $K'(\Gamma)$. Кроме того, величины $f_k = f_k(\Gamma)$ и f'_k связаны соотношениями:

$$f'_0 = f_0 + 3, \quad f'_1 = f_1 + 3, \quad f'_2 = f_2 + 1.$$

Поэтому согласно (1.6)

$$\frac{3(f_0+1)}{2} \le f_1 \le 3 \cdot f_0, \qquad \frac{f_0+5}{2} \le f_2 \le 2 \cdot f_0 + 1. \tag{1.7}$$

Значит, из (1.2) вытекает следующий результат.

Следствие 1.4. *Справедливы следующие оценки для максимального и среднего числа вершин, ребер и граней многогранников Клейна трехмерных целочисленных решеток:*

$$\max_{\Gamma\in\mathcal{L}_3(\mathbb{Z};N)} f_k(\Gamma) \asymp \ln^2 N, \quad \frac{1}{\mathcal{R}_3(N)} \sum_{\Gamma\in\mathcal{L}_3(\mathbb{Z};N)} f_k(\Gamma) \asymp \ln^2 N, \quad k = 0,1,2 \tag{1.8}$$

при любом целом $N > 1$.

Есть основания полагать, что справедливо такое утверждение.

Гипотеза. *Справедливы следующие оценки для максимального и среднего числа k-мерных граней многогранников Клейна s-мерных целочисленных решеток:*

$$\max_{\Gamma\in\mathcal{L}_s(\mathbb{Z};N)} f_k(\Gamma) \underset{s}{\asymp} \ln^{s-1} N, \quad \frac{1}{\mathcal{R}_s(N)} \sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};N)} f_k(\Gamma) \underset{s}{\asymp} \ln^{s-1} N, \quad k = \overline{0, s-1} \tag{1.9}$$

при любом целом $N > 1$.

Разумеется, некоторые из оценок (1.9) можно вывести из (1.2). Например, удвоенное количество 1-мерных граней s-мерного выпуклого ограниченного многогранника, не меньше, чем количество вершин, умноженное на s. Поэтому

$$\max_{\Gamma\in\mathcal{L}_s(\mathbb{Z};N)} f_1(\Gamma) \underset{s}{\gg} \ln^{s-1} N, \quad \frac{1}{\mathcal{R}_s(N)} \sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};N)} f_1(\Gamma) \underset{s}{\gg} \ln^{s-1} N.$$

Однако неравенств (1.2) не хватает для того, чтобы в полном объеме доказать оценки (1.9) при $s \ge 4$, используя только общую теорию выпуклых многогранников. Например, оценка для для максимального числа граней размерности $k < [s/2]$, вытекающая из теоремы о максимальном числе граней [6, 123], имеет вид

$$f_k(\Gamma) \underset{s}{\ll} (f_0(\Gamma))^{k+1} \underset{s}{\ll} (\ln^{s-1} N)^{k+1} \quad \text{при } \Gamma \in \mathcal{L}_s(\mathbb{Z}; N)$$

и является завышенной.

§ 2. Среднее количество граней фиксированного типа

В этом параграфе мы докажем асимптотическую формулу (0.1) для среднего числа граней трехмерных полиэдров Клейна.

Определение 2.1. Многоугольник (многогранник) с вершинами в узлах решетки Γ будем называть *пустым относительно* Γ, если он не содержит точек Γ, кроме своих вершин.

Определение 2.2. Пирамиду (с отмеченной вершиной) с вершинами в узлах решетки Γ будем называть *почти пустой относительно* Γ, если она не содержит точек Γ, отличных от вершины и точек основания.

Если $\Gamma = \mathbb{Z}^3$, то фразу «относительно Γ» в определениях 2.1, 2.2 опускаем.

Введем еще одно важное обозначение. Пусть $\Gamma \in \mathcal{L}_3(\mathbb{R})$, плоскость π содержит хотя бы три линейно независимых узла решетки Γ. Возьмем любые три линейно независимых узла $a, b, c \in \Gamma \cap \pi$ таких, что треугольник с вершинами в точках a, b, c является пустым относительно Γ. Обозначим

$$d(\Gamma; \pi) = \frac{|\det M(a, b, c)|}{\det \Gamma}$$

— индекс подрешетки, порожденной a, b, c. Напомним, что $M(a, b, c)$ — матрица со столбцами a, b, c. Если F — грань многогранника Клейна решетки Γ, содержащаяся в плоскости π_F, то полагаем

$$d(\Gamma; F) = d(\Gamma; \pi_F).$$

Замечание 2.1. Если M — базисная матрица Γ, то величина $d(\Gamma; \pi_F)$ совпадает с целочисленным расстоянием от начала координат до плоскости $M^{-1} \cdot \pi_F$. Значит, $d(\Gamma; F)$ однозначно определяется типом грани.

Минимальная окрестность грани

Пусть F — многоугольник из $[0, +\infty)^3$ с вершинами в узлах решетки $\Gamma \in \mathcal{L}_3(\mathbb{R})$. Через π_F обозначим плоскость, проходящую через F. Она делит $\mathbb{R}^3$ два открытых полупространства, которые мы обозначим S_F^+ и S_F^- так, что S_F^- содержит начало координат. По определению, множество F является гранью многогранника Клейна решетки Γ, если и только если любой ненулевой узел Γ из $S_F^- \cup \pi_F \setminus F$ имеет хотя бы одну отрицательную координату. Докажем, что достаточно рассматривать некоторое конечное множество узлов.

Определим множество $X = X(\Gamma; F)$ следующим образом. Пусть $d = d(\Gamma; \pi_F)$. Если $d = 1$, то полагаем $X = \pi_F \cap \Gamma$. Пусть $d > 1$. Все точки решетки Γ лежат на плоскостях, параллельных π_F, которые расположены на одинаковом расстоянии друг от друга. Занумеруем такие плоскости, лежащие в S_F^- через π_{d-1}, π_{d-2},... по возрастанию расстояния до $\pi_d = \pi_F$. Тогда π_0 проходит через начало координат. Положим

$$X = \bigcup_{r=1}^{d} \frac{d}{r} \cdot (\Gamma \cap \pi_r),$$

т.е. X состоит из узлов $\gamma \in \Gamma \cap \pi_F$ и точек пересечения π_F с прямыми, проходящими через начало координат и узлы решетки Γ, лежащие между плоскостями π_0 и $\pi_F = \pi_d$.

Определение 2.3. Если X — дискретное, а F — выпуклое замкнутое множество из $\mathbb{R}^s$, то множество

$$P(X,F)=\left\{u\in X\setminus F:\quad \Big(\operatorname{conv}\,(F\cup\{u\})\setminus F\Big)\cap X=\{u\}\right\},$$

будем называть *минимальной X-окрестностью F.*

Лемма 2.1. *Пусть F — многоугольник из $[0,+\infty)^3$ с вершинами в узлах решетки $\Gamma\in\mathcal{L}_3(\mathbb{R})$, $X=X(\Gamma;F)$ и $P=P(X;F)$ — минимальная X-окрестность F.*

Тогда F является гранью многогранника Клейна решетки Γ, если и только если выполняются следующие условия:

$$P\cap[0,+\infty)^3=\emptyset, \tag{2.1}$$

$$\begin{array}{l}\text{пирамида } \operatorname{conv}(F\cup\{0\}) \text{ с основанием } F\\ \text{является почти пустой относительно } \Gamma.\end{array} \tag{2.2}$$

Доказательство. Пусть F является гранью многогранника Клейна. Тогда любой ненулевой узел Γ из $(S_F^-\cup\pi_F)\setminus F$ имеет хотя бы одну отрицательную координату и, значит, выполняются (2.1), (2.2).

Пусть выполняются условия (2.1), (2.2), $d=d(\Gamma;F)$, $\pi_F=\pi_d$ — плоскость, проходящая через F. Докажем, что F является гранью полиэдра Клейна решетки Γ. Возьмем любой ненулевой узел $u\in\Gamma\cap(S_F^-\cup\pi_F)\setminus F$. Нужно показать, что $u\notin[0,+\infty)^3$. Имеем $u\in\pi_r$, где $r\le d$. Отдельно рассмотрим два случая.

1. Пусть $1\le r\le d$. Тогда $\tilde u=(d/r)\cdot u\in X$. Согласно (2.2) $\tilde u\notin F$. Значит, существует точка $v\in P$, принадлежащая множеству $\operatorname{conv}(F\cup\{\tilde u\})$. Если $u\in[0,+\infty)^3$, то $\tilde u\in[0,+\infty)^3$ и $v\in[0,+\infty)^3$. Противоречие с (2.1).

2. Пусть $r\le 0$. Из выше доказанного вытекает, что

$$\Gamma\cap\pi_F\cap[0,+\infty)^3=\Gamma\cap F.$$

Это возможно только в случае, когда плоскость π_F пересекает координатные оси в точках вида $(\theta_1,0,0)$, $(0,\theta_2,0)$, $(0,0,\theta_1)$, где $\theta_i>0$. Тогда любая из плоскостей π_r с $r\le 0$ не содержит точек из $[0,+\infty)^3\setminus\{0\}$. Значит, $u\notin[0,+\infty)^3$. □

Конечность минимальной окрестности

Лемма 2.2. *Пусть $t\in(1,+\infty)$, $\Gamma'\in\mathcal{L}_2(\mathbb{R})$. Возьмем любой треугольник $\Delta\subset\mathbb{R}^2$ такой, что две вершины Δ принадлежат Γ', а оставшаяся содержится в $t\Gamma'$ и Δ не содержит других точек множества $\Gamma'\cup(t\Gamma')$. Тогда*

$$\operatorname{mes}\Delta\le\frac{[t]+1}{2}\cdot\det\Gamma',$$

где $[t]$ — целая часть t.

Доказательство. Обозначим вершины Δ через a,b,c так, что

$$a,b\in\Gamma';\quad c\in t\Gamma'.$$

Пусть W — полоса, ограниченная прямыми l_1, l_2, где l_1 проходит через точку a параллельно отрезку $[c, b]$, а l_2 проходит через $[c, b]$. При этом считаем, что $l_1 \cap W = \emptyset$, $l_2 \subset W$.

Пусть W_+ — «половина» полосы W, состоящая из точек $x \in W$ таких, что x и b лежат по разные стороны от прямой, проходящей через a и c.

Так как $a, b \in \Gamma'$, то W_+ содержит бесконечно много точек решетки Γ'. Возьмем любой узел $d \in \Gamma' \cap W_+$ такой, что треугольник Δ_{abd} (с вершинами в точках a, b, d) пустой относительно Γ'. Рассмотрим точки $d_k = a + k(d - a)$, $k \in \mathbb{N}$. Они лежат на прямой, проходящей через d, a. Пусть n — наименьшее натуральное такое, что отрезок $[a, d_n]$ пересекается с прямой, проходящей через точку c параллельно $[a, b]$. Рассмотрим треугольник Δ_n с вершинами в a, b, d_n. Имеем

$$\operatorname{mes} \Delta \le \operatorname{mes} \Delta_n = n \cdot \operatorname{mes} \Delta_{abd} = n \cdot \frac{\det \Gamma'}{2}.$$

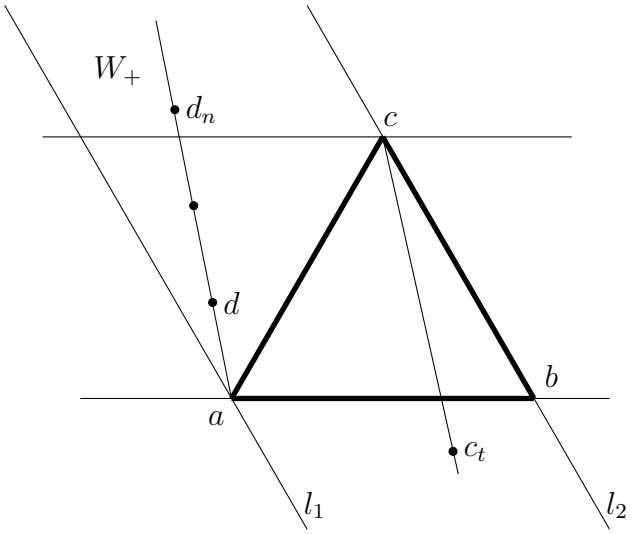


Рис. 1

Осталось оценить n. Рассмотрим точку

$$c_t = c - t(d - a) \in t\Gamma'.$$

Если $t \le n - 1$, то c_t принадлежит треугольнику Δ и не совпадает с его вершинами. Это противоречит условиям леммы. Значит, $n < t + 1$ и поэтому

$$\operatorname{mes} \Delta \le n \cdot \frac{\det \Gamma'}{2} \le ([t] + 1) \cdot \frac{\det \Gamma'}{2}.$$

□

Следствие 2.1. *Пусть* $t_1 = 1$ *и* $t_i \in (1, +\infty)$, $i = \overline{2, d}$. *Определим*

$$X = \bigcup_{i=1}^{d} (t_i \mathbb{Z}^2).$$

Пусть F *— выпуклый многоугольник с вершинами из* $\mathbb{Z}^2$, *причем* $F \cap X = F \cap \mathbb{Z}^2$. *Тогда минимальная* X*-окрестность* F *является конечным множеством.*

Доказательство. Пусть $P = P(X; F)$ — минимальная X-окрестность F. Достаточно доказать, что множество P ограниченное.

Пусть B — произвольный круг, содержащийся в F с центром в точке x_0 радиуса $R > 0$. Возьмем любую точку $x \in P$ и положим

$$U_F = \operatorname{conv}(F \cup \{x\}), \quad U_B = \operatorname{conv}(B \cup \{u\}).$$

Тогда $U_B \subset U_F$. Кроме того, $x \in t_j\mathbb{Z}^2$ с некоторым $j \in \{1, \dots, d\}$. Пусть $r = \#(\mathbb{Z}^2 \cap \partial F)$. Рассмотрим многоугольник $U_F \setminus F$. Он состоит из не более, чем r треугольников Δ, каждый из которых удовлетворяет условиям: 1) x — вершина Δ; 2) две остальные вершины Δ являются точками $F \cap X$ и поэтому принадлежат $\mathbb{Z}^2$; 3) треугольник Δ не содержит других точек множества $\mathbb{Z}^2 \cup (t_j\mathbb{Z}^2)$. Согласно лемме 2.2 площадь каждого такого треугольника, не больше, чем $[t_j + 1]/2$. Значит, $\operatorname{mes}(U_F \setminus F) \le r[t_j + 1]/2$, поэтому

$$R|x - x_0| + \frac{\pi R^2}{2} = \operatorname{mes} U_B \le \operatorname{mes} U_F \le \operatorname{mes} F + r[t_j + 1]/2.$$

Множество P ограниченное. Лемма доказана. □

Параметризация граней

Возьмем любой тип $\mathcal{T} \in TF_3$. Зафиксируем любой многоугольник $T \in \mathcal{T}$, который параллелен плоскости $x_3 = 0$, а также упорядоченную тройку целочисленных точек (α, β, γ) таких, что треугольник с вершинами в точках α, $(\beta + \alpha)$, $(\gamma + \alpha)$ содержится в T и является пустым, т.е.

$$\mathbb{Z}^3 \cap \operatorname{conv}\Big\{\alpha, (\alpha + \beta), (\alpha + \gamma)\Big\} = \Big\{\alpha, (\alpha + \beta), (\alpha + \gamma)\Big\} \subset T.$$

Не умаляя общности считаем, что $\det M(\alpha, \beta, \gamma) > 0$. Пусть d_1, d_2, d_3 — алгебраические дополнения к элементам последней строки матрицы $M(\alpha, \beta, \gamma)$ со столбцами α, β, γ. Определим

$$\tilde{\alpha} = \frac{\alpha + d_2\beta + d_3\gamma}{d}. \tag{2.3}$$

Нетрудно заметить, что

$$M(\alpha, \beta, \gamma) = \begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ d & 0 & 0 \end{pmatrix}, \quad d_1 = 1,$$

где $d = d(\mathcal{T})$ — целочисленное расстояние от плоскости, содержащей многоугольник типа $\mathcal{T}$, до начала координат. Поэтому $\tilde{\alpha} = (0, 0, 1)$ и тройка $\{\tilde{\alpha}, \beta, \gamma\}$ образует базис решетки $\mathbb{Z}^3$.

Так как T, α, β, γ фиксированы, то далее пишем

$$T = T(\mathcal{T}), \;\; (\alpha, \beta, \gamma) = (\alpha, \beta, \gamma)(\mathcal{T}), \;\; d_2 = d_2(\mathcal{T}), \;\; d_3 = d_3(\mathcal{T}),$$

имея в виду, что эти объекты однозначно определяются по типу $\mathcal{T}$.

Определим множество

$$X(\mathcal{T}) = \bigcup_{r=1}^{d} \frac{d}{r} \cdot \mathbb{Z}^3_r,$$

где $\mathbb{Z}^3_r$ — множество точек из $\mathbb{Z}^3$, у которых третья координата равна r.

Так как $\tilde{\alpha}, \beta, \gamma$ образуют базис $\mathbb{Z}^3$, причем $\tilde{\alpha}_3 = 1$, $\beta_3 = \gamma_3 = 0$, то $X(\mathcal{T})$ состоит из точек $x(r,n,k)$ следующего вида

$$x(r,n,k) = d \cdot \left(\tilde{\alpha} + \frac{n}{r} \cdot \beta + \frac{k}{r} \cdot \gamma \right), \qquad r \in \mathbb{Z} \cap [1,d], \quad n,k \in \mathbb{Z}.$$

Пусть $P(\mathcal{T})$ — минимальная $X(\mathcal{T})$-окрестность множества T. Так как $\mathcal{T} \in TF_3$, то пирамида с основанием T и вершиной в начале координат является почти пустой. Поэтому $X(\mathcal{T}) \cap T = \mathbb{Z}^3 \cap T$ и, используя лемму 2.2, получаем

$$\#P(\mathcal{T}) = O_{\mathcal{T}}(1). \tag{2.4}$$

Определим множества $J(\mathcal{T}) \subset \mathbb{Z}^2$, $J_P(\mathcal{T}) \subset \mathbb{Z}^3$, удовлетворяющие условиям

$$\begin{aligned} \mathbb{Z}^3 \cap T &= \{\alpha + n\beta + k\gamma : \ (n,k) \in J(\mathcal{T})\}, \\ P(\mathcal{T}) &= \{x(r,n,k) : \ (r,n,k) \in J_P(\mathcal{T})\}. \end{aligned}$$

Возьмем любую решетку $\Gamma \in \mathcal{L}_3(\mathbb{R})$ и грань $F \in \mathcal{F}(\Gamma; \mathcal{T})$, лежащую в угле $[0,+\infty)^3$. Согласно определению типа грани существует базисная матрица M решетки Γ такая, что $M^{-1} \cdot F = T$. Обозначим через $\Lambda(\Gamma; F)$ множество упорядоченных троек $(a,b,c) \in \Gamma^3$, для каждой из которых существует такая базисная матрица M решетки Γ, что

$$\begin{gathered} M^{-1} \cdot F = T, \\ M^{-1} \cdot a = \alpha, \quad M^{-1} \cdot b = \beta, \quad M^{-1} \cdot c = \gamma. \end{gathered} \tag{2.5}$$

Нетрудно заметить, что величина $\#\Lambda(\Gamma; F)$ зависит только от $\mathcal{T}$, а именно,

$$\#\Lambda(\Gamma; F) = \nu(\mathcal{T}), \tag{2.6}$$

где $\nu(\mathcal{T})$ — количество матриц $S \in \mathrm{GL}_3(\mathbb{Z})$ таких, что

$$S \cdot T = T, \quad S \cdot \{\alpha, \beta, \gamma\} = \{\alpha, \beta, \gamma\}.$$

Если базисная матрица M решетки Γ удовлетворяет (2.5), то

$$\begin{aligned} X(\Gamma; F) &= M \cdot X(\mathcal{T}), \\ P(X; F) &= M \cdot P(\mathcal{T}) = \left\{ d \left(\tilde{a} + \frac{n}{r} \cdot b + \frac{k}{r} \cdot c \right) : \ (r,n,k) \in J_P(\mathcal{T}) \right\}, \\ F &= M \cdot T = \left\{ (a + nb + kc) : \ (n,k) \in J(\mathcal{T}) \right\}, \end{aligned} \tag{2.7}$$

где $P(X; F)$ — минимальная $X(\Gamma; F)$-окрестность грани F.

Лемма 2.3. *Следующие утверждения эквивалентны.*

(a) $\Gamma \in \mathcal{L}_3(\mathbb{R})$, $F \in \mathcal{F}(\Gamma; \mathcal{T})$, $F \subset [0,+\infty)^3$, $(a,b,c) \in \Lambda(\Gamma; F)$.

(б) Линейно-независимые векторы $a, b, c \in \mathbb{R}^3$ удовлетворяют условиям

$$F = \operatorname{conv}\left\{a + nb + kc : \ \ (n,k) \in J(\mathcal{T})\right\} \subset [0,+\infty)^3, \tag{2.8}$$

$$\left(\tilde{a} + \frac{n}{r}\cdot b + \frac{k}{r}\cdot c\right) \notin [0,+\infty)^3 \ \textit{при}\ (r,n,k) \in J_P(\mathcal{T}), \tag{2.9}$$

а Γ — решетка с базисом $\{\tilde{a}, b, c\}$, где

$$\tilde{a} = \frac{a + d_2 b + d_3 c}{d}. \tag{2.10}$$

Доказательство. Пусть выполняется (а). Из (2.5), (2.3) вытекает, что $\{\tilde{a}, b, c\}$ — базис Γ. Соотношения (2.8) следуют из (2.7) и условия $F \subset [0,+\infty)^3$, а (2.9) — из (2.7) и леммы 2.1.

Пусть выполняется (б). Тогда справедливы соотношения (2.7). Докажем, что F — грань многогранника Клейна решетки Γ. Для этого достаточно проверить выполнение условий (2.1), (2.2). Соотношения (2.1) вытекает из (2.7) и (2.9). Докажем (2.2). Пусть M — базисная матрица Γ. Из определений F и $J(\mathcal{T})$ вытекает, что $M^{-1}\cdot F$ принадлежит целочисленно-линейному типу $\mathcal{T}$. Так как $\mathcal{T} \in TF_3$, то пирамида с основанием $M^{-1}\cdot F$ и вершиной в начале координат почти пустая. Значит, выполняется (2.2). Применяя лемму 2.1, получаем $F \in \mathcal{F}(\Gamma;\mathcal{T})$. Условие $(a,b,c) \in \Lambda(\Gamma;F)$ следует из определений Γ, F и $J(\mathcal{T})$. □

Замечание 2.2. Если выполняется условие (а) леммы 2.3 и $\Gamma \in \mathcal{L}_3(\mathbb{Z};N)$, то

$$a,b,c \in \mathbb{Z}^3, \quad |\det M(a,b,c)| = d\cdot N, \qquad (a + d_2 b + d_3 c) \in d\mathbb{Z}^3. \tag{2.11}$$

Если выполняется условие (б) и (2.11), то $\Gamma \in \mathcal{L}_3(\mathbb{Z};N)$.

Определим множество $U_+(N;\mathcal{T})$, состоящее из пар (Γ, F), где $\Gamma \in \mathcal{L}_3(\mathbb{Z};N)$, а $F \in \mathcal{F}(\Gamma;\mathcal{T})$, причем $F \subset [0,+\infty)^3$. Тогда

$$E_{\mathcal{T}}(N,3) = 2^3 \cdot \frac{\#U_+(N;\mathcal{T})}{\#\mathcal{L}_3(\mathbb{Z};N)}. \tag{2.12}$$

Будем использовать следующие матричные множества:

$$\begin{aligned} \Omega_{\mathcal{T}} &= \left\{M(a,b,c) \in \mathrm{M}_3(\mathbb{R}) : \text{ выполняются (2.8), (2.9)}\right\} \\ \omega_{\mathcal{T}}(N) &= \left\{M(a,b,c) \in \Omega_{\mathcal{T}} : \text{ выполняются (2.11)}\right\}. \end{aligned}$$

Следствие 2.2. *Для любых $N \in \mathbb{N}$, $\mathcal{T} \in TF_3$ справедлива формула*

$$\#U_+(N;\mathcal{T}) = \frac{1}{\nu(\mathcal{T})}\cdot \#\omega_{\mathcal{T}}(N). \tag{2.13}$$

Доказательство. Для каждой пары $(\Gamma, F) \in U_+(N;\mathcal{T})$ определим

$$\tilde{\Lambda}(\Gamma;F) = \{M(a,b,c) : (a,b,c) \in \Lambda(\Gamma;F)\}.$$

Согласно лемме 2.3 и замечанию 2.2

$$\bigcup_{(\Gamma,F)\in U_+(N;\mathcal{T})} \tilde{\Lambda}(\Gamma;F) = \omega_{\mathcal{T}}(N).$$

Если $(\Gamma_1,F_1) \neq (\Gamma_2,F_2)$, $(\Gamma_i,F_i) \in U_+(N;\mathcal{T})$, то $\Lambda(\Gamma_1;F_1) \cap \Lambda(\Gamma_2;F_2) = \emptyset$. Поэтому, учитывая (2.6), получаем

$$\#\omega_{\mathcal{T}}(N) = \sum_{(\Gamma;F)\in U_+(N;\mathcal{T})} \#\tilde{\Lambda}(\Gamma;F) = \nu(\mathcal{T}) \cdot \#U_+(N;\mathcal{T}).$$

□

Вычисление $\#\omega_{\mathcal{T}}(N)$ и окончательная формула

Покажем, что для вычисления $\#\omega_{\mathcal{T}}(N)$ можно применить следствие II.1.1. Очевидно, что множество $\Omega = \Omega_{\mathcal{T}}$ удовлетворяет условию (А). Осталось проверить выполнение (Б').

Лемма 2.4. *Пусть $\Gamma \in \mathcal{L}_3(\mathbb{R})$, минимумы $a,b,c \in \mathfrak{M}(\Gamma) \cap [0,+\infty)^3$ являются базисом Γ, причем*

$$a_1 \geq \max\{b_1,c_1\}; \quad b_2 \geq \max\{a_2,c_2\}; \quad c_3 \geq \max\{a_3,b_3\}.$$

Тогда $a_1b_2c_3 \ll \det\Gamma$.

Доказательство. Если минимум $v \in \mathfrak{M}(\Gamma)$ и ненулевой узел $u \in \Gamma$ имеют неотрицательные координаты, то существует такой номер k, что $u_k \geq 2v_k$ (в противном случае узел $(u-v)$ противоречит условию $v \in \mathfrak{M}(\Gamma)$). Поэтому

$$(2a-b),\ (2a-c),\ (2b-a),\ (2b-c),\ (2c-a),\ (2c-b) \notin \mathbb{R}^3_+. \tag{2.14}$$

Возьмем любое $\epsilon \in (0,1/4)$ (независящее от $\det\Gamma$). Если $a_1b_2c_3 \leq \epsilon^{-3}\det\Gamma$, то утверждение леммы выполнено. Пусть $a_1b_2c_3 > \epsilon^{-3}\det\Gamma$. Тогда по теореме Минковского о линейных формах существует ненулевой узел $u \in \Gamma$ такой, что

$$|u_1| < \epsilon \cdot a_1, \quad |u_2| < \epsilon \cdot b_2, \quad |u_3| < \epsilon \cdot c_3.$$

Так как a — минимум, то $a_2 < |u_2|$ либо $a_3 < |u_3|$. Поэтому

$$a_2 < \epsilon \cdot b_2 \quad \text{либо} \quad a_3 < \epsilon \cdot c_3.$$

Аналогично используя минимальность b,c, получаем

$$b_1 < \epsilon \cdot a_1 \quad \text{либо} \quad b_3 < \epsilon \cdot c_3;$$
$$c_1 < \epsilon \cdot a_1 \quad \text{либо} \quad c_2 < \epsilon \cdot b_2.$$

Применяя эти неравенства и учитывая (2.14), имеем

$$\det\Gamma = \left|\det\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}\right| \geq a_1b_2c_3 - a_3b_2c_1 - a_1b_3c_2 - a_2b_1c_3 > (1/2 - 2\cdot\epsilon)\, a_1b_2c_3.$$

Так как $(1/2-2\cdot\epsilon) > 0$, то лемма доказана. □

Следствие 2.3. *Пусть F — грань полиэдра Клейна решетки $\Gamma \in \mathcal{L}_3(\mathbb{R})$, причем $d = d(\Gamma; F)$, $S = \#(F \cap \Gamma)$. Тогда*

$$\prod_{i=1}^{3} \max_{u \in F \cap \Gamma} |u_i| \ll d \cdot S \cdot \det \Gamma.$$

Доказательство. Не умаляя общности считаем, что $F \subset [0, +\infty)^3$. Пусть $v^{(1)}, v^{(2)}, v^{(3)}$ — вершины F такие, что

$$|v_i^{(i)}| = \max_{u \in F \cap \Gamma} |u_i|, \quad i = 1, 2, 3.$$

Положим Γ' — решетка, порожденная $v^{(1)}, v^{(2)}, v^{(3)}$. Очевидно, что $\det \Gamma' = O(S \cdot d \cdot \det \Gamma)$. Кроме того, $v^{(i)} \in \mathfrak{M}(\Gamma)$, т.к. любая вершина многогранника Клейна является относительным минимумом (см. [13, 24]). Поэтому $v^{(i)} \in \mathfrak{M}(\Gamma')$. Осталось воспользоваться леммой 2.4, в которой Γ заменяем на Γ'. □

Оператор проективизации $\mathcal{P} : \mathrm{GL}_s(\mathbb{R}) \to \mathrm{P}_s(\mathbb{R})$ и мера μ определены в § II.1.

Теорема 2.1. *Пусть $\mathcal{T} \in TF_3$. Для любого целого $N > 1$ справедлива следующая асимптотическая формула для среднего числа граней типа $\mathcal{T}$:*

$$E_{\mathcal{T}}(N, 3) = \mathcal{C}_{\mathcal{T}} \cdot \ln^2 N + O_{\mathcal{T}}\left(\chi(N) \cdot \ln N\right), \tag{2.15}$$

где

$$\mathcal{C}_{\mathcal{T}} = \frac{4}{\nu(\mathcal{T})} \cdot \frac{\mu(\mathcal{P}(\Omega_{\mathcal{T}}))}{\zeta(2)\zeta(3)}.$$

Доказательство. Согласно следствию 2.3 множество $\Omega_{\mathcal{T}}$ удовлетворяет условию (Б') главы II (если $M(a, b, c) \in \Omega_{\mathcal{T}}$, то существует решетка Γ и грань $F \in \mathcal{F}(\Gamma; \mathcal{T})$ такие, что $a, (b + a), (c + a) \in \Gamma \cap F$). Все условия следствия II.1.1 выполнены. Применяя его, получаем

$$\#\omega_{\mathcal{T}}(N) = \frac{\mathcal{R}_3(N)}{2\zeta(2)\zeta(3)} \left(\mu(\Omega_{\mathcal{T}}) \ln^2 N + O_{\Omega_{\mathcal{T}}, d_2, d_3, d}(\chi(N) \cdot \ln N)\right).$$

Осталось воспользоваться (2.12), (2.13). □

Замечание 2.3. Нетрудно проверить, что множество $\Omega_{\mathcal{T}}$ имеет непустую внутренность и поэтому $\mu(\mathcal{P}(\Omega_{\mathcal{T}})) > 0$, $\mathcal{C}_{\mathcal{T}} > 0$. Действительно, так как $\mathcal{T} \in TF_3$, то существует решетка $\Gamma \in \mathcal{L}_3(\mathbb{R})$ и грань $F \in \mathcal{F}(\Gamma; \mathcal{T})$, $F \subset [0, +\infty)^3$. Тогда найдется решетка общего положения Γ^* (то есть $\gamma_i \neq 0$ при $i = 1, 2, 3$ для всех $\gamma \in \Gamma^* \setminus \{0\}$) и грань $F^* \in \mathcal{F}(\Gamma^*; \mathcal{T})$, $F^* \subset [0, +\infty)^3$. Для матрицы $M = M(a, b, c) \in \Lambda(\Gamma^*; F^*)$ все неравенства, входящие в определение $\Omega_{\mathcal{T}}$ будут строгими, то есть M принадлежит внутренности $\Omega_{\mathcal{T}}$.

Замечание 2.4. Утверждения леммы 2.4 и следствия 2.3 не обобщаются на случай размерности 4 и выше. Следующий пример построен О.Н. Германом. Рассмотрим решетку Γ с базисной матрицей

$$M(a^{(1)}, a^{(2)}, a^{(3)}, a^{(4)}) = \begin{pmatrix} 1 & 0 & 0 & \epsilon \\ 0 & 1 & \epsilon & 0 \\ 0 & 0 & 1/2 & 1/2+\epsilon \\ 0 & 0 & 1/2 & 1/2-\epsilon \end{pmatrix},$$

где $0 < \epsilon < 1/2$. Тогда множество $F = \operatorname{conv}\{a^{(i)}\}_{i=1}^{4}$ является пустой гранью многогранника Клейна решетки Γ. Поэтому $a^{(i)} \in \mathcal{V}(\Gamma) \subset \mathfrak{M}(\Gamma)$. Однако

$$\det \Gamma = \epsilon, \quad \prod_{i=1}^{4} \max_{1 \le j \le 4} |a_i^{(j)}| = \frac{1}{4} + \frac{\epsilon}{2}.$$

О множестве TF_3 реализуемых граней

Содержание этого пункта приводится для полноты изложения и нигде не используется. О.Н. Карпенковым [104] получено полное описание целочисленно-линейных типов $\mathcal{T} \in TF_3$ многоугольников, принадлежащих плоскостям, лежащим на целочисленном расстоянии, большем чем 1 от начала координат. Рассмотрим остальные типы.

Пусть $TF_3(1)$ состоит из $\mathcal{T} \in TF_3$ таких, что многоугольники целочисленно-линейного типа $\mathcal{T}$ принадлежат плоскостям, лежащим на единичном целочисленном расстоянии от начала координат.

Лемма 2.5. *Пусть $\mathcal{T}$ — целочисленно-линейный тип выпуклых многоугольников из $\mathbb{R}^3$. Тогда $\mathcal{T} \in TF_3(1)$, если и только, если для любого $T \in \mathcal{T}$*

а) целочисленное расстояние от плоскости, содержащей T, до начала координат равно единице;

б) существует треугольник Δ такой, что $T \subset \Delta$, $\quad \Delta \cap \mathbb{Z}^3 = T \cap \mathbb{Z}^3$.

Замечание 2.5. Если условия а), б) выполняются *для некоторого* $T \in \mathcal{T}$, то они выполняются *для всех* $T \in \mathcal{T}$.

Доказательство. Пусть $\mathcal{T} \in TF_3(1)$. Тогда существует решетка $\Gamma \in \mathcal{L}_3(\mathbb{R})$ и грань $F \in \mathcal{F}(\Gamma; \mathcal{T})$. Причем их всегда можно выбрать так, что $F \subset [0, +\infty)^3$. Рассмотрим треугольник Δ_Γ равный пересечению плоскости, проходящей через F, и угла $[0, +\infty)^3$. Тогда $\Delta_\Gamma \cap \Gamma = F \cap \Gamma$. Возьмем любую базисную матрицу M решетки Γ. Тогда $M^{-1}\Gamma = \mathbb{Z}^3$ и условие б), в котором $T = M^{-1} \cdot F$, $\Delta = M^{-1} \cdot \Delta_\Gamma$ выполнено. Условие а) выполняется по определению.

Пусть выполнены условия а) и б). Докажем, что $\mathcal{T} \in TF_3(1)$. Возьмем любой многоугольник $T \in \mathcal{T}$. Пусть Δ — треугольник из б). Рассмотрим пирамиду P с основанием Δ и вершиной в начале координат. Согласно а), б) она является почти пустой. Возьмем любое линейное преобразование L, которое плоскости, проходящие через стороны треугольника Δ и начало координат, переводит в координатные плоскости. Тогда $\Gamma = L\mathbb{Z}^3 \in \mathcal{L}_3(\mathbb{R})$, $F = LT \in \mathcal{F}(\Gamma; \mathcal{T})$. $\square$

§ 3. Среднее количество вершин

В этом параграфе мы докажем асимптотическую формулу (0.2) для среднего числа вершин трехмерных многогранников Клейна.

Формулировка основного результата

Пусть

$$\hat{\Omega}_1 = \left\{ \begin{pmatrix} a_1 & -b_1 & -c_1 \\ a_2 & b_2 & -c_2 \\ a_3 & -b_3 & c_3 \end{pmatrix} : \begin{array}{l} a_i, b_i, c_i \in (0, +\infty), \quad i = 1, 2, 3, \\ a_1 \geq \max\{b_1, c_1\}; \quad b_2 > \max\{a_2, c_2\}; \quad c_3 > a_3 \geq b_3, \\ a_1 < b_1 + c_1 \end{array} \right\}.$$

Отметим, что $\hat{\Omega}_1 \subset \Omega_1$, $\Omega_1 \setminus \hat{\Omega}_1 \subset \partial\Omega_1$, множество Ω_1 определено в § III.2.

Кроме того, определим

Ω_V — множество матриц из $\hat{\Omega}_1$, у которых

$$b_2 \leq a_2 + c_2, \quad c_3 \leq a_3 + b_3, \quad a_2 \geq c_2;$$

Ω'_V — множество матриц из Ω_V, у которых

$$\begin{array}{ccc} b_2 > \dfrac{a_2}{2} + c_2 & \text{либо} & c_3 > \dfrac{a_3}{2} + b_3; \\ a_1 < 2c_1 & \text{либо} & a_2 < 2c_2; \\ a_1 < 2b_1 & \text{либо} & a_3 < 2b_3; \end{array}$$

Ω''_V — множество матриц из Ω_V, у которых

$$b_2 \leq \frac{a_2}{2} + c_2, \quad c_3 \leq \frac{a_3}{2} + b_3;$$

$\Omega_{V,3}$ — множество матриц из Ω_V, у которых

$$a_1 < \frac{b_1}{2} + c_1, \quad a_2 + \frac{c_2}{2} < b_2, \quad 2a_3 < b_3 + c_3.$$

Сразу отметим, что все эти множества удовлетворяют условиям (А), (Б) главы II.

В этом параграфе мы докажем следующий результат.

Теорема 3.1. *Для любого целого $N > 1$ справедлива следующая асимптотическая формула для среднего числа вершин трехмерных полиэдров Клейна:*

$$E_{\mathcal{V}}(N, 3) = C_{\mathcal{V}} \cdot \ln^2 N + O\left(\chi(N) \cdot \ln N\right),$$

где

$$\begin{aligned} C_{\mathcal{V}} &= \mathcal{C}(3) - C_{\mathfrak{M}\setminus\mathcal{V}}, \\ C_{\mathfrak{M}\setminus\mathcal{V}} &= \frac{4}{\zeta(2)\zeta(3)} \left(\mu(\mathcal{P}(\Omega'_V)) + 3 \cdot \mu(\mathcal{P}(\Omega''_V)) + 2 \cdot \mu(\mathcal{P}(\Omega_{V,3})\right), \end{aligned}$$

а $\mathcal{C}(3)$ — постоянная из теоремы III.2.1.

Теорема будет доказана в конце параграфа.

Замечание 3.1. Множество Ω'_V можно представить в виде:

$$\Omega'_V = \Omega_V \setminus (\Omega''_V \cup \Omega^I_V \cup \Omega^{II}_V),$$

где Ω^I_V (Ω^{II}_V) — множество матриц из Ω_V, у которых

$$a_1 \geq 2c_1, \quad a_2 \geq 2c_2 \quad (a_1 \geq 2b_1, \quad a_3 \geq 2b_3).$$

Множества $\mathcal{P}(\Omega''_V)$, $\mathcal{P}(\Omega^I_V)$, $\mathcal{P}(\Omega^{II}_V)$ попарно не пересекаются. Преобразование, которое сначала меняет местами 2-ю и 3-ю строки матрицы, а потом 2-й и 3-й столбцы, осуществляет биекцию между Ω^I_V и Ω^{II}_V. Поэтому

$$\mu(\mathcal{P}(\Omega'_V)) = \mu(\mathcal{P}(\Omega_V)) - \mu(\mathcal{P}(\Omega''_V)) - 2 \cdot \mu(\mathcal{P}(\Omega^I_V)),$$
$$C_{\mathfrak{M}\setminus\mathcal{V}} = \frac{4}{\zeta(2)\zeta(3)} \left(\mu(\mathcal{P}(\Omega_V)) + 2\mu(\mathcal{P}(\Omega''_V)) + 2\mu(\mathcal{P}(\Omega_{V,3})) - 2\mu(\mathcal{P}(\Omega^I_V))\right).$$

Последняя формула является более удобной для вычислений.

Замечание 3.2. По-видимому, постоянные $\mathcal{C}(3)$, $C_{\mathcal{V}}$ не выражаются через известные. Приближенные вычисления дали следующие результаты:

$$\mu(\Omega_V) \approx 0.00248, \quad \mu(\Omega''_V) \approx 0.00049, \quad \mu(\Omega_{V,3}) \approx 0.00017, \quad \mu(\Omega^I_V) \approx 0.00022,$$
$$\mathcal{C}(3) \approx 0.8335, \quad C_{\mathfrak{M}\setminus\mathcal{V}} \approx 0.0068.$$

Замечание 3.3. Есть основания полагать, что для любой размерности s существует предел

$$\theta(s) = 1 - \lim_{N\to+\infty} \frac{\sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};N)} \#\mathcal{V}(\Gamma)}{\sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};N)} \#\mathfrak{M}(\Gamma)}$$

— доля относительных минимумов, которые не являются вершинами многогранников Клейна s-мерных решеток. Известно, что $\theta(2) = 0$. Из приведенных результатов вытекает, что

$$\theta(3) = \frac{C_{\mathfrak{M}\setminus\mathcal{V}}}{\mathcal{C}(3)} \approx 0.0082.$$

Начиная с размерности $s = 4$ почти ничего неизвестно. Интересными представляются следующие вопросы:

1) *верно ли, что функция θ монотонно возрастает?*

2) *верно ли, что* $\theta(s) \to 1$ при $s \to +\infty$?

Положительные ответы на эти вопросы означают, что с ростом размерности конструкции «относительные минимумы» и «многогранники Клейна» начинают сколь угодно сильно отличаться.

Доказательство основного результата

Возьмем любое целое $N > 1$. Пусть

$$U_{\mathfrak{M}\setminus\mathcal{V}}(N) = \left\{(\Gamma, a) : \ \Gamma \in \mathcal{L}_3(\mathbb{Z}; N), \ \ a \in \mathfrak{M}(\Gamma) \setminus \mathcal{V}(\Gamma), \ \ a \in (0, +\infty)^3\right\}.$$

Известно (см. [13, 24]), что любая вершина многогранника Клейна является относительным минимумом соответствующей решетки. Учитывая, что у любой решетки из $\mathcal{L}_3(\mathbb{Z};N)$ количество относительных минимумов, имеющих хотя бы одну нулевую координату, оценивается величиной $O(\ln N)$ (см., например, [10, 35] либо неравенство (I.3.12)), получаем

$$E_{\mathcal{V}}(N,3)=E_{\mathfrak{M}}(N,3)-2^3\cdot\frac{\#U_{\mathfrak{M}\setminus\mathcal{V}}(N)}{\mathcal{R}_3(N)}+O(\ln N). \tag{3.1}$$

Осталось вычислить количество минимумов, которые не являются вершинами многогранников Клейна.

Пусть $U(N)$ — множество пар (Γ,a) удовлетворяющих условиям:

1) $\Gamma\in\mathcal{L}_3(\mathbb{Z};N)$, $a\in\Gamma\cap(0,+\infty)^3$;

2) существуют такие $b',c'\in\Gamma\cap[0,+\infty)^3$, $n\in\mathbb{N}$, что $a\in F$, где F — треугольная грань полиэдра Клейна решетки Γ с вершинами в точках

$$b',\quad c',\quad u=(2n+1)a-nb'-nc',$$

причем

$$F\cap\Gamma=\Big\{a,\ b',\ c',\ (2k+1)a-kb'-kc'\Big\}_{k=1}^{n}, \tag{3.2}$$

т.е. F из узлов Γ содержит только свои вершины и точки принадлежащие отрезку $[a,u]$, который лежит на медиане выходящей из u.

Докажем, что множества $U_{\mathfrak{M}\setminus\mathcal{V}}(N)$ и $U(N)$ «почти» совпадают.

Теорема 3.2. *Справедливо вложение $U(N)\subset U_{\mathfrak{M}\setminus\mathcal{V}}(N)$. Кроме того, если $(\Gamma,a)\in U_{\mathfrak{M}\setminus\mathcal{V}}(N)$, причем $(\Gamma,a)\notin U(N)$, то хотя бы одна из точек*

$$(2a_1,0,0),\quad (0,2a_2,0),\quad (0,0,2a_3) \tag{3.3}$$

является узлом Γ.

Доказательство теоремы вытекает из результатов [24].

Лемма 3.1. *Для любой решетки $\Gamma\in\mathcal{L}_s(\mathbb{Z};N)$ количество относительных минимумов, у которых хотя бы одна координата фиксирована, не больше, чем $O_s(\ln^{s-2}N)$.*

Для доказательство достаточно воспользоваться леммой I.1.2 и учесть, что

$$|\gamma|_\infty\le N\quad\text{ при }\gamma\in\mathfrak{M}(\Gamma),\ \ \Gamma\in\mathcal{L}_s(\mathbb{Z};N).$$

Лемма 3.2. *Пусть $\Gamma\in\mathcal{L}_3(\mathbb{Z};N)$, $\mathfrak{M}'(\Gamma)$ — множество $a\in\mathfrak{M}(\Gamma)\cap[0,+\infty)^3$ таких, что хотя бы одна из точек (3.3) является узлом Γ. Тогда $\#\mathfrak{M}'(\Gamma)\ll\ln N$.*

Доказательство. Возьмем любой $a\in\mathfrak{M}'(\Gamma)$. Пусть, например, $(2a_1,0,0)\in\Gamma$. Тогда $(2a_1,0,0)\in\mathfrak{M}(\Gamma)$, т.к. в противном случае существует узел $\gamma=(\gamma_1,0,0)\in\Gamma$ такой, что $0<\gamma_1<2a_1$ и точка $(a-\gamma)$ противоречит условию $a\in\mathfrak{M}(\Gamma)$. Минимум вида $(2a_1,0,0)$ единственен. Поэтому одна из координат a однозначно определяется решеткой Γ. Используя лемму 3.1, получаем требуемое утверждение. □

Из леммы 3.2 и теоремы 3.2 вытекает оценка

$$\#U_{\mathfrak{M}\setminus\mathcal{V}}(N) = \#U(N) + O(\mathcal{R}_3(N)\cdot \ln N).$$

Подставляя ее в (3.1), заключаем

$$E_{\mathcal{V}}(N,3) = E_{\mathfrak{M}}(N,3) - 8\cdot\frac{\#U(N)}{\mathcal{R}_3(N)} + O(\ln N). \tag{3.4}$$

Осталось вычислить количество элементов множества $U(N)$.

Лемма 3.3. *Возьмем любую пару $(\Gamma, a) \in U(N)$. Пусть (b', c', u) — вершины грани $F = F(\Gamma, a)$, удовлетворяющие (3.2). Тогда*

$$3a_i \geq b'_i + c'_i, \quad i = 1,2,3, \tag{3.5}$$

и существует такая перестановка (k,m,n) из $\{1,2,3\}$, что

$$b'_k + c'_k < a_k, \quad c'_m < a_m < b'_m, \quad b'_n < a_n < c'_n, \tag{3.6}$$

$$2a_m < b'_m, \quad 2a_n < c'_n. \tag{3.7}$$

Доказательство. Ввиду (3.2), $(3a - b' - c') \in [0,+\infty)^3$. Поэтому выполняется (3.5). Кроме того,

$$(b' + c' - a), \ \ (2a - b'), \ \ (2a - c') \notin [0,+\infty)^3. \tag{3.8}$$

Из первого условия следует, что найдется номер k такой, что выполняется первое из неравенств (3.6). Пусть $\{m,n\} = \{1,2,3\}\setminus\{k\}$. Если $a_m \geq \max\{b'_m, c'_m\}$, то (в силу 2-го и 3-го соотношений из (3.8)) $2a_k < \min\{b'_k, c'_k\}$. Противоречие с (3.5). Поэтому

$$a_m < \max\{b'_m, c'_m\}, \quad a_n < \max\{b'_n, c'_n\}. \tag{3.9}$$

Если $a_m < b'_m, \ \ a_n < b'_n$ (либо $a_m < c'_m$, $c'_n < b'_n$), то из (3.5) вытекает, что $(2a - c') \in [0,+\infty)^3$ (либо $(2a - b') \in [0,+\infty)^3$). Противоречие. Значит, существуют номера k,m,n, удовлетворяющие (3.6). Неравенства (3.7) следуют из (3.6), (3.8). □

Пусть $U_1(N)$ — множество пар $(\Gamma, a) \in U(N)$ таких, что грань $F = F(\Gamma, a)$ удовлетворяет условию: $d(\Gamma; F) = 1$. Напомним, что $d(\Gamma; F)$ совпадает с индексом подрешетки, порожденной векторами a, b', c', где b', c' — вершины треугольника F, удовлетворяющие (3.2).

Разобьем $U_1(N)$ на две непересекающиеся части: $U'(N)$ и $U''(N)$, где $U'(N)$ состоит из таких пар, что в условиях (3.2) $n = 1$ (т.е. грань F из узлов решетки содержит только свои вершины и a), а для $U''(N)$ соответственно $n \geq 2$.

Лемма 3.4. *Справедлива формула*

$$\#U'(N) = \#\Omega'_V(\mathbb{Z}; N),$$

где $\Omega'_V(\mathbb{Z}; N)$ — множество целочисленных матриц $M \in \Omega'_V$ таких, что $\det M = N$.

Доказательство. Возьмем любую пару $(\Gamma, a) \in U'(N)$. Пусть $F = F(\Gamma; a)$. Согласно лемме 3.3 мы всегда можем единственным образом занумеровать вершины F через b', c', u так, что будут выполнены неравенства

$$\begin{array}{ll} b'_1 + c'_1 < a_1, & \\ 2a_2 < b'_2, & c'_2 < a_2 < b'_2, \\ b'_3 < a_3 < c'_3, & 2a_3 < c'_3. \end{array} \tag{3.10}$$

Определим взаимно однозначное отображение Φ, которое каждой паре $(\Gamma, a) \in U'(N)$ ставит в соответствие матрицу $M = M(a, b' - a, c' - a)$ со столбцами $a, (b' - a), (c' - a)$, где b', c' определяются указанным выше способом. Осталось доказать, что

$$\Phi(U'(N)) = \Omega'_V(\mathbb{Z}; N). \tag{3.11}$$

1. Докажем, что $\Phi(U'(N)) \subset \Omega'_V(\mathbb{Z}; N)$. Пусть $(\Gamma, a) \in U'(N)$. Положим $M = M(a, b' - a, c' - a) = \Phi(\Gamma, a)$. Тогда выполняются неравенства (3.5), (3.10). Поскольку узлы $(5a - 2b' - 2c')$, $(2b' - a)$, $(2c' - a)$ не принадлежит $[0, +\infty)^3$, то

$$\begin{array}{rcl} 5a_2 < 2(b'_2 + c'_2) & \text{либо} & 5a_3 < 2(b'_3 + c'_3); \\ a_1 > 2b'_1 & \text{либо} & a_3 > 2b'_3; \\ a_1 > 2c'_1 & \text{либо} & a_2 > 2c'_2. \end{array} \tag{3.12}$$

Из (3.5), (3.10), (3.12) (и условий $a \in (0, +\infty)^3$, $b', c' \in [0, +\infty)^3$) следует, что $M \in \Omega'_V$. Так как $d(\Gamma; F) = 1$, то a, b', c' — базис Γ. Поэтому $\det M = N$. Значит, $M \in \Omega'_V(\mathbb{Z}; N)$ и $\Phi(U'(N)) \subset \Omega'_V(\mathbb{Z}; N)$.

2. Осталось доказать, что $\Omega'_V(\mathbb{Z}; N) \subset \Phi(U'(N))$. Пусть $M = M(a, b, c) \in \Omega'_V(\mathbb{Z}; N)$. Положим $b' = b + a$, $c' = c + a$ и определим решетку $\Gamma \in \mathcal{L}_3(\mathbb{Z}; N)$ с базисом a, b, c, а также узел $u = 3a - b' - c'$ и треугольник F с вершинами в точках b', c', u. Тогда

$$\Gamma \cap F = \{a, b', c', u\}.$$

Кроме того, $a \in (0, +\infty)^3$, $b', c' \in [0, +\infty)^3$ и выполняются неравенства (3.5), (3.10), (3.12). Применим лемму 2.1. Учитывая, что минимальная $X(\Gamma; F)$-окрестность F состоит из точек

$$(2c' - a),\ (2b' - a),\ (2a - b'),\ (2a - c'),\ (5a - 2b' - 2c'),\ (b' + c' - a),$$

получаем F — грань многогранника Клейна решетки Γ. Поэтому $(\Gamma, a) \in U'(N)$ и, значит, $\Omega'_V(\mathbb{Z}; N) \subset \Phi(U'(N))$. Равенство (3.11) доказано. □

Лемма 3.5. *Справедлива формула*

$$\#U''(N) = 3 \cdot \#\Omega''_V(\mathbb{Z}; N),$$

где $\Omega''_V(\mathbb{Z}; N)$ *— множество целочисленных матриц* $M \in \Omega''_V$ *таких, что* $\det M = N$.

Доказательство. Согласно лемме 3.3 множество $U''(N)$ можно разбить на три непересекающиеся части $U''_k(N)$, $k = 1, 2, 3$ так, что

$$\forall (\Gamma, a) \in U''_k(N) \qquad a_k > b'_k + c'_k,$$

где b', c' — вершины $F = F(\Gamma, a)$, удовлетворяющие (3.2). Очевидно, что

$$\#U_1''(N) = \#U_2''(N) = \#U_3''(N), \quad \#U''(N) = 3 \cdot \#U_1''(N). \tag{3.13}$$

Вычислим $\#U_1''(N)$. Согласно лемме 3.3 для любой пары $(\Gamma, a) \in U_1''(N)$ существует единственная нумерация вершин грани $F = F(\Gamma, a)$ через b', c', u так, что выполняются (3.2), (3.10). Определим взаимно однозначное отображение Φ, которое каждой паре $(\Gamma, a) \in U_1''(N)$ ставит в соответствие матрицу $M = M(a, b'-a, c'-a)$, где b', c' определяются указанным выше способом. Осталось показать, что Φ отображает $U_1''(N)$ на $\Omega_V''(\mathbb{Z}; N)$.

1. Пусть $(\Gamma, a) \in U''(N)$, $M = M(a, b'-a, c'-a) = \Phi(\Gamma, a)$. Так как $(5a-2b'-2c') \in [0, +\infty)^3$, то, помимо (3.5), (3.10), выполняются оценки

$$5a_2 \geq 2(b_2' + c_2'), \quad 5a_3 \geq 2(b_3' + c_3'). \tag{3.14}$$

Используя (3.5), (3.10), (3.14), получаем $M \in \Omega_V''$. Так как $d(\Gamma; F) = 1$, то a, b', c' — базис Γ. Кроме того, $\det M > 0$, и поэтому $\det M = N$. Значит, $M \in \Omega_V''(\mathbb{Z}; N)$ и $\Phi(U''(N)) \subset \Omega_V''(\mathbb{Z}; N)$.

2. Пусть $M(a, b, c) \in \Omega_V''(\mathbb{Z}; N)$. Положим $b' = b+a$, $c' = c+a$ и определим решетку $\Gamma \in \mathcal{L}_3(\mathbb{Z}; N)$ с базисом a, b, c и треугольник F с вершинами в точках b', c', u, где $u = (2n+1)a - n(b'+c')$, а n — наибольшее натуральное для которого соответствующий u имеет неотрицательные координаты. Тогда выполняются (3.2), (3.5), (3.10) (3.14). Минимальная $X(\Gamma; F)$-окрестность F состоит из четырех точек

$$(2a - b'), \quad (2a - c'), \quad ((2n+3)a - (n+1)(b' + c')), \quad (b' + c' - a).$$

Используя лемму 2.1, получаем F — грань многогранника Клейна решетки Γ. Значит, $(\Gamma, a) \in U_1''(N)$, причем $M = \Phi(\Gamma, a)$. Следовательно, $\Omega_V''(\mathbb{Z}; N) \subset \Phi(U_1''(N))$. Поэтому $\Phi(U_1''(N)) = \Omega_1''(\mathbb{Z}; N)$, $\#U_1''(N) = \#\Omega_V''(\mathbb{Z}; N)$. Применяя (3.13), приходим к требуемой формуле. □

Осталось рассмотреть множество $U(N) \setminus U_1(N)$. В [104] получено полное описание типов граней трехмерных полиэдров Клейна, у которых $d(\Gamma; F) > 1$. Согласно [104], если $(\Gamma, a) \in U(N)$, $F = F(\Gamma, a)$, причем $d(\Gamma; F) > 1$, то $d(\Gamma; F) = 3$ и грань F принадлежит типу $\mathcal{T}_3$, где $\mathcal{T}_3$ — множество многоугольников целочисленно-линейно эквивалентных треугольнику с вершинами в точках

$$(1, 1, 3), \quad (0, 2, 3), \quad (2, 3, 3).$$

Отметим, что тогда a — единственная точка Γ, лежащая на $F(\Gamma, a)$ и не совпадающая с вершиной (т.е. $n = 1$).

Лемма 3.6. *Пусть $U_3(N) = U(N) \setminus U_1(N)$, а $\omega_{V,3}(N)$ — множество целочисленных матриц $M = M(a, b, c) \in \Omega_{V,3}$, удовлетворяющих условиям:*

$$\det M = 3N, \quad (a - b + c) \in 3\mathbb{Z}^3. \tag{3.15}$$

Тогда $\#U_3(N) = 2 \cdot \#\omega_{V,3}(N)$.

Доказательство. Согласно лемме 3.3 для любой пары $(\Gamma; a) \in U_3(N)$ существует единственная нумерация вершин треугольника $F = F(\Gamma; a)$ через b', c', u так, что выполняются (3.10). Так как F принадлежит типу $\mathcal{T}_3$, то

$$\frac{a - b' + c'}{3} \in \Gamma \quad \text{либо} \quad \frac{a + b' - c'}{3} \in \Gamma. \tag{3.16}$$

Одновременно эти включения выполняться не могут (иначе $2a/3 \in \Gamma$, что противоречит условию $a \in \mathfrak{M}(\Gamma)$). Поэтому $U_3(N)$ можно разбить на две непересекающиеся части: $U_{3,1}(N)$ и $U_{3,2}(N)$ так, что для первого множества выполняется первое из включений (3.16), а для второго — второе. Очевидно, что

$$\#U_{3,1}(N) = \#U_{3,2}(N), \quad \#U_3(N) = 2 \cdot \#U_{3,1}(N). \tag{3.17}$$

Определим взаимно однозначное отображение Φ, которое паре $(\Gamma, F) \in U_{3,1}(N)$ ставит в соответствие матрицу $M(a, b' - a, c' - a)$, где b', c' определяются указанным выше образом. Осталось доказать, что $\Phi(U_{3,1}(N)) = \omega_{V,3}(N)$.

1. Пусть $(\Gamma, a) \in U_{3,1}(N)$. Тогда выполняются (3.5), (3.10), (3.15). Узлы $\tilde{a}$, b, c образуют базис Γ, где

$$\tilde{a} = \frac{a - b + c}{3}, \quad b = b' - a, \quad c = c' - a. \tag{3.18}$$

Кроме того,

$$b'_1 + 2c'_1 < a_1, \quad 5a_2 < c'_2 + 2b'_2, \quad 2a_3 + b'_3 < c'_3. \tag{3.19}$$

Для доказательства (3.19) достаточно рассмотреть узлы

$$\begin{aligned} u^{(1)} &= 2\tilde{a} + b = \frac{2}{3}(a + \frac{b}{2} + c) = \frac{-a + b' + 2c'}{3}, \\ u^{(2)} &= 2\tilde{a} - c = \frac{2}{3}(a - b - \frac{c}{2}) = \frac{5a - 2b' - c'}{3}, \\ u^{(3)} &= 2\tilde{a} + b - c = \frac{2}{3}(a + \frac{b}{2} - \frac{c}{2}) = \frac{2a + b' - c'}{3}, \end{aligned}$$

которые не должны принадлежать $[0, +\infty)^3$. Используя указанные соотношения, получаем $M = M(a, b' - a, c' - a) \in \omega_{V,3}(N)$. Значит, $\Phi(U_{3,1}(N)) \subset \omega_{V,3}(N)$.

2. Пусть $M(a, b, c) \in \omega_{V,3}(N)$. Определим $b' = b + a$, $c' = c + a$ и решетку $\Gamma \in \mathcal{L}_3(\mathbb{Z}; N)$ с базисом $\tilde{a}, b, c$, где $\tilde{a}$ удовлетворяет (3.18). Тогда выполняются соотношения (3.5), (3.10), (3.15), (3.19). Пусть F — треугольник с вершинами в точках b', c', u, где $u = 3a - (b' + c')$. Тогда $F \subset [0, +\infty)^3$. Докажем, что F — грань многогранника Клейна решетки Γ. Будем использовать лемму 2.1. Множество $X(\Gamma; F)$ состоит из точек вида

$$3\tilde{a} + \frac{3n}{2}b + \frac{3m}{2}c = a + (b - a)(3n/2 - 1) + (c - a)(3m/2 + 1), \quad n, m \in \mathbb{Z},$$

а также узлов Γ, лежащих на плоскости, проходящей через F. Поэтому минимальная $X(\Gamma; F)$-окрестность F состоит из точек $\frac{3}{2}u^{(i)}$, $i = 1, 2, 3$. Согласно (3.19) эти точки не принадлежат $[0, +\infty)^3$. Используя лемму 2.1, получаем F — грань многогранника Клейна решетки Γ. Значит, $(\Gamma, a) \in U_{3,1}(N)$, причем $\Phi(\Gamma; a) = M(a, b, c)$. Поэтому $\omega_{V,3}(N) \subset \Phi(U_{3,1}(N))$ и, следовательно, $\Phi(U_{3,1}(N)) = \omega_{V,3}(N)$,

$$\#U_{3,1}(N) = \#\omega_{V,3}(N).$$

Используя (3.17), получаем утверждение леммы. □

Доказательство теоремы 3.1. Согласно леммам 3.4, 3.5, 3.6

$$\#U(N) = \#\Omega'_V(\mathbb{Z}; N) + 3 \cdot \#\Omega''_V(\mathbb{Z}; N) + 2 \cdot \#\omega_{V,3}(N).$$

Применяя теорему II.1.1 и следствие II.1.1, получаем

$$\#U(N) = \frac{\mathcal{R}_3(N)}{2\zeta(2)\zeta(3)} \left(\left(\mu(\Omega'_V) + 3 \cdot \mu(\Omega''_V) + 2 \cdot \mu(\Omega_{V,3}) \right) \ln^2 N + O(\chi(N) \ln N) \right).$$

Используя последнее соотношение, (3.4) и теорему III.2.1 приходим к требуемой формуле. □

Глава V
Среднее количество цилиндрических минимумов и наилучших приближений линейных форм

Пусть f — кусочно-дифференцируемая, непрерывная, лучевая функция, определенная на $\mathbb{R}^{s-1}$. Напомним, что ненулевой узел a решетки $\Gamma \in \mathcal{L}_s(\mathbb{R})$ мы называем цилиндрическим f-минимумом, если не существует ненулевого узла $\gamma \in \Gamma$ такого, что

$$f(\gamma_1, \dots, \gamma_{s-1}) \le f(a_1, \dots, a_{s-1}), \quad |\gamma_s| \le |a_s|, \tag{0.1}$$

причем хотя бы одно из неравенств строгое.

Ненулевой вектор $(u, v) \in \mathbb{Z}^{s-1} \times \mathbb{Z}$ называется f-наилучшим приближением линейной формы $L : \mathbb{R}^{s-1} \to \mathbb{R}$, если не существует ненулевого $(u', v') \in \mathbb{Z}^{s-1} \times \mathbb{Z}$ такого, что

$$|Lu' - v'| \le |Lu - v|, \quad f(u') \le f(u),$$

причем хотя бы одно из неравенств строгое.

В § 1 мы построим и исследуем процедуру дополнения цилиндрического минимума до базиса решетки, основанную на идеях Г.Ф. Вороного [20]. В § 2 мы получим асимптотическую формулу для среднего количества f-цилиндрических минимумов решеток из $\mathcal{L}_s(\mathbb{Z}; [1, R])$, а в § 3 — асимптотические формулы для среднего числа наилучших приближений линейных форм.

§ 1. Базис Вороного и его свойства

Приведенные базисы.

Базис $e^{(1)}, \dots, e^{(m)}$ решетки $\Lambda \subset \mathbb{R}^m$ называется *приведенным* (по Минковскому), если выполняются следующие условия

1) $|e^{(1)}| = \min\{|\gamma| : \gamma \in \Lambda \setminus \{0\}\}$;

2) для любого $j \ge 2$ $|e^{(j)}| = \min |\eta|$, где минимум берется по всем узлам $\eta \in \Lambda$ таким, что система $e^{(1)}, \dots, e^{(j-1)}, \eta$ дополняется до базиса решетки Λ.

Известно (см., например, [54, гл. II, § 2]), что базис $\left\{e^{(i)}\right\}_{i=1}^{m}$ является приведенным тогда и только тогда, когда для любого $j \in \{1, \ldots, m\}$

$$\left|e^{(j)}\right| \le \left|\sum_{i=1}^{m} k_i e^{(i)}\right| \tag{1.1}$$

при всех $(k_1, \ldots, k_m) \in \mathbb{Z}^m$ таких, что нод $(k_j, k_{j+1}, \ldots, k_m) = 1$.

Введем следующее отношение упорядоченности на $\mathbb{R}^m$ (лексикографическое). Пусть $x, y \in \mathbb{R}^m$. Будем писать $x \prec y$, если существует такой номер $l \in \{1, \ldots, m\}$, что

$$x_i = y_i, \;\; i = \overline{1, l-1}; \quad x_l < y_l.$$

Пусть у нас есть два набора векторов $\left\{e^{(i)}\right\}_{i=1}^{m}$ и $\left\{f^{(i)}\right\}_{i=1}^{m}$ из $\mathbb{R}^m$. Пишем $\left\{e^{(i)}\right\}_{i=1}^{m} \prec \left\{f^{(i)}\right\}_{i=1}^{m}$, если существует такой номер $l \in \{1, \ldots, m\}$, что

$$e^{(i)} = f^{(i)}, \;\; i = \overline{1, l-1}; \quad e^{(l)} \prec f^{(l)}.$$

Приведенный базис $\left\{e^{(i)}\right\}_{i=1}^{m}$ решетки Λ будем называть *вполне приведенным*, если $\left\{e^{(i)}\right\}_{i=1}^{m} \prec \left\{f^{(i)}\right\}_{i=1}^{m}$ для любого другого приведенного базиса $\left\{f^{(i)}\right\}_{i=1}^{m}$ решетки Λ.

Любая решетка имеет единственный вполне приведенный базис.

Пусть множество

$$\tilde{\mathfrak{R}}_m \subset \underbrace{\mathbb{R}^m \times \ldots \times \mathbb{R}^m}_{m}$$

состоит из всех приведенных базисов m-мерных решеток. Согласно известным свойствам приведенных квадратичных форм (см., например, [53, гл. 12, теорема 1.3]) существует такое конечное множество (зависящее только от размерности m) условий вида (1.1), что если базис $\left\{e^{(i)}\right\}_{i=1}^{m}$ удовлетворяет условиям этого множества, то $\left\{e^{(i)}\right\}_{i=1}^{m}$ — приведенный базис. В частности, это означает, что граница множества $\tilde{\mathfrak{R}}_m$ состоит из фиксированного числа поверхностей класса C^∞.

Рассмотрим теперь множество $\mathfrak{R}_m \subset \tilde{\mathfrak{R}}_m$, составленное из всех вполне приведенных базисов m-мерных решеток. Если $\left\{e^{(i)}\right\}_{i=1}^{m}$ — приведенный базис Λ, то элементы матрицы перехода от $\left\{e^{(i)}\right\}_{i=1}^{m}$ к любому другому приведенному базису решетки Λ ограничены некоторой константой, зависящей только от m (см., например, [53, гл. 12, теорема 1.2]). Поэтому граница множества $\mathfrak{R}_m$ также состоит из фиксированного числа поверхностей класса C^∞.

Базис Вороного.

Рассмотрим метод дополнения примитивного узла решетки до базиса, предложенный Г.Ф. Вороным. Используем определения из [32, глава 5, § 60]).

Пусть Γ — решетка из $\mathbb{R}^s$. Возьмем любой примитивный узел $a = (a_1, \ldots, a_s) \in \Gamma$ такой, что $a_s > 0$. Все точки решетки лежат на прямых, параллельных a (*параллелях*). Эти прямые пересекают плоскость $\pi_s = \{x \in \mathbb{R}^s : x_s = 0\}$ в узлах некоторой решетки Λ, которую можно рассматривать как $(s-1)$-мерную полную решетку, если вычеркнуть последние координаты узлов (которые равны нулю). Узел решетки Λ будем называть *основанием* параллели. Отрезок параллели от основания до первой,

лежащей не ниже плоскости π_s, точки решетки Γ будем называть *гвоздиком*, первую точку решетки — *шапочкой* гвоздика, а основание параллели — основанием гвоздика.

Отметим, что гвоздик может иметь нулевую длину (если его основание является узлом Γ). Шапочка γ и основание η гвоздика связаны между собой соотношением

$$\eta = \gamma - a \cdot \frac{\gamma_s}{a_s}. \tag{1.2}$$

Узел $\gamma \in \Gamma$ является шапочкой некоторого гвоздика, если и только если $0 \le \gamma_s < a_s$. Поэтому для любого гвоздика с шапочкой γ и основанием η

$$\rho(\gamma) - \rho(a) < |\eta| < \rho(\gamma) + \rho(a). \tag{1.3}$$

Здесь и далее

$$\rho(x) = \sqrt{x_1^2 + \ldots + x_{s-1}^2} \text{ при } x = (x_1, \ldots, x_{s-1}, x_s) \in \mathbb{R}^s.$$

Пусть $\left\{b^{(j)}\right\}_{j=2}^{s}$ — вполне приведенный базис Λ. Обозначим $a^{(1)} = a$ и $a^{(j)}$ — шапочка гвоздика с основанием в точке $b^{(j)}$, $j \ge 2$. Тогда $\left\{a^{(j)}\right\}_{j=1}^{s}$ будет базисом Γ. Назовем его *базисом Вороного*.

Будем говорить, что ненулевой узел $\gamma \in \Gamma$ *нарушает минимальность* узла a, если выполняются неравенства (0.1), причем хотя бы одно из них является строгим. Отметим, что если шапочка γ некоторого гвоздика *не* нарушает минимальность a, то $f(\gamma) > f(a)$.

Лемма 1.1. *Пусть шапочки гвоздиков с основаниями в точках $\pm b^{(2)}$ не нарушают минимальность узла $a^{(1)}$. Положим $\rho_j = \rho(a^{(j)})$, $j = \overline{1,s}$. Тогда*

$$\rho_1 \underset{f}{\ll} |b^{(2)}|, \tag{1.4}$$

Если, дополнительно, узлы $a^{(3)}, \ldots, a^{(s)}$ не нарушают минимальность $a^{(1)}$, то

$$\rho_j \underset{f}{\asymp} |b^{(j)}|, \quad j = \overline{2,s}, \tag{1.5}$$

$$\rho_j \underset{f}{\ll} \rho_{j+1}, \quad j = \overline{1,s-1}. \tag{1.6}$$

$$a_s \cdot \prod_{j=2}^{s} \rho_j \underset{f}{\asymp} \det\Gamma, \tag{1.7}$$

Доказательство. Для удобства записи будем считать, что функция f определена на всем $\mathbb{R}^s$ по правилу:

$$f(x) = f(x_1, \ldots, x_{s-1}) \quad \text{при } x = (x_1, \ldots, x_{s-1}, x_s) \in \mathbb{R}^s.$$

Так как f непрерывная и лучевая, то

$$\forall x \in \mathbb{R}^s \quad f(x) \underset{f}{\asymp} \rho(x). \tag{1.8}$$

Так как f непрерывная и кусочно-дифференцируемая, то она удовлетворяет условию Липшица, т.е. существует такая постоянная $l > 0$, что для любых $x, y \in \mathbb{R}^s$

$$|f(x) - f(y)| \le l \cdot |x - y|.$$

Перепишем последнюю оценку в таком виде:

$$f(x + y) \le f(y) + l \cdot |x|. \tag{1.9}$$

Если шапочка γ некоторого гвоздика не нарушает минимальность a, то $f(a) < f(\gamma)$ и, согласно (1.8),

$$\rho_1 \underset{f}{\ll} \rho(\gamma).$$

Докажем (1.4). Пусть $\tilde{a}$ — шапочка гвоздика с основанием в точке $(-b^{(2)})$. Ввиду (1.2), $a^{(2)}$ и $\tilde{a}$ можно представить в виде:

$$a^{(2)} = b^{(2)} + t \cdot a, \quad \tilde{a} = -b^{(2)} + (1 - t) \cdot a$$

где $t \in [0, 1)$. Так как $\tilde{a}$ и $a^{(2)}$ не могут нарушать минимальность a, то, согласно (1.9)

$$\begin{aligned} f(a) &< f(a^{(2)}) = f(b^{(2)} + t \cdot a) \le t \cdot f(a) + l \cdot |b^{(2)}|, \\ f(a) &< f(\tilde{a}) = f(-b^{(2)} + (1 - t) \cdot a) \le (1 - t) \cdot f(a) + l \cdot |b^{(2)}|. \end{aligned}$$

Складывая эти неравенства, получаем, $f(a) < 2 \cdot l \cdot |b^{(2)}|$. Используя (1.8), приходим к (1.4).

Докажем (1.5). Пусть $j \in \{2, \dots, s\}$. Согласно (1.3)

$$\rho_j - \rho_1 < |b^{(j)}| < \rho_j + \rho_1.$$

Так как $a^{(j)}$ не нарушает минимальность a, то $\rho_1 \underset{f}{\ll} \rho_j$. Значит,

$$|b^{(j)}| < \rho_j + \rho_1 \underset{f}{\ll} \rho_j.$$

По определению приведенного базиса, $|b^{(2)}| \le |b^{(j)}|$. Поэтому, учитывая (1.4), имеем

$$\rho_j < |b^{(j)}| + \rho_1 \underset{f}{\ll} |b^{(j)}| + |b^{(2)}| \le 2|b^{(j)}|.$$

Оценки (1.5) доказаны. Неравенства (1.6) вытекают из (1.5) и оценок $|b^{(j)}| \le |b^{(j+1)}|$.

Осталось доказать (1.7). Пусть $A = (\!(a_i^{(j)})\!)$ — матрица со столбцами ${a^{(1)}}^T, \dots, {a^{(s)}}^T$. Из каждого j-го ($j \ge 2$) столбца A вычтем первый столбец, умноженный на $a_s^{(j)}/a_s$. Определитель матрицы не изменится. Учитывая (1.2), получаем

$$\begin{aligned} \det \Gamma &= \left| \det \begin{pmatrix} a_1^{(1)} & a_1^{(2)} & \dots & a_1^{(s)} \\ a_2^{(1)} & a_2^{(2)} & \dots & a_2^{(s)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s-1}^{(1)} & a_{s-1}^{(2)} & \dots & a_{s-1}^{(s)} \\ a_s^{(1)} & a_s^{(2)} & \dots & a_s^{(s)} \end{pmatrix} \right| = \\ &= \left| \det \begin{pmatrix} a_1^{(1)} & b_1^{(2)} & \dots & b_1^{(s)} \\ a_2^{(1)} & b_2^{(2)} & \dots & b_2^{(s)} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s-1}^{(1)} & b_{s-1}^{(2)} & \dots & b_{s-1}^{(s)} \\ a_s^{(1)} & 0 & \dots & 0 \end{pmatrix} \right| = a_s \cdot \det \Lambda. \end{aligned}$$

Согласно известному свойству приведенных базисов

$$\prod_{j=2}^{s} |b^{(j)}| \underset{s}{\asymp} \det \Lambda.$$

Используя (1.5), заключаем

$$\det \Gamma = a_s \cdot \det \Lambda \underset{s}{\asymp} a_s \cdot \prod_{j=2}^{s} |b^{(j)}| \underset{f}{\asymp} a_s \cdot \prod_{j=2}^{s} \rho_j.$$

□

Лемма 1.2. *Существует такое конечное множество $\mathfrak{C}_f \subset \mathbb{Z}^s$, зависящее только от f, что если $\left\{a^{(j)}\right\}_{j=1}^{s}$ — базис Вороного решетки Γ, причем узлы*

$$\gamma = \sum_{j=1}^{s} k_j a^{(j)}, \quad (k_1, \ldots, k_s) \in \mathfrak{C}_f \tag{1.10}$$

не нарушают минимальность $a^{(1)}$, то $a^{(1)}$ является цилиндрическим f-минимумом решетки Γ.

Доказательство. Определим матрицу $A = (\!(a_i^{(j)})\!)$ со столбцами ${a^{(1)}}^T, \ldots, {a^{(s)}}^T$. Для краткости положим $\rho_j = \rho(a^{(j)})$, $j = \overline{1,s}$. Предположим, что узел

$$\gamma = \sum_{j=1}^{s} k_j a^{(j)}$$

нарушает минимальность $a^{(1)}$. Тогда, ввиду (1.8),

$$\rho(\gamma) \underset{f}{\ll} \rho_1, \quad |\gamma_s| \le a_s, \tag{1.11}$$

а согласно формулам Крамера

$$k_j = \frac{D_j}{\det A}, \quad j = \overline{1,s},$$

где D_j — определитель матрицы, полученной из A заменой j-го столбца на γ^T. Раскладывая определитель D_j по последней строке и используя (1.6), (1.7), (1.11), получаем

$$D_j \underset{f}{\ll} a_s^{(1)} \cdot \prod_{j=2}^{s} \rho_j \underset{f}{\ll} \det \Gamma = |\det A| \implies |k_j| \underset{f}{\ll} 1,$$

т.е. существует такая постоянная C, зависящая только от f, что $|k_j| \le C$ при всех j. Значит, в качестве $\mathfrak{C}_f$ можно взять, например,

$$\mathfrak{C}_f = \{k \in \mathbb{Z}^s \setminus \{0\} : |k|_\infty \le C\}.$$

□

Рассмотрим базис Вороного $\left\{a^{(j)}\right\}_{j=1}^{s}$ решетки Γ, удовлетворяющий дополнительному условию: $a^{(1)}$ — цилиндрический f-минимум Γ. Пусть $A = (\!(a_i^{(j)})\!)$ — соответствующая базисная матрица (со столбцами ${a^{(1)}}^T, \ldots, {a^{(s)}}^T$). Будем называть ее *матрицей Вороного*.

Определим множество $\Omega_{c,f}$, состоящее из всех матриц Вороного решеток из $\mathcal{L}_s(\mathbb{R})$.

Любая матрица $A = (\!(a_i^{(j)})\!) \in \Omega_{c,f}$ обладает следующими свойствами.

j) *Справедливы оценки:* $0 \le a_s^{(j)} < a_s^{(1)}$, $j = \overline{2, s}$.

jj) *Если*

$$b^{(j)} = a^{(j)} - a^{(1)} \cdot \frac{a_s^{(j)}}{a_s^{(1)}}, \quad j = \overline{2, s}$$

— основания гвоздиков с шапочками в точках $a^{(j)}$, то $(b^{(2)}, \ldots, b^{(s)})$ содержится во множестве вполне приведенных базисов $\mathfrak{R}_{s-1}$.

jjj) *Узлы (1.10) не нарушают минимальность $a^{(1)}$.*

Верно и обратное: если матрица $A \in \mathrm{GL}_s(\mathbb{R})$ (со столбцами ${a^{(1)}}^T, \ldots, {a^{(s)}}^T$) удовлетворяет j), jj), jjj), то $A \in \Omega_{c,f}$.

Пусть $\mathrm{D}'_s(\mathbb{R}_+)$ — множество диагональных матриц из $\mathrm{GL}_s(\mathbb{R})$ с главной диагональю вида: $\rho, \rho, \ldots, \rho, h$, где $\rho,\ h \in \mathbb{R}_+$.

Для любой матрицы $X = (\!(x_{ij})\!) \in \mathrm{M}_s(\mathbb{R})$, определим

$$h_j(X) = x_{sj}, \quad \rho_j(X) = \sqrt{\sum_{i=1}^{s-1} x_{ij}^2}, \quad j = \overline{1, s}.$$

Множество Ω_f обладает следующими свойствами.

i) $\Omega_{c,f}$ инвариантно относительно левого действия группы $\mathrm{D}'_s(\mathbb{R}_+)$;

ii) существует такая постоянная $C = C(\Omega) > 0$, что для любой матрицы $X \in \Omega_{c,f}$

$$\begin{aligned} &\max_{1 \le j \le s} |h_j(X)| < h_1(X), \\ &\rho_j(X) \le C \cdot \rho_{j+1}(X), \quad j = \overline{1, s-1}, \\ &h_1(X) \cdot \prod_{j=2}^{s} \rho_j(X) \le C \cdot |\det X|; \end{aligned}$$

iii) граница $\partial\Omega_f$ кусочно-дифференцируемая;

Выполнение i) вытекает из определения матрицы Вороного, условие ii) — из j), (1.7), (1.6). Условие iii) следует из j), jj), jjj).

О множестве $\Omega_{c,f}$ при $s = 3$.

В частном случае $s = 3$, $f(x) = \rho(x)$ условия jjj) можно уточнить.

Пусть $a = (a_1, a_2, a_3)$ — примитивный узел трехмерной решетки Γ и $a_3 > 0$. Пусть l_a — луч, выходящий из начала координат и проходящий через точку $(a_1, a_2, 0)$. На двумерной решетке оснований гвоздиков Λ определим *шестиугольник Зеллинга*, как шестиугольник, составленный из 6 остроугольных (или прямоугольных) примитивных треугольников решетки Λ, сходящихся в начале координат. Определим *основной треугольник Зеллинга*, как тот из шести треугольников через который проходит луч l_a.

Рассмотрим шапочки семи гвоздиков с основаниями в вершинах шестиугольника Зеллинга и в точке $(\beta + \gamma)$, где β и γ — вершины основного треугольника Зеллинга отличные от нуля. Будем называть их *шапочками Вороного*.

Теорема. *Пусть* $s = 3$, $f(x) = \sqrt{x_1^2 + x_2^2}$. *Если шапочки Вороного не нарушают минимальность* a, *то* a *является цилиндрическим* f*-минимумом.*

Теорема была доказана Г.Ф. Вороным [19, 20] (переработанное доказательство см. в [32, глава 5, § 60]) в случае, когда решетка Γ удовлетворяет условию (решетка общего положения):

$$\rho(\gamma) \neq \rho(\eta), \quad |\gamma_s| \neq |\eta_s| \qquad \text{при } \gamma, \eta \in \Gamma, \ \ \eta \neq \gamma. \tag{1.12}$$

Доказательство для произвольных решеток (в том числе и целочисленных) см. в [71].

Таким образом, в случае $s = 3$, $f(x) = \sqrt{x_1^2 + x_2^2}$ условие jjj) можно заменить на следующее

jjj') *шапочки Вороного не нарушают минимальность* a.

Замечание 1.1. Если (1.12) не выполняется, то основной треугольник Зеллинга (и даже шестиугольник Зеллинга) может определяться неоднозначно. Однако утверждение теоремы Вороного остается в силе независимо от выбора этого треугольника (и шестиугольника). Отметим, что в этом случае число рассматриваемых шапочек Вороного можно уменьшить (см. [71]).

§ 2. Среднее количество цилиндрических минимумов.

Определим отображение Ψ, которое каждой матрице $X \in \mathrm{GL}_s(\mathbb{R})$ ставит в соответствие пару $(\Gamma(X), a(X))$, где

$\Gamma(X)$ — решетка с базисной матрицей X (т.е. столбцы X образуют базис $\Gamma(X)$);

$a(X) = (x_{11}, \ldots, x_{s1})$ — узел $\Gamma(X)$ (первый столбец X).

Пусть $\mathfrak{M}_{c,f}(\Gamma)$ — множество цилиндрических f-минимумов решетки Γ и $\mathfrak{M}^+_{c,f}(\Gamma)$ — множество минимумов $a \in \mathfrak{M}_{c,f}(\Gamma)$, удовлетворяющих условию $a_s > 0$.

Определим множество $\mathcal{U}_{c,f}$, состоящее из пар (Γ, a), где $\Gamma \in \mathcal{L}_s(\mathbb{R})$, а $a \in \mathfrak{M}^+_{c,f}(\Gamma)$.

Замечание 2.1. Согласно определениям отображение Ψ взаимно однозначно переводит $\Omega_{c,f}$ на все $\mathcal{U}_{c,f}$. Кроме того, если $M(\Gamma)$ — множество базисных матриц решетки Γ, то

$$\mathfrak{M}^+_{c,f}(\Gamma) = \Big\{ a(M) : M \in \Omega_{c,f} \cap M(\Gamma) \Big\},$$

т.е. множество цилиндрических минимумов, у которых $a_s > 0$, состоит из первых столбцов базисных матриц Вороного. Последнюю формулу можно записать еще так

$$\forall X \in M(\Gamma) \qquad \mathfrak{M}^{+}_{c,f}(\Gamma) = \left\{ a(Y) : Y \in \Omega_{c,f} \cap (X \cdot \mathrm{GL}_s(\mathbb{Z})) \right\}. \tag{2.1}$$

Замечание 2.2. Для любой решетки $\Gamma \in \mathcal{L}_s(\mathbb{R})$ количество минимумов $a \in \mathfrak{M}_{c,f}(\Gamma)$, у которых $a_s = 0$, не больше, чем $O_f(1)$. Если $a \in \mathfrak{M}_{c,f}(\Gamma)$, то $(-a) \in \mathfrak{M}_{c,f}(\Gamma)$.

Используя замечания 2.1, 2.2, можно сводить вычисление усредненного по некоторому множеству решеток числа цилиндрических минимумов к нахождению количества матриц из некоторого подмножества $\Omega_{c,f}$.

Выведем, например, асимптотическую формулу для $E_{c,f}[1, R]$, где

$$E_{c,f}[1, R] = \frac{1}{\mathcal{R}_s[1, R]} \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z};[1,R])} \#\mathfrak{M}_{c,f}(\Gamma)$$

— среднее количество цилиндрических f-минимумов целочисленных s-мерных решеток с определителем из отрезка $[1, R]$.

Согласно условиям i), ii), iii) множество $\Omega_{c,f}$ можно представить в виде

$$\Omega_{c,f} = \mathrm{D}'_s(\mathbb{R}_+) \cdot \Omega'_{c,f} = \left\{ \mathrm{Diag}(\rho, h) \cdot M : \quad M \in \Omega'_{c,f}, \quad \rho, h \in \mathbb{R}_+ \right\},$$

где $\mathrm{Diag}(\rho, h)$ — матрица из $\mathrm{D}'_s(\mathbb{R}_+)$ с главной диагональю $\rho, \rho, \ldots, \rho, h$; а $\Omega'_{c,f}$ — ограниченное множество с кусочно-дифференцируемой границей, лежащее на поверхности

$$\mathcal{S} = \{ X \in \mathrm{GL}_s(\mathbb{R}) : \quad h_1(X) = \rho_s(X) = 1 \}.$$

Определим

$$\mu_c(\Omega_{c,f}) = \int_{\Omega'_{c,f}} \frac{d\mathcal{S}(X)}{|\det X|^s},$$

где $d\mathcal{S}(X)$ — дифференциал $(s^2 - 2)$-мерной меры Лебега поверхности $\mathcal{S}$ в точке X.

Далее будем использовать приложение § A.1. Так как выполняются свойства i), ii), iii), то интеграл $\mu_c(\Omega_{c,f})$ сходится, причем, согласно лемме A.1.1,

$$\# \left\{ M \in \Omega_{c,f} \cap \mathrm{M}_s(\mathbb{Z}) : \ \ 1 \le |\det M| \le R \right\} = \frac{R^s}{s \cdot (s-1)} \left(\mu_c(\Omega_{c,f}) \cdot \ln R + O_f(1) \right). \tag{2.2}$$

Теорема 2.1. *Для любого $R \ge 1$ имеет место следующая асимптотическая формула для среднего числа цилиндрических минимумов*

$$E_{c,f}[1, R] = \mathcal{C}_f \cdot \ln R + O_f(1),$$

где

$$\mathcal{C}_f = \frac{2}{s-1} \cdot \frac{\mu_c(\Omega_{c,f})}{\zeta(2) \cdot \ldots \cdot \zeta(s)}. \tag{2.3}$$

Доказательство. Вычислим сначала $\mathcal{R}_s[1,R] = \#\mathcal{L}_s(\mathbb{Z};[1,R])$. Используя теорему III.2.1, получаем

$$\mathcal{R}_s(n) = \sum_{\substack{m_1,\ldots,m_s\in\mathbb{N},\\ m_1\cdot\ldots\cdot m_s=n}} m_1^{s-1}m_2^{s-2}\cdot\ldots\cdot m_{s-1},$$

$$\mathcal{R}_s([1,R]) = \sum_{1\le n\le R}\mathcal{R}_s(n) = \sum_{\substack{m_1,\ldots,m_s\in\mathbb{N},\\ m_1\cdot\ldots\cdot m_s\le R}} m_1^{s-1}m_2^{s-2}\cdot\ldots\cdot m_{s-1} =$$

$$= \frac{R^s}{s}\sum_{\substack{m_2,\ldots,m_s\in\mathbb{N},\\ m_2\cdot\ldots\cdot m_s\le R}}\frac{1}{m_2^2m_3^3\cdot\ldots\cdot m_s^s} + O_s\left(\sum_{\substack{m_2,\ldots,m_s\in\mathbb{N},\\ m_2\cdot\ldots\cdot m_s\le R}}\frac{R^{s-1}}{m_2m_3^2\cdot\ldots\cdot m_s^{s-1}}\right) =$$

$$= \frac{R^s}{s}\cdot\zeta(2)\cdot\ldots\cdot\zeta(s) + O_s\left(R^{s-1}\cdot\ln R\right). \tag{2.4}$$

Согласно замечанию 2.2

$$\sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};[1,R])}\#\mathfrak{M}_{c,f}(\Gamma) = 2\cdot\sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};[1,R])}\#\mathfrak{M}^+_{c,f}(\Gamma) + O_{s,f}\left(\mathcal{R}_s[1,R]\right).$$

Пусть множество $\mathcal{U}_{c,f}[1,R]$ состоит из всех пар $(\Gamma,a)\in\mathcal{U}_{c,f}$ таких, что $\Gamma\in\mathcal{L}_s(\mathbb{Z};[1,R])$, Тогда

$$\sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};[1,R])}\#\mathfrak{M}^+_{c,f}(\Gamma) = \#\mathcal{U}_{c,f}[1,R].$$

Пусть $\Omega_{c,f}(R)$ — множество всех возможных матриц Вороного для пар из $\mathcal{U}_{c,f}(\mathbb{Z};[1,R])$, т.е. $\mathcal{U}_{c,f}[1,R] = \Psi(\Omega_{c,f}(R))$. Тогда

$$\#\mathcal{U}_{c,f}(\mathbb{Z};[1,R]) = \#\Omega_{c,f}(R).$$

Следовательно,

$$\sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};[1,R])}\#\mathfrak{M}_{c,f}(\Gamma) = 2\cdot\#\Omega_{c,f}(R) + O_{s,f}\left(\mathcal{R}_s[1,R]\right).$$

Множество $\Omega_{c,f}(R)$ состоит из целочисленных $M\in\Omega_{c,f}$, удовлетворяющих условию: $|\det M|\in[1,R]$. Поэтому, учитывая (2.2), получаем

$$\sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};[1,R])}\#\mathfrak{M}_{c,f}(\Gamma) = 2\cdot\frac{R^s}{s\cdot(s-1)}\mu_c(\Omega_{c,f})\cdot\ln R + O_{s,f}\left(\mathcal{R}_s[1,R]\right).$$

Осталось воспользоваться (2.4). □

§ 3. Среднее количество наилучших приближений линейных форм

Считаем, что размерность n рассматриваемых линейных форм и размерность s решеток из предыдущих разделов связаны соотношением: $s = n+1$.

Пусть $\mathfrak{B}_f(\alpha)$ — множество f-наилучших приближений (u, v) линейной формы $L_\alpha x = \alpha_1 x_1 + \ldots + \alpha_n x_n$. Для любого вещественного $P > 1$ определим

$$\mathfrak{B}_f(\alpha, P) = \{(u, v) \in \mathfrak{B}_f(\alpha) : f(u) \le P\}.$$

Возьмем любое вещественное $R > 1$. Пусть множество $\Delta_n(R)$ состоит из рациональных векторов $\alpha \in [0, 1)^{s-1}$ с координатами $\alpha_i = P_i/Q$, где P_i, Q — целые, причем

$$0 \le P_i < Q \le R, \quad i = \overline{1, n}.$$

Определим среднее количество

$$E_{\mathfrak{B},f}([1, R], P) = \frac{1}{\#\Delta_n(R)} \sum_{\alpha \in \Delta_n(R)} \#\mathfrak{B}_f(\alpha, P),$$

f-наилучших приближений линейных форм с рациональными коэффициентами из $\Delta_n(R)$, а также математическое ожидание

$$\mathcal{E}_{\mathfrak{B},f}(P) = \int_{[0,1)^n} \#\mathfrak{B}_f(\alpha, P)\, d\alpha$$

количества f-наилучших приближений (удовлетворяющих условию $f(u) \le P$) линейных форм с вещественными коэффициентами. Нашей целью является получение асимптотических формулы для этих величин.

Для любого $\alpha = (\alpha_1, \ldots, \alpha_{s-1}) \in [0, 1)^{s-1}$ определим решетку Γ_α с базисной матрицей

$$T_\alpha = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ \alpha_1 & \alpha_2 & \ldots & \alpha_{s-1} & 1 \end{pmatrix}, \tag{3.1}$$

то есть Γ_α состоит из узлов вида

$$\gamma = (k_1,\ k_2,\ \ldots,\ k_{s-1},\ k_1\alpha_1 + \ldots + k_{s-1}\alpha_{s-1} - k_s), \quad k_i \in \mathbb{Z}.$$

Согласно определениям

$$\mathfrak{M}_{c,f}(\Gamma_\alpha) = \{(u, L_\alpha u - v) : (u, v) \in \mathfrak{B}_f(\alpha)\}, \tag{3.2}$$

то есть существует взаимно однозначное соответствие между цилиндрическими минимумами решетки Γ_α и наилучшими приближениями линейной формы $L_\alpha x = \alpha_1 x_1 + \ldots + \alpha_n x_n$. Таким образом задача об исследовании наилучших приближений линейных форм сводится к изучению цилиндрических минимумов решеток вида Γ_α. В частности, используя теорему I.3.1, получаем, что для любых $\alpha \in [0, 1)^n$ и $P \ge 2$

$$\#\mathfrak{B}_f(\alpha, P) \underset{f}{\ll} \ln P \tag{3.3}$$

Рассмотрим сначала линейные формы с рациональными коэффициентами.

Дискретный случай

Исследуем некоторые дополнительные свойства множества $\Omega_{c,f}$.

Возьмем любую целочисленную s-мерную решетку Γ и положительные вещественные $r_2 \geq r_1$, $h_2 \geq h_1$. Согласно теореме I.3.1 справедливы оценки

$$\#\{a \in \mathfrak{M}_{c,f}(\Gamma) : \quad r_1 \leq \rho(a) \leq r_2\} \underset{f}{\ll} \ln(r_2/r_1 + 1), \tag{3.4}$$

$$\#\{a \in \mathfrak{M}_{c,f}(\Gamma) : \quad h_1 \leq |a_s| \leq h_2\} \underset{f}{\ll} \ln(h_2/h_1 + 1). \tag{3.5}$$

Лемма 3.1. *Пусть $r \in [1, +\infty)$; Q — целочисленная матрица из $\Omega_{c,f}$. Тогда количество матриц $M \in \Omega_{c,f} \cap (Q \cdot \mathrm{GL}_s(\mathbb{Z}))$, удовлетворяющих условиям:*

$$\rho_1(M) \leq r \text{ либо } h_1(M) \leq r, \tag{3.6}$$

не больше, чем $O_f(\ln r + 1)$.

Доказательство. Пусть Γ — решетка с базисной матрицей Q. Ввиду (2.1) количество матриц $M \in Q \cdot \mathrm{GL}_s(\mathbb{Z})$, удовлетворяющих (3.6), не больше, чем число минимумов $a \in \mathfrak{M}^+_{c,f}(\Gamma(Q))$, у которых $\rho(a) \leq r$ либо $|a_s| \leq r$. Так как решетка $\Gamma(Q)$ целочисленная, то согласно (3.4), (3.5) таких минимумов не больше, чем $O_f(\ln r + 1)$. □

Для любых $\mathbf{P} = (P_1, \ldots, P_{s-1}) \in \mathbb{Z}_+^{s-1}$ и $N \in \mathbb{N}$ определим решетку $\Gamma(\mathbf{P}, N)$ с базисной матрицей $T = T(\mathbf{P}, N)$, где

$$T = \begin{pmatrix} 1 & 0 & \ldots & 0 & 0 \\ 0 & 1 & \ldots & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \ldots & 1 & 0 \\ P_1 & P_2 & \ldots & P_{s-1} & N \end{pmatrix}. \tag{3.7}$$

Пусть $L_s(R)$ — множество, состоящее из решеток $\Gamma(\mathbf{P}, N)$ с целыми P_i, N, удовлетворяющими неравенствам: $0 \leq P_i < N \leq R$, $i = \overline{1, s-1}$. Сразу отметим, что

$$\#L_s(R) = \frac{R^s}{s} + O_s(R^{s-1}). \tag{3.8}$$

Выясним какие матрицы порождают решетки из $L_s(R)$. Также как и в главе II через $d_{s-1}(M)$ обозначаем наибольший общий делитель алгебраических дополнений к элементам последней строки матрицы $M \in \mathrm{M}_s(\mathbb{Z})$.

Лемма 3.2. *Пусть M — целочисленная матрица из $\mathrm{GL}_s(\mathbb{R})$. Пусть $\Gamma = \Gamma(M)$ — решетка с базисной матрицей M. Тогда $\Gamma \in L_s(R)$, если и только, если $|\det M| \in [1, R]$, $d_{s-1}(M) = 1$.*

Доказательство. Пусть $\Gamma \in L_s(R)$. Тогда $\det \Gamma \in [1, R]$ и поэтому $|\det M| \in [1, R]$. Кроме того, существует такой $S \in \mathrm{GL}_s(\mathbb{Z})$, что $M = T \cdot S$, где T — матрица вида (3.7). Так как $d_{s-1}(T) = 1$, то, по лемме II.2.1, $d_{s-1}(M) = 1$.

Пусть $|\det M| \in [1, R]$, $d_{s-1}(M) = 1$. Согласно следствию II.2.1, матрицу M можно представить в виде: $M = T \cdot S$, где $S \in \mathrm{GL}_s(\mathbb{Z})$, а $T \in \mathrm{TM}_s(\mathbb{Z})$ — еще одна базисная матрица Γ. Так как $d_{s-1}(M) = 1$, то по лемме II.2.1, $d_{s-1}(T) = 1$. Значит, $t_{ii} = 1$, $i = \overline{1, s-1}$ и, следовательно, матрица T имеет вид (3.7). Так как $|\det M| \in [1, R]$, то $N \leq R$, т.е. $\Gamma \in L_s(R)$. □

Рассмотрим теперь решетки с базисными матрицами вида (3.1).
Определим функции $\varphi, \psi : [0,1)^{s-1} \to \mathbb{Z}_+$, действующие по формулам

$$\varphi(\alpha) = \#\{a \in \mathfrak{M}^+_{c,f}(\Gamma_\alpha) : \quad f(a_1, \dots, a_{s-1}) \le P\}, \tag{3.9}$$

$$\psi(\alpha) = \#\{a \in \mathfrak{M}^+_{c,f}(\Gamma_\alpha) : \quad f(a_1, \dots, a_{s-1}) \le P, \quad P^{-s} \le a_s\}. \tag{3.10}$$

Лемма 3.3. *Для любых $P, R \in (1, +\infty)$ имеют место асимптотические формулы:*

$$\frac{1}{\#\Delta_{s-1}(R)} \sum_{\alpha \in \Delta_{s-1}(R)} \varphi(\alpha) \;=\; \frac{\mathcal{C}_f}{2} \cdot n \cdot \ln P + O_f(C_{P,R}), \tag{3.11}$$

$$\frac{1}{\#\Delta_{s-1}(R)} \sum_{\alpha \in \Delta_{s-1}(R)} \psi(\alpha) \;=\; \frac{\mathcal{C}_f}{2} \cdot n \cdot \ln P + O_f(C_{P,R}), \tag{3.12}$$

где постоянная $\mathcal{C}_f$ определяется формулой (2.3), а $C_{P,R} = \max\{1, \ln(P^n/R)\}$.

Доказательство. Докажем сначала (3.11) Пусть $\alpha = (P_1/N, \dots, P_{s-1}/N) \in \Delta_{s-1}(R)$. Отображение

$$(x_1, \dots, x_{s-1}, x_s) \in \mathbb{R}^s \to (x_1, \dots, x_{s-1}, N \cdot x_s)$$

взаимно однозначно переводит Γ_α на решетку $\Gamma = \Gamma(\mathbf{P}, N) \in L_s(R)$ при этом цилиндрические минимумы Γ_α переходят в цилиндрические минимумы Γ. Поэтому $\varphi(\alpha) = \varphi(\Gamma)$, где $\varphi(\Gamma)$ — количество минимумов $a \in \mathfrak{M}^+_{c,f}(\Gamma)$ таких, что $f(a_1, \dots, a_{s-1}) \le P$. Пусть

$$\tilde{\varphi}(\Gamma) = \#\{a \in \mathfrak{M}^+_{c,f}(\Gamma) : \rho(a) \le P\}.$$

Если $a \in \mathfrak{M}_{c,f}(\Gamma)$, причем $\rho(a) \le P \le f(a)$ либо $f(a) \le P \le \rho(a)$, то, согласно (1.8), $\rho(a) \underset{f}{\asymp} P$. Ввиду (3.4), таких минимумов, не больше, чем $O_f(1)$. Следовательно,

$$\varphi(\alpha) = \varphi(\Gamma) = \tilde{\varphi}(\Gamma) + O_f(1).$$

Таким образом,

$$\sum_{\alpha \in \Delta_{s-1}(R)} \varphi(\alpha) = \sum_{\Gamma \in L_s(R)} \tilde{\varphi}(\Gamma) + O_f(\#L_s(R)). \tag{3.13}$$

Пусть $\mathcal{U}^*_{c,f} = \mathcal{U}^*_{c,f}(P,R)$ — множество пар $(\Gamma, a) \in \mathcal{U}_{c,f}$, где $\Gamma \in L_s(R)$ и a — минимум из $\mathfrak{M}^+_{c,f}(\Gamma)$, удовлетворяющий условию $\rho(a) \le P$. Тогда

$$\sum_{\Gamma \in L_s(R)} \tilde{\varphi}(\Gamma) = \#\mathcal{U}^*_{c,f}.$$

Определим множество $\Omega^*_{c,f} = \Omega^*_{c,f}(P,R)$, составленное из всех матриц Вороного для пар (Γ, a) из $\mathcal{U}^*_{c,f}$, то есть $\Psi(\Omega^*_{c,f}) = \mathcal{U}^*_{c,f}$. Так как отображение Ψ взаимно однозначное, то $\#\mathcal{U}^*_{c,f} = \#\Omega^*_{c,f}$. Используя определения и лемму 3.2, получаем, что множество $\Omega^*_{c,f}$ состоит из целочисленных матриц $M \in \Omega_{c,f}$ таких, что

$$\rho_1(M) \le P, \quad |\det M| \in [1, R], \quad d_{s-1}(M) = 1.$$

Множество $\Omega = \Omega_{c,f}$ удовлетворяет условиям i)–iv) из § A.1. Поэтому по лемме A.1.2 a)

$$\sum_{\Gamma \in L_s(R)} \tilde{\varphi}(\Gamma) = \#\mathcal{U}^*_{c,f} = \#\Omega^*_{c,f} = \frac{R^s}{s} \left(\frac{\mu_c(\Omega_{c,f})}{\zeta(2) \cdot \ldots \cdot \zeta(s)} \cdot \ln P + O_f(C_{P,R}) \right).$$

Подставляя последнее соотношение в (3.13), получаем (3.11).

Для доказательства (3.12) достаточно повторить рассуждения, использованные при обосновании (3.11). В итоге, получаем

$$\sum_{\alpha\in\Delta_{s-1}(R)} \psi(\alpha) = \#\Omega_{c,f}^{**} + O_f(\#L_s(R)),$$

где $\Omega_{c,f}^{**}$ состоит из целочисленных матриц $M \in \Omega_{c,f}$ таких, что

$$\rho_1(M) \le P, \quad |\det M| \cdot P^{-s} \le h_1(M), \quad |\det M| \in [1, R], \quad d_{s-1}(M) = 1.$$

Применяя для вычисления $\#\Omega_{c,f}^{**}$ лемму А.1.2 б), приходим к требуемой формуле. □

Теорема 3.1. *Для любых $P, R > 1$ справедлива следующая асимптотическая формула для среднего количества f-наилучших приближений линейных форм:*

$$E_{\mathfrak{B},f}([1, R], P) = \frac{2 \cdot \mu_c(\Omega_{c,f})}{\zeta(2) \cdot \ldots \cdot \zeta(n+1)} \cdot \ln P + O_f(C_{P,R}),$$

где $C_{P,R} = \max\{1, \ln(P^n/R)\}$.

Доказательство. Согласно (3.2), для любого $\alpha \in [0, 1)^n$

$$\#\mathfrak{B}_f(\alpha; P) = \#\{a \in \mathfrak{M}_{c,f}(\Gamma_\alpha; P) : f(a_1, \ldots, a_{s-1}) \le P\}.$$

Если $a \in \mathfrak{M}_{c,f}(\Gamma_\alpha)$, то и $(-a) \in \mathfrak{M}_{c,f}(\Gamma_\alpha)$. Поэтому

$$\#\mathfrak{B}_f(\alpha; P) = 2 \cdot \varphi(\alpha) + \xi(\alpha), \tag{3.14}$$

где $\varphi(\alpha)$ определяется (3.9), а $\xi(\alpha)$ — количество таких $a \in \mathfrak{M}_{c,f}(\Gamma_\alpha)$, что $a_s = 0$, $f(a_1, \ldots, a_{s-1}) \le P$. Осталось заметить, что $\xi(\alpha) = O_f(1)$ и применить (3.11). □

Рассмотрим теперь вопрос о среднем количестве *всех* наилучших приближений линейных форм с коэффициентами из $\Delta_n(R)$.

Лемма 3.4. *Существует такая постоянная C_f^*, зависящая только от f, что для любого $\alpha \in \Delta_n(R)$ и любого наилучшего приближения $(u, v) \in \mathfrak{B}_f(\alpha)$, удовлетворяющего условию $L_\alpha u \ne v$, имеет место оценка*

$$f(u) \le C_f^* \cdot R^{1/n},$$

Доказательство. Пусть $\theta = |L_\alpha u - v|$. Согласно (1.8) и определению наилучшего приближения, существует такая константа $C = C(f) > 0$, что выпуклое множество

$$U(\gamma) = \Big\{x \in \mathbb{R}^s : \quad \rho(x) \le C \cdot f(u), \ \ |\alpha x_1 + \ldots + \alpha_n x_n - x_{n+1}| \le \theta\Big\}$$

не содержит ненулевых целочисленных точек. Отметим, что $\theta \ge R^{-1}$. Используя теорему Минковского о выпуклом теле, получаем

$$2^s \ge \operatorname{mes} U(\gamma) \underset{n}{\gg} (C \cdot f(u))^n \cdot \theta \ge (C \cdot f(u))^n \cdot R^{-1}.$$

□

Следствие 3.1. *Для любого* $R > 1$

$$\frac{1}{\#\Delta_n(R)} \sum_{\alpha \in \Delta_n(R)} \#\mathfrak{B}_f(\alpha) = \mathcal{C}_{c,f} \cdot \ln R + O_f(1),$$

где постоянная $\mathcal{C}_f$ *определяется формулой (2.3).*

Доказательство. Для любого $\alpha \in [0,1)^n$ количество $(u,v) \in \mathfrak{B}_f(\alpha)$, удовлетворяющих условию $v = \alpha_1 u_1 + \ldots + \alpha_n u_n$, оценивается величиной $O_f(1)$. Осталось применить лемму 3.4 и теорему 3.1, в которой $P = C_f^* \cdot R^{1/n}$. □

Замечание 3.1. По-видимому, справедлива следующая асимптотическая формула

$$\frac{1}{N^n} \sum_{P_i \in [0,N) \cap \mathbb{Z}} \#\mathfrak{B}_f\left(\frac{P_1}{N}, \ldots, \frac{P_n}{N}\right) \sim \mathcal{C}_{c,f} \cdot \ln N \text{ при } N \to \infty$$

— аналог результата Хейльбронна о средней длине непрерывной дроби для рациональных чисел с *фиксированным* знаменателем. Из результатов настоящей главы вытекает, что

$$\frac{1}{N^n} \sum_{P_i \in [0,N) \cap \mathbb{Z}} \#\mathfrak{B}_f\left(\frac{P_1}{N}, \ldots, \frac{P_n}{N}\right) = 2 \cdot \frac{\#\Omega_{c,f}^*(\mathbb{Z}; N)}{N^n} + O_f(1),$$

где $\Omega_{c,f}^*(\mathbb{Z}; N)$ — множество целочисленных матриц $M \in \Omega_{c,f}$, удовлетворяющих условию $d_{s-1}(M) = 1$ и имеющих *фиксированный* определитель $|\det M| = N$.

Непрерывный случай

Лемма 3.5. *Функция* $\alpha \in [0,1)^n \to \#\mathfrak{B}_f(\alpha, P)$ *измерима по Лебегу.*

Доказательство. Применим формулу (3.14). Если $\xi(\alpha) \neq 0$, то $\alpha_1, \ldots, \alpha_{s-1}$ линейно-зависимы над кольцом $\mathbb{Q}$. Множество таких α имеет меру ноль по Лебегу. Поэтому

$$\#\mathfrak{B}_f(\alpha, P) = 2 \cdot \varphi(\alpha) \text{ почти при всех } \alpha \in [0,1)^{s-1}. \tag{3.15}$$

Осталось доказать, что функция φ измерима по Лебегу. Определим

$$\Omega_{c,f,P} = \{X \in \Omega_{c,f} : f(x_{11}, \ldots, x_{(s-1)1}) \leq P\}.$$

Используя (2.1), получаем

$$\varphi(\alpha) = \#\left(\Omega_{c,f,P} \cap (T_\alpha \cdot \mathrm{GL}_s(\mathbb{Z}))\right) = \sum_{S \in \mathrm{GL}_s(\mathbb{Z})} \chi(\alpha, S),$$

где

$$\chi(\alpha, S) = \begin{cases} 1, & \text{если } T_\alpha \in \Omega_{c,f,P} \cdot S^{-1} \\ 0 & \text{в противном случае} \end{cases},$$

а матрица T_α определяется (3.1), Для любой $S \in \mathrm{GL}_s(\mathbb{Z})$ функция $\alpha \in [0,1)^{s-1} \to \chi(\alpha, S)$ является измеримой по Лебегу, как характеристическая функция некоторого измеримого множества. Значит, φ измерима, как поточечный предел последовательности измеримых функций. □

Замечание 3.2. Пусть ω — связное подмножество $[0,1)^{s-1}$ с липшицевой границей $\partial\omega$. Тогда для любого $R \geq 1$

$$\frac{\#(\omega \cap \Delta_{s-1}(R))}{\#\Delta_{s-1}(R)} = \frac{1}{\#\Delta_{s-1}(R)} \cdot \sum_{1 \leq N \leq R} \#\left(\mathbb{Z}^{s-1} \cap (N \cdot \omega)\right) =$$

$$= \frac{1}{\#\Delta_{s-1}(R)} \cdot \sum_{1 \leq N \leq R} \left(N^{s-1} \cdot \operatorname{mes}\omega + O_\omega\left(N^{s-2}\right)\right) = \operatorname{mes}\omega + O_\omega\left(R^{-1}\right)$$

Вместо $\mathfrak{B}_f(\alpha, P)$, будем рассматривать множество

$$\mathfrak{B}'_f(\alpha, P) = \left\{(u,v) \in \mathfrak{B}_f(\alpha, P) : |L_\alpha u - v| \geq P^{-(n+1)}\right\}. \tag{3.16}$$

Нам нужна оценка меры множества α, для которых $\mathfrak{B}'_f(\alpha, P) \neq \mathfrak{B}_f(\alpha, P)$.

Лемма 3.6. *Пусть $P, Q > 1$. Определим множество $G = G(P,Q)$, состоящее из точек $\alpha \in [0,1)^n$, удовлетворяющих условию: для любой $\alpha \in G$ существует ненулевой целочисленных вектор $(u,v) \in \mathbb{Z}^n \times \mathbb{Z}$ такой, что*

$$|u|_\infty \leq P, \quad |L_\alpha u - v| \leq \frac{1}{Q}. \tag{3.17}$$

Тогда $\operatorname{mes} G \underset{n}{\ll} P^n/Q$.

Доказательство. Возьмем любой ненулевой $(u,v) \in \mathbb{Z}^n \times \mathbb{Z}$. Пусть $g(u,v)$ — множество $\alpha \in [0,1)^n$, удовлетворяющих (3.17). Тогда

$$\operatorname{mes} g(u,v) \leq \frac{2}{Q \cdot |u|_\infty}.$$

Если набор (u,v) удовлетворяет (3.17) с некоторым $\alpha \in [0,1)^n$, то

$$|v| \leq \frac{1}{Q} + |L_\alpha u| \leq (n+1)|u|_\infty.$$

Следовательно,

$$\operatorname{mes} G \leq \sum_{u,v} \operatorname{mes} g(u,v) \leq \sum_{u,v} \frac{2}{Q \cdot |u|_\infty} \underset{n}{\ll} \frac{P^n}{Q},$$

где суммирование ведется по всем $(u,v) \in \mathbb{Z}^n \times \mathbb{Z}$, удовлетворяющим условиям: $1 \leq |u|_\infty \leq P$, $|v| \leq (n+1)|u|_\infty$. □

Теорема 3.2. *Для любого $P \geq 1$ справедлива следующая асимптотическая формула для математического ожидания количества f-наилучших приближений*

$$\mathcal{E}_{\mathfrak{B},f}(P) = \frac{2 \cdot \mu_c(\Omega_{c,f})}{\zeta(2) \cdot \ldots \cdot \zeta(n+1)} \cdot \ln P + O_f(1).$$

Доказательство. Согласно лемме 3.6,

$$\operatorname{mes}\left\{\alpha\in[0,1)^n:\ \ \mathfrak{B}'_f(\alpha,P)\neq\mathfrak{B}_f(\alpha,P)\right\}=O_n(P^{-1}).$$

Поэтому, учитывая (3.3), получаем

$$\int_{[0,1)^n}\#\mathfrak{B}_f(\alpha,P)\,d\alpha=\int_{[0,1)^n}\#\mathfrak{B}'_f(\alpha,P)\,d\alpha+O_f\left(\frac{\ln P+1}{P}\right).$$

Рассуждая также, как и при доказательстве (3.15), приходим к формуле

$$\#\mathfrak{B}'_f(\alpha,P)=2\cdot\psi(\alpha)\text{ почти при всех }\alpha\in[0,1)^n.$$

Следовательно,

$$\mathcal{E}_{\mathfrak{B},f}(P)=2\int_{[0,1)^{s-1}}\psi(\alpha)\,d\alpha+O_f\left(\frac{\ln P+1}{P}\right).\tag{3.18}$$

Также, как и в лемме 3.5, используя (2.1), получаем соотношение

$$\psi(\alpha)=\sum_{S\in\mathrm{GL}_s(\mathbb{Z})}\tilde{\chi}(\alpha,S),$$

где

$$\tilde{\chi}(\alpha,S)=\begin{cases}1, & \text{если } Y_\alpha\cdot S\in\Omega'_{c,f,P}\\ 0 & \text{в противном случае}\end{cases},$$

а множество $\Omega'_{c,f,P}$ состоит из матриц $X\in\Omega_{c,f}$, удовлетворяющих следующим условиям:

1) $f(x_{11},\dots,x_{(s-1)1})\le P$, $h_1(X)\ge P^{-s}$;

2) существуют такие $\alpha\in[0,1)^n$, $S\in\mathrm{GL}_s(\mathbb{Z})$, что $X\cdot S=T_\alpha$, где матрица T_α определяется формулой (3.1) (т.е. $\Gamma(X)=\Gamma_\alpha$).

Согласно свойствам $\Omega_{f,c}$, для любой $X\in\Omega'_{c,f,P}$ справедливы оценки

$$P^{-s}\le h_1(X)=\max_{1\le j\le s}|h_j(X)|,\qquad \rho_1(X)\underset{f}{\ll}\rho_2(X),$$

$$h_1(X)\cdot\prod_{j=2}^{s}\rho_j(X)\underset{f}{\ll}|\det X|=1.$$

Кроме того, $\rho_j(X)\neq 0$ при любом $j\ge 2$ (иначе $\det X=0$). Поскольку первые $(s-1)$ строк матрицы X целочисленные, то $\rho_j(X)\ge 1$. Используя эти соотношения, нетрудно проверить, что множество $\Omega'_{c,f,P}$ ограниченное. Значит, множество $Y_\alpha^{-1}\cdot\Omega'_{f,P}$ ограничено равномерно по α. Поэтому существует такое конечное множество $W\subset\mathrm{GL}_s(\mathbb{Z})$ (зависящее только от P и f), что для любого $\alpha\in[0,1)^{s-1}$

$$\tilde{\chi}(\alpha,S)=0\text{ при }S\notin W,$$

и следовательно,

$$\sum_{S\in W}\tilde{\chi}(\alpha,S)=\sum_{S\in\mathrm{GL}_s(\mathbb{Z})}\tilde{\chi}(\alpha,S)=\psi(\alpha)\tag{3.19}$$

Пусть

$$\omega(S) = \{\alpha \in [0,1)^{s-1} : \ \ Y_\alpha \cdot S \in \Omega'_{c,f,P}\}.$$

Тогда

$$\begin{aligned}\int_{[0,1)^n} \psi(\alpha)\, d\alpha &= \int_{[0,1)^{s-1}} \left(\sum_{S \in W} \tilde{\chi}(\alpha, S) \right) d\alpha = \\ &= \sum_{S \in W} \left(\int_{[0,1)^{s-1}} \tilde{\chi}(\alpha, S)\, d\alpha \right) = \sum_{S \in W} \operatorname{mes} \omega(S). \end{aligned} \tag{3.20}$$

Если множество $\omega(S)$ не пусто, то оно имеет кусочно-дифференцируемую границу (т.к. граница Ω_f кусочно-дифференцируемая). Возьмем любое $R > P$. Ввиду замечания 3.2

$$\operatorname{mes} \omega(S) = \frac{\#(\omega(S) \cap \Delta_{s-1}(R))}{\#\Delta_{s-1}(R)} + O_{\omega(S)}(R^{-1}). \tag{3.21}$$

Согласно (3.19) и (3.12),

$$\begin{aligned}&\sum_{S \in W} \frac{\#(\omega(S) \cap \Delta_{s-1}(R))}{\#\Delta_{s-1}(R)} = \frac{1}{\#\Delta_{s-1}(R)} \sum_{S \in W} \sum_{\alpha \in \Delta_{s-1}(R)} \tilde{\chi}(\alpha, S) = \\ &= \frac{1}{\#\Delta_{s-1}(R)} \sum_{\alpha \in \Delta_{s-1}(R)} \psi(\alpha) = \frac{\mathcal{C}_f}{2} \cdot n \cdot \ln P + O_f(1).\end{aligned}$$

Из последней формулы, а также (3.20), (3.21) вытекает соотношение

$$\int_{[0,1)^n} \psi(\alpha)\, d\alpha = \sum_{S \in \mathcal{S}} \operatorname{mes} \omega(S) = \frac{\mathcal{C}_f}{2} \cdot \ln P + O_f(1) + \sum_{S \in \mathcal{S}} O_{\omega(S)}(R^{-1}).$$

Константы, входящие в символы $O(\ldots)$ не зависят от R. Множество W также не зависит от R. Поэтому, переходя к пределу при $R \to +\infty$, получаем

$$\int_{[0,1)^n} \psi(\alpha)\, d\alpha = \frac{\mathcal{C}_f}{2} \cdot n \cdot \ln P + O_f(1).$$

Осталось подставить последнее соотношение в (3.18). □

В заключение отметим, что аналогичным образом можно исследовать вопросы о статистических свойствах наилучших *совместных* приближений вещественных $\alpha = (\alpha_1, \ldots, \alpha_n)$. Например, чтобы получить асимптотическую формулу для среднего числа f-наилучших совместных приближений рациональных $\alpha \in \Delta_n(R)$, нужно найти количество целочисленных матриц $M \in \Omega_{c,f}$, удовлетворяющих условиям:

$$|\det M| \in [1, R], \quad \text{НОД}\,(m_{s1}, m_{s2}, \ldots, m_{ss}) = 1, \quad \prod_{i=1}^{s-1} D_i(M) = |\det M|^{s-2},$$

где $D_i(M)$ — наибольший общий делитель алгебраических дополнений к элементам i-й строки M.

Глава VI
Среднее количество локальных Φ-минимумов

Пусть $s_0, \ldots, s_r$ — целые числа, причем

$$0 = s_0 < s_1 < \ldots < s_r = s.$$

Положим

$$t_l = s_l - s_{l-1}, \quad l = \overline{1, r}.$$

Пусть функции $\phi_l : \mathbb{R}^{t_l} \to \mathbb{R}$ $(l = \overline{1, r})$ лучевые, непрерывные и кусочно-дифференцируемые. Определим $\mathbf{\Phi} = (\Phi_1, \ldots, \Phi_r) : \mathbb{R}^s \to \mathbb{R}^r$ следующим образом

$$\Phi_1(x) = \phi_1(x_1, \ldots, x_{s_1}), \ldots, \Phi_l(x) = \phi_l(x_{s_{l-1}+1}, \ldots, x_{s_l}), \ldots, \Phi_r(x) = \phi_r(x_{s_{r-1}+1}, \ldots, s).$$

Напомним, что ненулевой узел γ решетки $\Gamma \in \mathcal{L}_s(\mathbb{R})$ мы называем локальным $\mathbf{\Phi}$-минимумом, если не существует ненулевого узла $\eta \in \Gamma$ такого, что

$$\Phi_l(\eta) \leq \Phi_l(\gamma), \quad l = \overline{1, r},$$

причем хотя бы одно из неравенств строгое.

Пусть $\mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$ — множество локальных $\mathbf{\Phi}$-минимумов решетки Γ, а $E_{\mathbf{\Phi}}[1, R]$ — среднее число локальных $\mathbf{\Phi}$-минимумов s-мерных целочисленных решеток с определителем из отрезка $[1, R]$, т.е.

$$E_{\mathbf{\Phi}}[1, R] = \frac{1}{\mathcal{R}_s[1, R]} \sum_{\Gamma \in \mathcal{L}_s(\mathbb{Z}; [1, R])} \#\mathfrak{M}_{\mathbf{\Phi}}(\Gamma).$$

Целью настоящей главы является доказательство асимптотической формулы

$$E_{\mathbf{\Phi}}[1, R] = \mathcal{C}_{\mathbf{\Phi}} \cdot \ln^{r-1} R + O_{\mathbf{\Phi}}(\ln^{r-2} R), \tag{0.1}$$

где $\mathcal{C}_{\mathbf{\Phi}}$ — положительная постоянная, зависящая только от $\mathbf{\Phi}$, а $R \geq 2$.

Для доказательства мы построим процедуру дополнения локального минимума до базиса решетки специального вида. Она похожа на применяемую в главе III для случая относительных минимумов и отлична от использованной для цилиндрических минимумов. В результате, вычисление $E_{\mathbf{\Phi}}[1, R]$ сводится к нахождению количества базисов специального вида, то есть к подсчету целочисленных матриц, лежащих в некотором заданном множестве и имеющих определитель из отрезка $[1, R]$. Для этого

используется лемма A.2.7 из приложения. Основная сложность состоит в построении подходящих базисов решеток.

На протяжении всей главы используем следующие множества индексов

$$I_1 = \{1, \dots, s_1\}, \quad I_2 = \{s_1 + 1, \dots, s_2\}, \dots, I_r = \{s_{r-1} + 1, \dots, s\},$$

т.е. $I_l = \{s_{l-1} + 1, \dots, s_l\}$, $l = \overline{1, r}$.

§ 1. Дополнение локального минимума до базиса: частные случаи

Замечание 1.1. Пусть $\Gamma \in \mathcal{L}_s(\mathbb{R})$ и $b^{(1)}, \dots, b^{(s)}$ — линейно независимые узлы Γ. Тогда существует такой базис $a^{(1)}, \dots, a^{(s)}$ решетки Γ, что [54, глава 1, следствие 2]

$$\begin{gathered} b^{(j)} = \sum_{i=1}^{j} v_{ij} a^{(i)}, \\ 0 < v_{11}; \qquad 0 \le v_{ij} < v_{jj} \quad \text{при } i < j, \quad j = \overline{1, s}. \end{gathered} \tag{1.1}$$

Пусть, дополнительно, $b^{(1)}$ является примитивным узлом Γ. Тогда $v_{11} = 1$, $a^{(1)} = b^{(1)}$. Из (1.1) вытекает, что для любых $k \in \{2, \dots, s\}$, $i \in \{1, \dots, s\}$

$$\left|a_i^{(k)}\right| \le \left|b_i^{(k)}\right| + \sum_{j=1}^{k-1} \left|a_i^{(j)}\right|.$$

Поэтому

$$\left|a_i^{(k)}\right| \le \left|b_i^{(k)}\right| + 2^{k-1} \cdot \sum_{j=1}^{k-1} \frac{1}{2^j} \cdot \left|b_i^{(j)}\right|, \tag{1.2}$$

и следовательно,

$$\left|a_i^{(k)}\right| \underset{s}{\ll} \max_{1 \le j \le k-1} |b_i^{(j)}|. \tag{1.3}$$

Конец замечания.

Из оценки (I.3.9) вытекает, что любой минимум $\gamma \in \mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$ s-мерной решетки Γ удовлетворяет неравенству

$$\prod_{l=1}^{r} (\mathfrak{p}_l(\gamma))^{t_l} \underset{\mathbf{\Phi}}{\ll} \det \Gamma, \tag{1.4}$$

где

$$\mathfrak{p}_l(\gamma) = \max_{i \in I_l} |\gamma_i|.$$

В следующем разделе мы построим процедуру дополнения локального минимума до базиса специального вида, удовлетворяющего некоторому «аналогу» неравенства (1.4). Она состоит из двух частей.

1) Дополняем локальный минимум a до линейно независимой системы узлов $\{a, b^{(2)}, \dots, b^{(s)}\}$, удовлетворяющей некоторому «аналогу» неравенства (1.4).

2) Используя замечание 1.1, получаем базис $\{a, a^{(2)}, \dots, a^{(s)}\}$. Выполнение «аналога» (1.4) вытекает из (1.3).

Основная сложность состоит в построении подходящей линейно независимой системы. В частном случае

$$r = s; \quad \Phi_i(x) = |x_i|, \quad i = \overline{1, s}$$

локальные минимумы являются относительными и соответствующий метод совпадает с использованным в главе III. В общем случае используемая процедура является довольно громоздкой. Поэтому, для наглядности изложения, в этом разделе мы кратко рассмотрим два частных случая:

$$r = 1, \qquad \Phi_1(x) = |x|_\infty = \max_{1 \le i \le s} |x_i|;$$
$$r = 2, \qquad \Phi_1(x) = \mathfrak{p}_1(x), \quad \Phi_2(x) = \mathfrak{p}_2(x).$$

Отметим, что первый случай является «вырожденным» (локальный минимум является первым последовательным минимумом решетки Γ относительно нормы $|\cdot|_\infty$).

Далее всюду в этом разделе считаем, что

$$\epsilon \in (0, 1/s!); \quad \Gamma \in \mathcal{L}_s(\mathbb{R}); \quad a \in \mathfrak{M}_{\mathbf{\Phi}}(\Gamma); \quad \Phi_l(a) \neq 0, \;\; l = \overline{1, r}.$$

Замечание 1.2. Пусть $\Gamma \in \mathcal{L}_s(\mathbb{R})$. По теореме Минковского о линейных формах, для любого $\epsilon > 0$ и $k \in \{1, \dots, s\}$ существует такой $\gamma \in \Gamma \setminus \{0\}$, что $|\gamma_i| \le \epsilon$ при $i \neq k$.

Пример 1: $r = 1$, $\Phi_1(x) = |x|_\infty$

В этом случае условие $a \in \mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$ означает, что не существует ненулевого узла $a' \in \Gamma$ такого, что $|a'|_\infty < |a|_\infty$, то есть a является первым последовательным минимумом Γ. Не умаляя общности, считаем, что $|a_1| = |a|_\infty$.

1-й шаг. Положим $b^{(1)} = a$.

2-й шаг. Определим множество

$$H_2 = \{\gamma \in \Gamma \setminus \{0\} : \quad |\gamma_1| \le \epsilon |a_1|\}.$$

Оно непусто согласно замечанию 1.2. Выберем $b^{(2)} \in H_2$ так, что

$$|b^{(2)}|_\infty = \min_{\gamma \in H_2} |\gamma|_\infty.$$

Таких узлов как минимум два (с противоположными знаками). Чтобы избежать заведомой неоднозначности, наложим дополнительное условие:

$$\exists q \in \{1, \dots, s\} : \quad b_q^{(2)} = |b^{(2)}|_\infty.$$

Отметим, что $|b^{(2)}|_\infty \ge |a|_\infty$, поэтому $q \neq 1$. Пусть, например, $q = 2$, т.е. $b_2^{(2)} = |b^{(2)}|_\infty$

3-й шаг. Определим множество

$$H_3 = \left\{ \gamma \in \Gamma \setminus \{0\} : \quad \begin{array}{l} |\gamma_1| \le \epsilon |a_1|, \\ |\gamma_2| \le \epsilon \cdot b_2^{(2)} \end{array} \right\} = \{\gamma \in H_2 : |\gamma_2| \le \epsilon \cdot b_2^{(2)}\}$$

Оно непусто согласно замечанию 1.2. Возьмем в качестве $b^{(3)}$ такой узел из H_3, что

$$|b^{(3)}|_\infty = \min_{\gamma\in H_3} |\gamma|_\infty;$$
$$\exists q \in \{1,\dots,s\}: \quad b_q^{(3)} = |b^{(3)}|_\infty.$$

Так как $H_3 \subset H_2$, то $|b^{(3)}|_\infty \geq |b^{(2)}|_\infty$, и значит, $q \neq 1, 2$. Пусть, например, $q = 3$.

Продолжая процесс, получаем систему $b^{(1)} = a, b^{(2)}, \dots, b^{(s)}$, которая (возможно, после изменения нумерации координат) удовлетворяет для любого $k \in \{2,\dots,s\}$ условиям

$$b^{(k)} \in H_k = \left\{\gamma \in \Gamma \setminus \{0\}: \quad |\gamma_i| \leq \epsilon |b_i^{(i)}| \text{ при } i < k\right\},$$
$$b_k^{(k)} = |b^{(k)}|_\infty = \min_{\gamma\in H_k} |\gamma|_\infty,$$
$$|b^{(1)}|_\infty \leq |b^{(2)}|_\infty \leq \dots \leq |b^{(s)}|_\infty.$$

Рассмотрим матрицу $B = (\!(b_i^{(j)})\!)$. Максимальный по абсолютной величине элемент каждой строки матрицы находится на главной диагонали, то есть

$$\max_{1\leq j\leq s} |b_i^{(j)}| = b_i^{(i)}, \quad i = \overline{1,s}. \tag{1.5}$$

Кроме того, элементы, лежащие выше главной диагонали, малы, а именно

$$|b_i^{(j)}| \leq \epsilon \cdot b_i^{(i)} \text{ при } j > i. \tag{1.6}$$

Поэтому $\det B \neq 0$, система $\left\{b^{(j)}\right\}_{j=1}^s$ является линейно независимой. Более того,

$$\prod_{i=1}^s b_i^{(i)} < \frac{1}{\epsilon^{s-1}} \cdot \det\Gamma. \tag{1.7}$$

Если (1.7) не выполняется, то по теореме Минковского о линейных формах найдется такой узел $\gamma \in \Gamma \setminus \{0\}$, что $|\gamma_i| \leq \epsilon |b_i^{(i)}|$ $(i = \overline{1,s-1})$, $|\gamma_s| < b_s^{(s)}$. Это противоречит выбору $b^{(s)}$.

Из (1.5), (1.7) и соотношений $b_k^{(k)} = |b^{(k)}|_\infty$ вытекает неравенство

$$\prod_{i=1}^s T_i(B) \underset{s}{\ll} \det\Gamma, \quad T_i(B) = \max\left\{\max_{1\leq j\leq s} |b_i^{(j)}|, \max_{1\leq j\leq s} |b_j^{(i)}|\right\},$$

которое мы и рассматриваем, как аналог (1.4). Такая же оценка будет выполняться и для базиса $\{a^{(j)}\}_{j=1}^s$ из замечания 1.1.

Если $r = 1$, а $\Phi_1 : \mathbb{R}^s \to \mathbb{R}$ есть произвольная лучевая непрерывная функция, то минимум a дополняется до линейно независимой системы, обладающей аналогичными свойствами, точно таким же образом. Единственное отличие состоит в выборе ϵ: нужно взять $\epsilon < 1/(c \cdot s!)$, где

$$c = \frac{c^*}{c_*}, \quad c_* = \min_{|x|_\infty=1} \Phi_1(x), \quad c^* = \max_{|x|_\infty=1} \Phi_1(x).$$

Пример 2: $r = 2$, $\Phi_1(x) = \max\limits_{i\in I_1} |x_i|$, $\Phi_2(x) = \max\limits_{i\in I_2} |x_i|$

Пусть $I_1 = (1, \ldots, s_1)$, $I_2 = (s_1 + 1, \ldots, s)$ и

$$\Phi_l(x) \equiv \mathfrak{p}_l(x) \equiv \max_{i\in I_l} |x_i|, \quad l = 1, 2.$$

Положим $b^{(1)} = a$. Пусть, например, $\mathfrak{p}_1(a) = |a_1|$

Определим множество

$$H_2 = \{\gamma \in \Gamma \setminus \{0\} : \quad |\gamma_1| \le \epsilon |a_1|, \;\; \mathfrak{p}_2(\gamma) \le \mathfrak{p}_2(a)\}$$

и выберем в качестве $b^{(2)}$ такой узел из H_2, что

$$\mathfrak{p}_1(b^{(2)}) = \min_{\gamma\in H_2} \mathfrak{p}_1(\gamma),$$
$$\exists q \in I_1 : \quad b_q^{(2)} = \mathfrak{p}_1(b^{(2)}).$$

Так как $a \in \mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$, то $\mathfrak{p}_1(b^{(2)}) \ge \mathfrak{p}_1(a)$ и поэтому $q \ne 1$. Пусть, например, $q = 2$.

Определим

$$H_3 = \left\{\gamma \in H_2 : \quad |\gamma_2| \le \epsilon |b_2^{(2)}|\right\}$$

и выберем такой $b^{(3)} \in H_3$, что

$$\mathfrak{p}_1(b^{(3)}) = \min_{\gamma\in H_3} \mathfrak{p}_1(\gamma);$$
$$\exists q \in I_1 : \;\; b_q^{(3)} = \mathfrak{p}_1(b^{(3)}).$$

Так как $H_3 \subset H_2$, то $\mathfrak{p}_1(b^{(3)}) \ge \mathfrak{p}_1(b^{(2)})$, и значит, $q \ne 1$, $q \ne 2$.

Продолжая процесс, получаем систему $b^{(1)} = a, b^{(2)}, \ldots, b^{(s_1)}$, которая (возможно, после изменения нумерации координат) удовлетворяет для любого $k \in \{2, \ldots, s_1\}$ условиям

$$b^{(k)} \in H_k = \left\{\gamma \in \Gamma \setminus \{0\} : \quad \begin{array}{ll} |\gamma_i| \le \epsilon |b_i^{(i)}| & \text{при } i < k, \\ \mathfrak{p}_2(\gamma) \le \mathfrak{p}_2(a) & \end{array}\right\},$$
$$b_k^{(k)} = \mathfrak{p}_1(b^{(k)}) = \min_{\gamma\in H_k} \mathfrak{p}_1(\gamma_k),$$
$$\mathfrak{p}_1(b^{(1)}) \le \mathfrak{p}_1(b^{(2)}) \le \ldots \le \mathfrak{p}_1(b^{(s_1)}).$$

Узлы $b^{(s_1+1)}, \ldots, b^{(s)}$ выберем следующим образом. Определим

$$H_{s_1+1} = \left\{\gamma \in \Gamma \setminus \{0\} : \quad |\gamma_i| \le \epsilon |b_i^{(i)}| \text{ при } i \le s_1\right\}$$

и возьмем в качестве $b^{(s_1+1)}$ такой узел из H_{s_1+1}, что

$$\mathfrak{p}_2(b^{(s_1+1)}) = \min_{\gamma\in H_{s_1+1}} \mathfrak{p}_2(\gamma),$$
$$\exists q \in I_2 : \quad b_q^{(s_1+1)} = \mathfrak{p}_2(b^{(s_1+1)}).$$

Тогда $\mathfrak{p}_1(b^{(s_1+1)}) < \mathfrak{p}_1(b^{(s_1)})$. Значит, $b^{(s_1+1)} \notin H_{s_1+1}$. Следовательно,

$$\mathfrak{p}_2(b^{(s_1+1)}) > \mathfrak{p}_2(a).$$

Пусть $q = s_1 + 1$. Определим

$$H_{s_1+2} = \left\{\gamma \in \Gamma \setminus \{0\} : \quad |\gamma_i| \le \epsilon |b_i^{(i)}| \text{ при } i \le s_1 + 1\right\}$$

и выберем $b^{(s_1+2)} \in H_{s_1+2}$ так, что

$$\mathfrak{p}_2(b^{(s_1+2)}) = \min_{\gamma \in H_{s_1+2}} \mathfrak{p}_2(\gamma),$$
$$\exists q \in I_2 : \quad b_q^{(s_1+2)} = \mathfrak{p}_2(b^{(s_1+2)}).$$

Так как $H_{s_1+2} \subset H_{s_1+1}$, то $\mathfrak{p}_2(b^{(s_1+2)}) \ge \mathfrak{p}_2(b^{(s_1+1)})$, поэтому $q \ne s_1+1$. Пусть $q = s_1+2$.

Продолжая процесс, получаем узлы $b^{(s_1+1)}, \dots, b^{(s)}$, которые (возможно, после изменения нумерации координат) удовлетворяют следующим условиям:

$$b^{(k)} \in H_k = \left\{\gamma \in \Gamma \setminus \{0\} : \quad |\gamma_i| \le \epsilon |b_i^{(i)}| \text{ при } i < k\right\},$$
$$b_k^{(k)} = \mathfrak{p}_2(b^{(k)}) = \min_{\gamma \in H_k} \mathfrak{p}_2(\gamma), \quad k = \overline{s_1+1, s},$$
$$\mathfrak{p}_2(a) < \mathfrak{p}_2(b^{(s_1+2)}) \le \mathfrak{p}_2(b^{(s_1+2)}) \le \ldots \le \mathfrak{p}_2(b^{(s)})$$

Полученная система $\{b^{(j)}\}_{j=1}^s$ удовлетворяет соотношениям (1.5), (1.6). Поэтому так же, как и в примере 1, заключаем, что $\{b^{(j)}\}_{j=1}^s$ является линейно независимой и выполняется оценка (1.7). Из (1.7) вытекает неравенство

$$\prod_{i=1}^s T_i(B) \underset{s}{\ll} \det\Gamma; \;\; T_i(B) = \max\left\{\max_{1\le j\le s} |b_i^{(j)}|, \mathfrak{p}_l(b^{(i)})\right\} \text{ при } i \in I_l, \;\; l = 1, 2,$$

которое мы и рассматриваем как аналог (1.4). Соответствующая оценка будет выполняться и для базиса $\{a^{(j)}\}_{j=1}^s$ из замечания 1.1.

Если Φ_1, Φ_2 — произвольные функций, то линейно независимую систему, обладающую подобными свойствами, можно построить таким же образом, если взять $\epsilon < 1/(c \cdot s!)$, где

$$c = \frac{c^*}{c_*}, \quad c_* = \min_{|x|_\infty = 1} \min_{l=1,2} \Phi_l(x), \quad c^* = \max_{|x|_\infty = 1} \max_{l=1,2} \Phi_l(x),$$

а множества H_k при $k = 2, \dots, s_1$ определить следующим образом:

$$H_k = \left\{\gamma \in \Gamma \setminus \{0\} : \quad \begin{array}{ll} |\gamma_i| \le \epsilon |b_i^{(i)}| & \text{при } i < k, \\ \mathfrak{p}_2(\gamma) \le c \cdot \mathfrak{p}_2(a) & \end{array}\right\}.$$

§ 2. Дополнение локального минимума до базиса

Напомним, что функции $\mathfrak{p}_l : \mathbb{R}^s \to \mathbb{R}$ $(l = \overline{1, r})$ действуют по формулам

$$\mathfrak{p}_l(x) = \max_{i \in I_l} |x_i|.$$

Также, как и в § I.3, получаем, что существует такая постоянная $c_{\mathbf{\Phi}} \ge 1$, что

$$\forall x \in \mathbb{R}^s \qquad c_{\mathbf{\Phi}}^{-1/2} \cdot \mathfrak{p}_l(x) \le \Phi_l(x) \le c_{\mathbf{\Phi}}^{1/2} \cdot \mathfrak{p}_l(x); \qquad l = \overline{1, r}.$$

Замечание 2.1. Если $\mathfrak{p}_l(x) \le c_{\mathbf{\Phi}}^{-1} \cdot \mathfrak{p}_l(y)$, то $\Phi_l(x) \le \Phi_l(y)$. Если $\Phi_l(x) \le c_{\mathbf{\Phi}}^{-1} \cdot \Phi_l(y)$, то $\mathfrak{p}_l(x) \le \mathfrak{p}_l(y)$. Поэтому, если $a \in \mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$, $J \subset \{1, \dots, r\}$, то не существует ненулевого узла $\gamma \in \Gamma$, удовлетворяющего неравенствам

$$\begin{array}{ll} \mathfrak{p}_l(\gamma) \le c_{\mathbf{\Phi}}^{-1} \cdot \mathfrak{p}_l(a), & l \in J; \\ \Phi_l(\gamma) \le \Phi_l(a), & l \notin J, \end{array}$$

хотя бы одно из которых является строгим.

Возьмем любую постоянную ϵ такую, что

$$0 < \epsilon < \frac{1}{s! \cdot c_{\mathbf{\Phi}}}.$$

Замечание 2.2. Пусть $x, y \in \mathbb{R}^s$, $l \in \{1, \dots, r\}$, причем $|x_i| \le \epsilon |y_i|$ для всех $i \in I_l$. Тогда $\Phi_l(x) < (s!)^{-1} \Phi_l(y)$.

Пусть $\Gamma \in \mathcal{L}_s(\mathbb{R})$ и a — минимум из $\mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$, причем $\mathfrak{p}_l(a) \ne 0$, $l = \overline{1, r}$

Построим набор номеров $n = (n_1, \dots, n_s) \in \{1, \dots, s\}^s$ и узлов $b^{(1)}, \dots, b^{(s)} \in \Gamma \setminus \{0\}$ следующим образом.

1-й шаг. Полагаем $b^{(1)} = a$; n_1 — любой номер из I_1 для которого $|a_{n_1}| = \mathfrak{p}_1(a)$.

k-й шаг. Пусть $(b_1^{(1)}, \dots, b^{(k-1)})$ и $(n_1, \dots, n_{k-1})$ выбраны. Пусть $l \in \{1, \dots, r\}$ — такой номер, что $k \in I_l$. Определим множество $H_k = H_k(\Gamma; b^{(1)}, \dots, b^{(k-1)}; n_1, \dots, n_{k-1})$ по формуле

$$H_k = \left\{ \gamma \in \Gamma \setminus \{0\} : \quad \begin{array}{ll} |\gamma_{n_i}| \le \epsilon \cdot |b_{n_i}^{(i)}| & \text{при } i < k; \\ \mathfrak{p}_j(\gamma) \le c_{\mathbf{\Phi}}^{-1} \cdot \mathfrak{p}_j(a) & \text{при } j > l. \end{array} \right\}$$

Множество H_k не пусто (согласно замечанию 1.2). Узел $b^{(k)}$ выберем из следующих условий:

$$\begin{aligned} & b^{(k)} \in H_k, \quad \mathfrak{p}_l\left(b^{(k)}\right) = \min_{\gamma \in H_k} \mathfrak{p}_l(\gamma), \\ & \exists q \in I_l : \quad \mathfrak{p}_l(b^{(k)}) = b_q^{(k)}. \end{aligned} \tag{2.1}$$

Положим $n_k = q$.

Таким образом построенную систему $b^{(1)}, \dots, b^{(s)}$ будем называть $(\mathbf{\Phi}; n)$-*подходящей* (для пары (Γ, a)). Отметим, что подходящих систем может быть несколько.

Пусть $(k-1)$ и k принадлежат одному и тому же набору I_l, причем $k \ge 3$. Тогда $H_k \subset H_{k-1}$, и поэтому

$$\mathfrak{p}_l\left(b^{(k-1)}\right) \le \mathfrak{p}_l\left(b^{(k)}\right), \text{ если } (k-1), k \in I_l; \quad k > 2. \tag{2.2}$$

Лемма 2.1. *Пусть $b^{(1)}, \dots, b^{(s)}$ — $(\mathbf{\Phi}; n)$-подходящая система для пары (Γ, a). Тогда для любого $l \in \{1, \dots, r\}$*

$$\mathfrak{p}_l(a) < c_{\mathbf{\Phi}} \cdot \mathfrak{p}_l(b^{(k)}), \quad k \in I_l, \tag{2.3}$$

$$\mathfrak{p}_l(b^{(i)}) \le \mathfrak{p}_l(b^{(k)}), \quad k \in I_l, \quad i = \overline{2, k-1}, \tag{2.4}$$

$$\left(n_{s_{l-1}+1}, \dots, n_{s_l}\right) \text{ — } \textit{перестановка из } I_l. \tag{2.5}$$

Доказательство. Докажем (2.3), используя индукцию по $k = 2, 3, \ldots$.

База индукции. Пусть $k = 2$. Рассмотрим отдельно два случая.

1. Пусть $l = 1$ (т.е. $2 \in I_1$). Тогда $\mathfrak{p}_j\left(b^{(2)}\right) \le c_{\mathbf{\Phi}}^{-1} \cdot \mathfrak{p}_j(a)$ при $j \ge 2$. Следовательно, согласно замечанию 2.1, $\mathfrak{p}_1\left(b^{(2)}\right) > c_{\mathbf{\Phi}}^{-1} \cdot \mathfrak{p}_1(a)$.

2. Пусть $l = 2$ (т.е. $I_1 = \{1\}$). Так как $|b_1^{(2)}| < \epsilon|a_1|$, то $\Phi_1(b^{(2)}) < \Phi_1(a)$. Кроме того, $\mathfrak{p}_j\left(b^{(2)}\right) \le c_{\mathbf{\Phi}}^{-1} \cdot \mathfrak{p}_j(a)$ при $j > 2$, и, ввиду замечания 2.1, $\mathfrak{p}_2(a) < c_{\mathbf{\Phi}} \cdot \mathfrak{p}_2\left(b^{(2)}\right)$.

Индукционный переход от $(k-1)$ к k. Отдельно рассмотрим два случая.

1. Пусть $k = s_{l-1} + 1$ (т.е. набор I_l начинается с номера k). Так как $b^{(k)} \in H_k$, то, используя предположение индукции, получаем $\mathfrak{p}_{l-1}\left(b^{(k)}\right) < \mathfrak{p}_{l-1}\left(b^{(k-1)}\right)$. Значит, $b^{(k)} \notin H_{k-1}$ (иначе возникает противоречие с выбором $b^{(k-1)}$), и поэтому $\mathfrak{p}_l\left(b^{(k)}\right) > c_{\mathbf{\Phi}}^{-1} \cdot \mathfrak{p}_l(a)$.

2. Если $k > s_{l-1} + 1$, то(2.3) вытекает из (2.2) и предположения индукции.

Неравенства (2.3) доказаны. Оценки (2.4) вытекают из (2.2) при $i \in I_l$; и из (2.3), а также из условия $\mathfrak{p}_l(b^{(i)}) \le c_{\mathbf{\Phi}}^{-1} \cdot \mathfrak{p}_l(a)$ при $i \notin I_l$.

Докажем (2.5). Возьмем любой l. По определению, $\{n_{s_{l-1}+1}, \ldots, n_{s_l}\} \subset I_l$. Осталось доказать, что $n_i \ne n_k$ при $s_{l-1} + 1 \le i < k \le s_l$. Для этого заметим следующее.

Если $i = 1$, то $l = 1$. Используя условие $b^{(k)} \in H_k$ и (2.3), получаем

$$\left|b_{n_1}^{(k)}\right| \le \epsilon \cdot |a_{n_1}| < c_{\mathbf{\Phi}}^{-1} \cdot |a_{n_1}| = c_{\mathbf{\Phi}}^{-1} \cdot \mathfrak{p}_1(a) < \mathfrak{p}_1\left(b^{(k)}\right) = b_{n_k}^{(k)};$$

Если $i > 1$, то, учитывая условие $b^{(k)} \in H_k$ и (2.2), имеем

$$\left|b_{n_i}^{(k)}\right| \le \epsilon \cdot \left|b_{n_i}^{(i)}\right| < \mathfrak{p}_l\left(b^{(i)}\right) \le \mathfrak{p}_l\left(b^{(k)}\right) = b_{n_k}^{(k)}.$$

В обоих случаях $n_i \ne n_k$. □

Если $n = (1, 2, \ldots, s)$, то $(\mathbf{\Phi}, n)$-подходящие системы называем $\mathbf{\Phi}$-*подходящими*.

Далее считаем, что минимум a можно дополнить до $\mathbf{\Phi}$-подходящей системы.

Пусть $\{b^{(j)}\}_{j=1}^s$ — $\mathbf{\Phi}$-подходящая система для пары (Γ, a). Тогда для любого $l \in \{1, \ldots, r\}$ и любого $k \in I_l$, справедливы соотношения

$$\left|b_i^{(k)}\right| \le \epsilon \cdot \left|b_i^{(i)}\right|, \quad i = \overline{1, k-1}, \tag{2.6}$$

$$\mathfrak{p}_j\left(b^{(k)}\right) \le c_{\mathbf{\Phi}}^{-1} \cdot \mathfrak{p}_j(a), \quad j = \overline{l+1, r}, \tag{2.7}$$

$$b_k^{(k)} = \mathfrak{p}_l\left(b^{(k)}\right) = \min_{\gamma \in H_k} \mathfrak{p}_l(\gamma), \tag{2.8}$$

где

$$H_k = \left\{ \gamma \in \Gamma \setminus \{0\} : \begin{array}{ll} |\gamma_i| \le \epsilon \cdot |b_i^{(i)}|, & i = \overline{1, k-1}, \\ \mathfrak{p}_j(\gamma) \le c_{\mathbf{\Phi}} \cdot \mathfrak{p}_j(a), & j = \overline{l+1, r} \end{array} \right\}.$$

Кроме того, выполняются (2.3), (2.4).

Лемма 2.2. *Пусть* $\{b^{(j)}\}_{j=1}^s$ — $\mathbf{\Phi}$-*подходящая система для пары* (Γ, a). *Тогда*

а) система $\{b^{(j)}\}_{j=1}^s$ *линейно независимая;*

б) справедлива оценка

$$\prod_{k=1}^{s} b_k^{(k)} \le \frac{1}{\epsilon^{s-1}} \cdot \det \Gamma. \tag{2.9}$$

Доказательство. Докажем утверждение а). Пусть $l \in \{1, \dots, r\}$, $k \in I_l$. Имеем

$$\begin{aligned} &|b_k^{(1)}| < c_\Phi |b_k^{(k)}|, \\ &|b_k^{(j)}| < |b_k^{(k)}| \qquad \text{при } 1 < j < k, \\ &|b_k^{(j)}| < \epsilon |b_k^{(k)}| \qquad \text{при } j > k, \end{aligned} \tag{2.10}$$

Первая оценка следует из (2.3) и условий $b^{(1)} = a$, $\mathfrak{p}_l(b^{(k)}) = |b_k^{(k)}|$; вторая — из (2.4) и соотношений $|b_k^{(j)}| \le \mathfrak{p}_l(b^{(j)})$, $\mathfrak{p}_l(b^{(k)}) = |b_k^{(k)}|$; а третья — из (2.6).

Согласно (2.10) для любой нетождественной перестановки $(m_1, \dots, m_s)$ из $\{1, \dots, s\}$

$$\left| \prod_{i=1}^{s} b_k^{(m_k)} \right| \le \epsilon \cdot c_{\mathbf{\Phi}} \cdot \left| \prod_{k=1}^{s} b_k^{(k)} \right|$$

Значит,

$$\det(\!(b_i^{(j)})\!) \ge \prod_{i=1}^{s} b_i^{(i)} \cdot \Big(1 - (s! - 1) \cdot \epsilon \cdot c_{\mathbf{\Phi}}\Big) > \prod_{i=1}^{s} b_i^{(i)} \cdot \frac{1}{s!}. \tag{2.11}$$

Утверждение а) доказано.

Докажем (б). Если (2.9) не выполняется, то по теореме Минковского о линейных формах найдется такой ненулевой узел $\gamma \in \Gamma$, что

$$|\gamma_i| \le \epsilon \left| b_i^{(i)} \right| \quad \text{при } i < s; \quad |\gamma_s| < b_s^{(s)},$$

то есть $\gamma \in H_s$ и $|\gamma_s| < b_s^{(s)}$. Это противоречит выбору $b^{(s)}$. Утверждение б) доказано. □

Пусть $\{b^{(j)}\}_{j=1}^s$ — Ф-подходящая система для пары (Γ, a). Согласно замечанию 1.1 существует единственный базис $\{a^{(j)}\}_{j=1}^s$ решетки Γ, удовлетворяющий (1.1). Этот базис будем называть **Φ**-*подходящим* (для пары (Γ, a)). Определим матрицы

$$B = (\!(b_i^{(j)})\!), \quad A = (\!(a_i^{(j)})\!), \quad V = (\!(v_{ij})\!)$$

(элементы V, лежащие ниже главной диагонали, считаем равными нулю). Тогда

$$B = A \cdot V. \tag{2.12}$$

Возьмем любое $l \in \{1, \dots, r\}$ и для всех $k \in I_l$ определим

$$T_k(A) = \max \left\{ \max_{1 \le j \le s} \left| a_k^{(j)} \right|, \ \mathfrak{p}_l\left(a^{(k)}\right) \right\} \equiv \max \left\{ \max_{1 \le j \le s} |a_k^{(j)}|, \ \max_{i \in I_l} |a_i^{(k)}| \right\}.$$

Следствие 2.1. *Пусть* $\{b^{(j)}\}_{j=1}^s$ *—* **Φ***-подходящая система,* $\{a^{(j)}\}_{j=1}^s$ *—* **Φ***-подходящий базис для пары* (Γ, a)*, удовлетворяющий (1.1). Тогда*

$$\prod_{i=1}^{s} v_{ii} \le C_1 = \frac{s! \cdot c_{\mathbf{\Phi}}}{\epsilon^{s-1}}, \tag{2.13}$$

$$T_k(A) \le (2^{s-1} c_{\mathbf{\Phi}}) \cdot |b_k^{(k)}|, \quad k = \overline{1, s}, \tag{2.14}$$

$$\prod_{k=1}^{s} T_k(A) \le C_2 \cdot \det \Gamma, \quad C_2 = \frac{2^{s(s-1)} \cdot c_{\mathbf{\Phi}}^s}{\epsilon^{s-1}}. \tag{2.15}$$

Доказательство. Из (2.12), (2.9), (2.10) и из равенства $|\det A| = \det \Gamma$ вытекает

$$\prod_{i=1}^{s} v_{ii} = \det V = \frac{\det B}{\det A} \le \frac{s! \cdot c_{\mathbf{\Phi}}}{\det \Gamma} \cdot \left| \prod_{i=1}^{s} b_i^{(i)} \right| \le \frac{s! \cdot c_{\mathbf{\Phi}}}{\epsilon^{s-1}} = C_1.$$

Оценка (2.13) доказана.

Пусть $l \in \{1, \dots, r\}$, $k \in I_l$. Используя (1.2), (2.10), получаем для любого i

$$\left| a_i^{(k)} \right| \le \left| b_k^{(k)} \right| + 2^{s-2} \cdot \sum_{j=1}^{k-1} \frac{1}{2^j} \cdot \left| b_i^{(j)} \right| \le c_{\mathbf{\Phi}} \cdot \left| b_k^{(k)} \right| \cdot \left(1 + 2^{s-2} \cdot \sum_{j=1}^{s-1} \frac{1}{2^j} \right) = c_{\mathbf{\Phi}} |b_k^{(k)}| 2^{s-1},$$

а используя (1.2), (2.3), (2.4), приходим к

$$\mathfrak{p}_l \left(a^{(k)} \right) \le \mathfrak{p}_l \left(b^{(k)} \right) + 2^{s-2} \cdot \sum_{j=1}^{k-1} \frac{1}{2^j} \cdot \mathfrak{p}_l \left(b^{(j)} \right) \le c_{\mathbf{\Phi}} \cdot \mathfrak{p}_l \left(b^{(k)} \right) \cdot \left(1 + 2^{s-2} \cdot \sum_{j=1}^{s-1} \frac{1}{2^j} \right) = c_{\mathbf{\Phi}} |b_k^{(k)}| 2^{s-1}.$$

Оценка (2.14) доказана. Из (2.14) и (2.9) вытекает (2.15). □

Пусть $\Gamma \in \mathcal{L}_s(\mathbb{R})$, $a \in \mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$, причем

$$\mathfrak{q}_l(a) \ne 0, \quad l = \overline{1, r}$$

и существует $\mathbf{\Phi}$-подходящий базис $a^{(1)}, \dots, a^{(s)}$ для пары (Γ, a). Тогда матрицу $A = (\!(a_i^{(j)})\!)$ будем называть $\mathbf{\Phi}$-*подходящей матрицей* (для пары (Γ, a)).

Пусть множество $\Omega_{\mathbf{\Phi}}$ состоит из всех возможных $\mathbf{\Phi}$-подходящих матриц для пар (Γ, a), где $a \in \mathcal{L}_s(\mathbb{R})$, $a \in \mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$, $\mathfrak{q}_l(a) \ne 0, \quad l = \overline{1, r}$.

Через $\mathrm{D}_I(\mathbb{R}_+)$ обозначим множество, состоящее из таких диагональных матриц $X \in \mathrm{GL}_s(\mathbb{R})$, что $0 < x_{ii}$, $i = \overline{1, s}$, причем $x_{ii} = x_{jj}$, если i, j принадлежат одному и тому же набору I_l.

Справедливы следующие свойства множества $\Omega_{\mathbf{\Phi}}$.

1. Для всех $X \in \Omega_{\mathbf{\Phi}}$ справедлива оценка

$$\prod_{i=1}^{s} T_i(X) \underset{\mathbf{\Phi}}{\ll} |\det X|.$$

2. Множество $\Omega_{\mathbf{\Phi}}$ инвариантно относительного левого действия группы $\mathrm{D}_I(\mathbb{R}_+)$.

Первое свойство вытекает из (2.15), а второе — из определений множества $\Omega_{\mathbf{\Phi}}$, $\mathbf{\Phi}$-подходящей системы и локального $\mathbf{\Phi}$-минимума.

Свойство 2 можно усилить. Если $X \in \mathrm{M}_s(\mathbb{R})$, $l \in \{1, \dots, r\}$, то через $X(I_l) \in \mathrm{M}_{t_l, s}(\mathbb{R})$ обозначаем матрицу, составленную из строк X с номерами из I_l.

Лемма 2.3. *Множество $\Omega_{\mathbf{\Phi}}$ можно представить в виде*

$$\Omega_{\mathbf{\Phi}} = \{X \in \mathrm{GL}_s(\mathbb{R}) : \quad X(I_l) \in V_l, \ \ l = \overline{1, r}\}, \tag{2.16}$$

где каждое V_l является конусом в $\mathrm{M}_{t_l, s}(\mathbb{R})$ с кусочно-дифференцируемой границей.

Доказательство. Рассуждаем также, как и при доказательстве теоремы III.3.1 в). Будем говорить, что множество $\Omega \subset \mathrm{M}_s(\mathbb{R})$ удовлетворяет условию (*), если его можно представить в виде

$$\Omega = \{X \in \mathrm{GL}_s(\mathbb{R}) : \quad X(I_l) \in V_l, \;\; l = \overline{1,r}\},$$

где каждое V_l является множеством (не обязательно конусом) в $\mathrm{M}_{t_l,s}(\mathbb{R})$ с кусочно-дифференцируемой границей. Так как $\Omega_{\mathbf{\Phi}}$ инвариантно относительно левого действия группы $\mathrm{D}_I(\mathbb{R}_+)$, то нам достаточно доказать, что $\Omega_{\mathbf{\Phi}}$ удовлетворяет (*).

Возьмем любую $A = (\!(a_i^{(j)})\!) \in \mathrm{GL}_s(\mathbb{R})$, удовлетворяющую условию $\mathfrak{p}_l(a^{(1)}) \neq 0$, $l = \overline{1,r}$. Определим решетку $\Gamma = \Gamma(A)$ с базисом $\{a^{(j)}\}_{j=1}^s$. Матрица A принадлежит $\Omega_{\mathbf{\Phi}}$ тогда, и только тогда, когда выполняются следующие условия:

а) существует верхнетреугольная целочисленная матрица $V = (\!(v_{ij})\!)$, удовлетворяющая оценкам (1.1), (2.13) такая, что для системы векторов $\{b^{(j)}\}_{j=1}^s$, определенной формулами (1.1), выполняются оценки (2.6), (2.7), (2.10);

б) среди систем $\{b^{(j)}\}_{j=1}^s$ из условия а) найдется хотя бы одна, удовлетворяющая (2.8);

в) вектор $a^{(1)}$ принадлежит $\mathfrak{M}_{\mathbf{\Phi}}(\Gamma)$.

Пусть Ω_1 состоит из матриц $A \in \mathrm{GL}_s(\mathbb{R})$, удовлетворяющих условию а). Очевидно, что для Ω_1 выполняется условие (*), так как множество верхнетреугольных целочисленных матриц V, удовлетворяющих оценкам (1.1), (2.13), конечное. Кроме того, для любой $A \in \Omega_1$ выполняется оценка

$$\prod_{i=1}^{s} \max_{1\le j\le s} |a_{ij}| \underset{\mathbf{\Phi}}{\ll} |\det A|. \tag{2.17}$$

Для этого достаточно заметить следующее:

$$\max_{1\le j\le s} |a_{ij}| \underset{\mathbf{\Phi}}{\ll} |b_k^{(k)}| \quad \text{(доказывается так же, как и (2.14))};$$

$$|\det B| \ge \frac{1}{s!} \prod_{k=1}^{s} |b_k^{(k)}| \quad \text{(доказывается так же, как и (2.11))};$$

$$|\det B| = |\det A| \cdot \det V = |\det A| \cdot \prod_{i=1}^{s} v_{ii} \underset{\mathbf{\Phi}}{\ll} |\det A|.$$

Возьмем любую матрицу $A = (\!(a_i^{(j)})\!) \in \Omega_1$. Пусть $\{b^{(j)}\}_{j=1}^s$ — любая система векторов из условия а). Используя (2.17) и лемму III.3.3, мы видим, что любой узел $\gamma = n_1 a^{(1)} + \ldots + n_s a^{(s)}$, который может нарушать условие (2.8) (т.е. $\exists k, l : \;\; k \in I_l$, $\gamma \in H_k$, $\mathfrak{p}_l(\gamma) < \mathfrak{p}_k(b^{(k)})$), удовлетворяет оценке: $|n_j| \underset{s,c_{\mathbf{\Phi}}}{\ll} 1$. Поэтому множество

$$\Omega_2 = \{A \in \mathrm{GL}_s(\mathbb{R}) : \text{ выполняются а), б)}\}$$

удовлетворяет условию (*). Аналогичным образом доказывается, что множество

$$\Omega_{\mathbf{\Phi}} = \{A \in \mathrm{GL}_s(\mathbb{R}) : \text{ выполняются а), б), в)}\}$$

также удовлетворяет (*). □

Замечание 2.3. Гладкость границы $\partial\Omega_{\mathbf{\Phi}}$ определяется функцией $\mathbf{\Phi}$. Если, например, $\mathbf{\Phi} \in C^n(\mathbb{R}^s)$, то $\partial\Omega_{\mathbf{\Phi}}$ состоит из фиксированного числа поверхностей класса C^n.

§ 3. Среднее количество локальных минимумов

Рассмотрим отображение $\Psi : \mathrm{GL}_s(\mathbb{R}) \to \mathcal{L}_s(\mathbb{R}) \times \mathbb{R}^s$, действующее по правилу: $\Psi(X) = (\Gamma(X), a(X))$, где

$\Gamma(X)$ — решетка с базисной матрицей X (столбцы X образуют базис $\Gamma(X)$);

$a(X) = (x_{11}, \ldots, x_{s1})$ — узел $\Gamma(X)$ (первый столбец X).

Пусть

$$\mathfrak{M}'_{\mathbf{\Phi}}(\Gamma) = \{a \in \mathfrak{M}_{\mathbf{\Phi}}(\Gamma) : \quad \mathfrak{q}_l(a) \neq 0, \;\; l = \overline{1, r}\}.$$

Определим множество пар «решетка-минимум» $U_{\mathbf{\Phi}}$, состоящее из (Γ, a), где $\Gamma \in \mathcal{L}_s(\mathbb{R})$ и a — минимум из $\mathfrak{M}'_{\mathbf{\Phi}}(\Gamma)$.

Пусть $\mathcal{U}_{\mathbf{\Phi}}$ (подмножество $U_{\mathbf{\Phi}}$) состоит из $(\Gamma, a) \in U_{\mathbf{\Phi}}$ таких, что минимум a можно дополнить до $\mathbf{\Phi}$-подходящего базиса.

Справедливы следующие свойства.

1^0. *Оператор Ψ отображает $\Omega_{\mathbf{\Phi}}$ на все $\mathcal{U}_{\mathbf{\Phi}}$* (вытекает из определения $\Omega_{\mathbf{\Phi}}$).

2^0. *Пусть $X \in \Omega'_{\mathbf{\Phi}}$, где $\Omega'_{\mathbf{\Phi}}$ — внутренность $\Omega_{\mathbf{\Phi}}$. Тогда узел $a(X)$ решетки $\Gamma(X)$ можно единственным образом дополнить до $\mathbf{\Phi}$-подходящей системы и нельзя дополнить до какой-то другой $(\mathbf{\Phi}, n)$-подходящей системы* (так как все неравенства для X, входящие в определение $\Omega_{\mathbf{\Phi}}$, будут строгими).

Рассмотрим теперь пары (Γ, a), принадлежащие $U_{\mathbf{\Phi}} \setminus \mathcal{U}_{\mathbf{\Phi}}$. Пусть $J(I)$ — множество наборов $n = (n_1, \ldots, n_s) \in \mathbb{N}^s$, удовлетворяющих (2.5). Для любого $n \in J(I)$ определим оператор ${}^{(n)}\cdot$, меняющий нумерацию координат у векторов и строк у матриц по правилу $(1, 2, \ldots, s) \to (n_1, n_2, \ldots, n_s)$. То есть

если $x = (x_1, \ldots, x_s) \in \mathbb{R}^s$, то ${}^{(n)}x = (x_{n_1}, \ldots, x_{n_s})$;

если $\Gamma \in \mathcal{L}_s(\mathbb{R})$, то ${}^{(n)}\Gamma = \{{}^{(n)}\gamma : \gamma \in \Gamma\}$;

если $X \in \mathrm{M}_s(\mathbb{R})$, то ${}^{(n)}X$ — матрица, i-я строка которой совпадает с n_i-й строкой X.

Из определений и утверждений 1^0, 2^0 вытекают следующие свойства.

3^0. *Пусть ${}^{(n)}\mathcal{U}_{\mathbf{\Phi}} = \big\{\big({}^{(n)}\Gamma, {}^{(n)}a\big) : (\Gamma, a) \in \mathcal{U}_{\mathbf{\Phi}}\big\}$. Тогда $U_{\mathbf{\Phi}} = \bigcup\limits_{n \in J(I)} {}^{(n)}\mathcal{U}_{\mathbf{\Phi}}$.*

Отметим, что множества ${}^{(n)}\mathcal{U}_{\mathbf{\Phi}}$ могут попарно пересекаться.

4^0. *Оператор Ψ отображает ${}^{(n)}\Omega_{\mathbf{\Phi}}$ на все ${}^{(n)}\mathcal{U}_{\mathbf{\Phi}}$. Если $X \in {}^{(n)}\Omega'_{\mathbf{\Phi}}$, то узел $a(X)$ решетки $\Gamma(X)$ можно единственным образом дополнить до $(\mathbf{\Phi}, n)$-подходящей системы и нельзя дополнить до какой-то другой $(\mathbf{\Phi}, k)$-подходящей системы.*

Определим

$\Theta_{\mathbf{\Phi}} = \bigcup\limits_{n \in J(I)} {}^{(n)}\Omega'_{\mathbf{\Phi}}$ — объединение внутренностей всех ${}^{(n)}\Omega_{\mathbf{\Phi}}$,

$\partial\Theta_{\mathbf{\Phi}} = \bigcup\limits_{n \in J(I)} {}^{(n)}\partial\Omega_{\mathbf{\Phi}}$ — граница $\Theta_{\mathbf{\Phi}}$ (объединение границ всех ${}^{(n)}\Omega_{\mathbf{\Phi}}$).

Тогда из утверждений 3^0, 4^0 вытекает следующее свойство.

5^0. *Оператор* Ψ *отображает* $\Theta_{\mathbf{\Phi}} \cup \partial\Theta_{\mathbf{\Phi}}$ *на все* $U_{\mathbf{\Phi}}$ *и взаимно однозначно отображает* $\Theta_{\mathbf{\Phi}}$ *на некоторую часть* $U_{\mathbf{\Phi}}$.

Применим последнее свойство к вычислению среднего количества локальных минимумов.

Пусть $\mathcal{L}^*$ — некоторое подмножество $\mathcal{L}_s(\mathbb{R})$. Определим

$\mathrm{M}^* = \{X \in \mathrm{GL}_s(\mathbb{R}) : \Gamma(X) \in \mathcal{L}^*\}$ — множество всех возможных базисных матриц решеток из $\mathcal{L}^*$;

$\Theta^*_{\mathbf{\Phi}} = \mathrm{M}^* \cap \Theta_{\mathbf{\Phi}}$ — множество всех матриц из $\Theta_{\mathbf{\Phi}}$, которые порождают решетки из $\mathcal{L}^*$;

$\partial\Theta^*_{\mathbf{\Phi}} = \mathrm{M}^* \cap \partial\Theta_{\mathbf{\Phi}}$.

Теорема 3.1. *Пусть* $\mathcal{L}^*$ *— конечное подмножество* $\mathcal{L}_s(\mathbb{R})$*, причем любая решетка из* $\mathcal{L}^*$ *имеет конечное число локальных* $\mathbf{\Phi}$*-минимумов. Тогда справедливы оценки*

$$0 \le \sum_{\Gamma\in\mathcal{L}^*} \#\mathfrak{M}'_{\mathbf{\Phi}}(\Gamma) - \#\Theta^*_{\mathbf{\Phi}} \le \#\partial\Theta^*_{\mathbf{\Phi}}.$$

Доказательство. Пусть $U^*_{\mathbf{\Phi}} = \{(\Gamma, a) : \ \Gamma \in \mathcal{L}^*,\ a \in \mathfrak{M}'_{\mathbf{\Phi}}(\Gamma)\}$. Тогда

$$\sum_{\Gamma\in\mathcal{L}^*} \#\mathfrak{M}'_{\mathbf{\Phi}}(\Gamma) = \#U^*_{\mathbf{\Phi}},$$

Согласно свойству 5^0 оператор Ψ отображает $\Theta^*_{\mathbf{\Phi}} \cup \partial\Theta^*_{\mathbf{\Phi}}$ на все $U^*_{\mathbf{\Phi}}$. Значит,

$$\#U^*_{\mathbf{\Phi}} \le \#\Theta^*_{\mathbf{\Phi}} + \#\partial\Theta^*_{\mathbf{\Phi}}.$$

Согласно этому же свойству оператор Ψ взаимно однозначно отображает $\Theta^*_{\mathbf{\Phi}}$ на некоторую часть $U^*_{\mathbf{\Phi}}$. Поэтому

$$\#\Theta^*_{\mathbf{\Phi}} \le \#U^*_{\mathbf{\Phi}}.$$

Из трех последних соотношений вытекает утверждение теоремы. □

Пусть множество $\mathcal{L}^*$ инвариантно относительно любого изменения нумерации координат вида: $(1, 2, \ldots, s) \to n$, где $n \in J(I)$, то есть

$$\text{если } \Gamma \in \mathcal{L}^*,\ n \in J(I), \ \text{ то } {}^{(n)}\Gamma \in \mathcal{L}^*. \tag{3.1}$$

Следствие 3.1. *Пусть в дополнение к условиям теоремы 3.1 выполняется (3.1). Тогда*

$$\sum_{\Gamma\in\mathcal{L}^*} \#\mathfrak{M}'_{\mathbf{\Phi}}(\Gamma) = \left(\prod_{l=1}^{r} t_l!\right) \cdot \#\Omega^*_{\mathbf{\Phi}} + O_I(\#\partial\Omega^*_{\mathbf{\Phi}}),$$

где $\Omega^*_{\mathbf{\Phi}} = \mathrm{M}^* \cap \Omega_{\mathbf{\Phi}}$, $\partial\Omega^*_{\mathbf{\Phi}} = \mathrm{M}^* \cap \partial\Omega_{\mathbf{\Phi}}$.

Доказательство. Возьмем любое $n \in J(I)$. Из определения ${}^{(n)}\Omega_{\mathbf{\Phi}}$ и условия (3.1) следует, что отображение ${}^{(n)}\cdot$ осуществляет биекцию $\Omega^*_{\mathbf{\Phi}}$ на ${}^{(n)}\Omega^*_{\mathbf{\Phi}} = \mathrm{M}^* \cap {}^{(n)}\Omega_{\mathbf{\Phi}}$ и $\partial\Omega^*_{\mathbf{\Phi}}$ на ${}^{(n)}\partial\Omega^*_{\mathbf{\Phi}} = \mathrm{M}^* \cap {}^{(n)}\partial\Omega_{\mathbf{\Phi}}$. Значит,

$$\begin{aligned} \#\Theta^* &= \sum_{n\in J(I)} \#\left({}^{(n)}\Omega^*_{\mathbf{\Phi}} \setminus {}^{(n)}\partial\Omega^*_{\mathbf{\Phi}}\right) = \#J(I)\cdot\#\Omega^*_{\mathbf{\Phi}} + O_I(\#\partial\Omega^*_{\mathbf{\Phi}}), \\ \#\partial\Theta^* &= \#J(I)\cdot\#\partial\Omega^*_{\mathbf{\Phi}} = O_I(\#\partial\Omega^*_{\mathbf{\Phi}}). \end{aligned}$$

Осталось учесть, что $\#J(I) = t_1!\cdot\ldots\cdot t_r!$ и воспользоваться теоремой 3.1. □

Определение постоянной $\mu_I(\mathcal{P}_I(\Omega_{\mathbf{\Phi}}))$ приведено в приложении (§ A.2).

Теорема 3.2. *Для любого $R \geq 2$ имеет место асимптотическая формула (0.1) для среднего количества локальных $\mathbf{\Phi}$-минимумов, в которой*

$$\mathcal{C}_{\mathbf{\Phi}} = \frac{\mu_I(\mathcal{P}_I(\Omega_{\mathbf{\Phi}}))}{\zeta(2)\cdot\ldots\cdot\zeta(s)}\cdot\frac{1}{(r-1)!}\cdot\prod_{l=1}^{r}(t_l-1)!.$$

Доказательство. Применим следствие 3.1, в котором полагаем $\mathcal{L}^* = \mathcal{L}_s(\mathbb{Z};[1,R])$. Учитывая формулу (V.2.4) для $\mathcal{R}_s[1,R]$ и оценку (I.3.12) для количества минимумов, не принадлежащих $\mathfrak{M}'_{\mathbf{\Phi}}(\Gamma)$, получаем

$$\begin{aligned} E_{\mathbf{\Phi}}[1,R] &= \frac{1}{\mathcal{R}_s[1,R]}\cdot\sum_{\Gamma\in\mathcal{L}_s(\mathbb{Z};[1,R])}\#\mathfrak{M}'(\Gamma) + O_{\mathbf{\Phi}}(\ln^{r-2}R) = \\ &= \frac{t_1!\cdot\ldots\cdot t_r!}{\mathcal{R}_s[1,R]}\cdot\#\Omega_{\mathbf{\Phi}}(\mathbb{Z};[1,R]) + O_{\mathbf{\Phi}}\left(\frac{\#\partial\Omega_{\mathbf{\Phi}}(\mathbb{Z};[1,R])}{R^s} + \ln^{r-2}R\right) = \\ &= \frac{t_1!\cdot\ldots\cdot t_r!}{R^s}\cdot\frac{s}{\zeta(2)\cdot\ldots\cdot\zeta(s)}\cdot\#\Omega_{\mathbf{\Phi}}(\mathbb{Z};[1,R]) + O_{\mathbf{\Phi}}\left(\frac{\#\partial\Omega_{\mathbf{\Phi}}(\mathbb{Z};[1,R])}{R^s} + \ln^{r-2}R\right), \end{aligned}$$

где $\Omega_{\mathbf{\Phi}}(\mathbb{Z};[1,R])$ ($\partial\Omega_{\mathbf{\Phi}}(\mathbb{Z};[1,R])$) — множество целочисленных матриц $M \in \Omega_{\mathbf{\Phi}}$ ($M \in \partial\Omega_{\mathbf{\Phi}}$), удовлетворяющих условию $|\det M| \in [1,R]$.

Множество $\Omega_{\mathbf{\Phi}}$ удовлетворяет условиям j), jj), jjj) из § A.2. Поэтому согласно лемме A.2.7

$$\begin{aligned} &\#\Omega_{\mathbf{\Phi}}(\mathbb{Z};[1,R]) = \frac{1}{s\cdot t_1\cdot\ldots\cdot t_r}\cdot\frac{R^s}{(r-1)!}\cdot\left(\mu_I(\mathcal{P}_I(\Omega_{\mathbf{\Phi}}))\cdot\ln^{r-1}R + O_{\Phi}(\ln^{r-2}R)\right) \\ &\#\partial\Omega_{\mathbf{\Phi}}(\mathbb{Z};[1,R]) = O_{\mathbf{\Phi}}\left(R^s\cdot\ln^{r-2}R\right). \end{aligned}$$

Из приведенных соотношений вытекает требуемая формула. □

Приложения

§ 1. Приложение к главе V

В этом параграфе используем следующие обозначения.

1. $\mathrm{D}'_s(\mathbb{R}_+)$ — множество диагональных матриц размера $s \times s$ с главной диагональю вида $\rho, \rho, \ldots, \rho, h$, где $\rho, h \in \mathbb{R}_+$;

2. Если $X = (\!(x_{ij})\!) \in \mathrm{M}_s(\mathbb{R})$, то

$$h_j(X) = x_{sj}, \quad \rho_j(X) = \sqrt{\sum_{i=1}^{s-1} x_{ij}^2}, \quad j = \overline{1, s}$$

   (цилиндрические координаты j-го столбца).

3. Если M — целочисленная матрица (не обязательно квадратная), то $d_t(M)$ — наибольший общий делитель миноров порядка t, составленных из первых t строк матрицы M. В частности, если $M \in \mathrm{M}_s(\mathbb{Z})$, то $d_{s-1}(M)$ — наибольший общий делитель алгебраических дополнений к элементами последней строки M.

Пусть множество $\Omega \subset \mathrm{GL}_s(\mathbb{R})$ удовлетворяет следующим условиям:

i) Ω инвариантно относительно левого действия группы $\mathrm{D}'_s(\mathbb{R}_+)$;

ii) существует такая постоянная $C > 0$, что для любого $X \in \Omega$

$$\max_{1 \le j \le s} |h_j(X)| \le C \cdot h_1(X), \tag{1.1}$$

$$\rho_j(X) \le C \cdot \rho_{j+1}(X), \quad j = \overline{1, s-1}, \tag{1.2}$$

$$h_1(X) \cdot \prod_{j=2}^{s} \rho_j(X) \le C \cdot |\det X|; \tag{1.3}$$

iii) граница $\partial\Omega$ кусочно-дифференцируемая;

iv) если $r \in [1, +\infty)$, Q — целочисленная матрица из $\mathrm{GL}_s(\mathbb{R})$, то количество матриц $M \in \Omega \cap (Q \cdot \mathrm{GL}_s(\mathbb{Z}))$ таких, что

$$h_1(M) \le r \text{ либо } \rho_1(M) \le r,$$

   не больше, чем $O_\Omega(\ln r + 1)$.

Согласно условиям i), ii), iii) множество Ω можно представить в виде

$$\Omega = \mathrm{D}_s'(\mathbb{R}_+) \cdot \Omega_0 = \left\{ \mathrm{Diag}(\rho, h) \cdot M : \quad M \in \Omega_0, \quad \rho, h \in \mathbb{R}_+ \right\},$$

где $\mathrm{Diag}(\rho, h)$ — матрица из $\mathrm{D}_s'(\mathbb{R}_+)$ с главной диагональю $\rho, \rho, \ldots, \rho, h$; а Ω_0 — ограниченное множество с кусочно-дифференцируемой границей, лежащее на поверхности

$$\mathcal{S} = \{ X \in \mathrm{GL}_s(\mathbb{R}) : \quad h_1(X) = \rho_s(X) = 1 \}.$$

Определим

$$\mu_c(\Omega) = \int_{\Omega_0} \frac{d\mathcal{S}(X)}{|\det X|^s},$$

где $d\mathcal{S}(X)$ — дифференциал (s^2-2)-мерной меры Лебега поверхности $\mathcal{S}$ в точке X.

Если множество Ω удовлетворяет условиям i), ii), iii), то интеграл Лебега $\mu_c(\Omega)$ сходится. Действительно, в этом случае

$$\begin{aligned} \mu_c(\Omega) &\underset{s,C}{\ll} \int_{0<\rho_1<\rho_2<\ldots<\rho_{s-1}<1} \frac{(\rho_1 \cdot \ldots \cdot \rho_{s-1})^{s-2}}{(\rho_2 \cdot \ldots \cdot \rho_{s-1})^{s}} \, d\rho_1 \ldots d\rho_{s-1} = \\ &= \int_{0<\rho_1<\rho_2<\ldots<\rho_{s-1}<1} \frac{\rho_1^{s-2}}{\rho_2^2 \cdot \ldots \cdot \rho_{s-1}^2} \, d\rho_1 \ldots d\rho_{s-1} \leq \\ &\leq \int_{0<\rho_1<\rho_2<\ldots<\rho_{s-1}<1} \frac{d\rho_1 \, d\rho_2 \ldots d\rho_{s-1}}{\rho_2 \cdot \ldots \cdot \rho_{s-1}} = 1. \end{aligned}$$

Основные результаты этого параграфа заключаются в следующих двух леммах.

Лемма 1.1. *Пусть выполняются условия i), ii), iii) (выполнение iv) не требуется). Тогда для любого $R \geq 1$ количество целочисленных матриц $M \in \Omega$, удовлетворяющих условию $|\det M| \in [1, R]$, равно*

$$\frac{R^s}{s \cdot (s-1)} \left(\mu_c(\Omega) \cdot \ln R + O_\Omega(1) \right).$$

Лемма 1.2. *Пусть выполняются условия i)–iv). Возьмем любые $R, P \geq 1$ и определим $C_{P,R} = \max\{1, \ln(P^{s-1}/R)\}$. Тогда*

а) количество целочисленных $M \in \Omega$, удовлетворяющих условиям

$$|\det M| \in [1, R], \qquad d_{s-1}(M) = 1, \qquad \rho_1(M) \leq P. \tag{1.4}$$

равно

$$\frac{R^s}{s} \left(\mu_c(\Omega) \cdot \ln P + O_\Omega(C_{P,R}) \right). \tag{1.5}$$

б) количество целочисленных $M \in \Omega$, удовлетворяющих (1.4) и условию

$$|\det M| \cdot P^{-s} \leq h_1(M). \tag{1.6}$$

равно (1.5)

В основном тексте диссертации используются только эти две леммы. Первая используется в § V.2, а вторая — в § V.3.

Пусть Ω_R — множество матриц $X \in \Omega$, удовлетворяющих условиям:

$$|\det X| \in [1, R], \quad h_1(X) \geq 1, \quad \min_{2 \leq j \leq s} \rho_j(X) \geq 1.$$

Определим также

$$\Omega_{R,P} = \{X \in \Omega_R : \rho_s(X) \leq P\}.$$

Сформулированные выше леммы являются следствиями результатов, полученных при решении следующих двух (связанных между собой) задач. Первая заключается в вычислении количества целочисленных точек в $\Omega_{R,P}$, а вторая — в нахождении числа целочисленных матриц $M \in \Omega_{R,P}$, удовлетворяющих условию $d_{s-1}(M) = 1$. Нас интересует только главный член, поэтому используем элементарные методы.

Количество целочисленных матриц из $\Omega_{R,P}$

Как и в главе II используем следующее обозначение: если S — гиперповерхность из $\mathbb{R}^s$, то

$$\forall \epsilon > 0 \qquad U(S, \epsilon) = \{x \in \mathbb{R}^s : \quad \inf_{y \in S} |x - y|_\infty \leq \epsilon\}$$

— замыкание ϵ-окрестности S относительно нормы $|\cdot|_\infty$. Для вычисления количества целочисленных матриц из $\Omega_{R,P}$ будем использовать следующий элементарный результат.

Лемма 1.3. *Пусть G — ограниченное измеримое по Лебегу множество из $\mathbb{R}^s$. Тогда*

$$|\#(\mathbb{Z}^s \cap G) - \operatorname{mes} G| \leq \operatorname{mes} U(\partial G, 1), \tag{1.7}$$

$$|\#(\mathbb{Z}^s \cap G) - \operatorname{mes} G| \leq \#(\mathbb{Z}^s \cap U(\partial G, 1)). \tag{1.8}$$

Доказательство повторяет рассуждения, использованные при обосновании леммы II.4.1.

Лемма 1.4. *Пусть S — ограниченная кусочно-дифференцируемая гиперповерхность в $\mathbb{R}^n$, $\mathbf{R} = (R_1, \ldots, R_n) \in \mathbb{R}^n_+$, $\epsilon \in \mathbb{R}_+$. Определим параллелепипед $\Pi(\mathbf{R}) = \{x \in \mathbb{R}^n : |x_i| \leq R_i\}$. Тогда*

$$\operatorname{mes}\left(U(S, \epsilon) \cap \Pi(\mathbf{R})\right) \underset{S}{\ll} \epsilon \cdot \sum_{j=1}^{n} \prod_{i \neq j} R_i. \tag{1.9}$$

Доказательство проводится стандартным образом (используя разбиение единицы и локальные координаты задача сводится к случаю, когда S — часть плоскости).

Следствие 1.1. *Пусть S — кусочно-дифференцируемая гиперповерхность в $\mathbb{R}^n$, которая является конусом. Пусть $\mathbf{R}$, ϵ и $\Pi(\mathbf{R})$ такие же, как и в лемме 1.4. Тогда справедлива оценка (1.9).*

Доказательство. Рассмотрим отображение $x \to R^{*-1}x$, где $R^* = \max_{1\le i\le n} R_i$. Оно переводит $U(S,\epsilon)\cap\Pi(\mathbf{R})$ в $U(S',\epsilon')\cap\Pi(\mathbf{R}')$, где

$$S' = \{x \in S : |x|_\infty \le 1\}, \quad \epsilon' = \frac{\epsilon}{R^*}, \quad \mathbf{R}' = \frac{\mathbf{R}}{R^*}.$$

Значит,

$$\operatorname{mes}\left(U(S,\epsilon)\cap\Pi(\mathbf{R})\right) = R^{*n}\cdot \operatorname{mes} U(S',\epsilon')\cap\Pi(\mathbf{R}').$$

Поверхность S' ограниченная. Поэтому, применяя лемму 1.4, получаем

$$\operatorname{mes} U(S',\epsilon')\cap\Pi(\mathbf{R}') \underset{S}{\ll} \epsilon'\cdot\sum_{j=1}^{n}\prod_{i\ne j} R_i' = \frac{\epsilon}{R^{*n}}\cdot\sum_{j=1}^{n}\prod_{i\ne j} R_i.$$

□

Лемма 1.5. *Пусть S — кусочно-дифференцируемая гиперповерхность в $\mathrm{M}_s(\mathbb{R})$, причем либо S ограниченная, либо является конусом. Возьмем любые положительные постоянные C, R, r, ϵ. Тогда мера Лебега множества, состоящего из точек $X \in U(S,\epsilon)$, удовлетворяющих (1.1), (1.2) и неравенствам*

$$|h_1(X)|\cdot\prod_{j=2}^{s}\rho_j(X) \le R, \quad \min\{|h_1(X)|, \rho_s(X)\} \ge r, \tag{1.10}$$

не больше, чем $O_s(\epsilon\cdot R^s/r)$.

Доказательство. Если $R < r^s/C^{s-1}$, то не существует матриц, удовлетворяющих (1.1), (1.2), (1.10). Поэтому далее считаем, что $R \ge r^s/C^{s-1}$.

Если матрица X удовлетворяет (1.1), (1.2), (1.10), то

$$\max_{1\le i\le s-1}|x_{ij}| \le C\cdot(s-1)\cdot\max_{1\le i\le s-1}|x_{i(j+1)}|, \quad j = \overline{1,s-1},$$

$$|h_1(X)| \ge r, \quad \max_{1\le i\le s-1}|x_{i1}| \ge r, \quad h_1(X)\cdot\prod_{j=2}^{s}\max_{1\le i\le s-1}|x_{ij}| \le R.$$

Множество таких X содержится в

$$\bigcup_{(m,n,k)\in Y} U_{m,n,k},$$

где $U_{m,n,k}$ состоит из матриц $X \in \mathrm{M}_s(\mathbb{R})$, удовлетворяющих неравенствам:

$$r2^{m-k_j-1} \le \max_{1\le i\le s-1}|x_{ij}| \le r2^{m-k_j}, \quad j = \overline{1,s-1},$$
$$r2^{m-1} \le \max_{1\le i\le s-1}|x_{is}| \le r2^m,$$
$$r2^{n-1} \le \max_{1\le j\le s}|x_{sj}| \le r2^n,$$

а $Y = Y(R,r,C)$ состоит из таких наборов $(m,n,k_1,\dots,k_{s-1}) \in \mathbb{Z}^{s+1}$, что

$$m \ge -C', \quad n \ge -C',$$
$$k_i \ge k_{i+1} - C',\ i = \overline{1,s-1}; \quad k_1 \le C',$$
$$(s-1)m + n \le \log_2(R/r^s) + (k_2+\ldots+k_{s-1}) + C',$$

где C' — некоторая положительная постоянная, зависящая только от s и C. Поэтому искомая мера оценивается величиной

$$\sum_{(m,n,k)\in Y} \operatorname{mes}\left(U_{m,n,k}\cap U(S,\epsilon)\right).$$

Используя лемму 1.4 и следствие 1.1, получаем

$$\operatorname{mes}\left(U_{m,n,k}\cap U(S,\epsilon)\right) \underset{S}{\ll} \epsilon\cdot(r2^m)^{s-1}(r2^n)^s\prod_{j=1}^{s-1}(r2^{m-k_j})^{s-1}\cdot\left(\frac{1}{r2^n}+\frac{1}{r2^m}+\sum_{j=1}^{s-1}\frac{1}{r2^{m-k_j}}\right).$$

Так как $k_j\geq k_1-jC'$, $n\geq k_1-sC'$, то

$$\operatorname{mes}\left(U_{m,n,k}\cap U(S,\epsilon)\right) \underset{S}{\ll} \epsilon\cdot r^{s^2-1}(g_1(m,n,k)+g_2(m,n,k)),$$

где

$$\begin{aligned} g_1(m,n,k) &= 2^{ms(s-1)}\cdot 2^{n(s-1)}\cdot\prod_{j=1}^{s-1}\frac{1}{2^{k_j(s-1)}},\\ g_2(m,n,k) &= 2^{m(s(s-1)-1)}\cdot 2^{ns}\cdot 2^{k_1}\cdot\prod_{j=1}^{s-1}\frac{1}{2^{k_j(s-1)}}. \end{aligned}$$

Для оценки $\sum g_1$, мы сначала суммируем g_1 по целым m таким, что

$$(s-1)m\leq\log_2(R/r^s)+(k_2+\ldots+k_{s-1})+C'-n,$$

потом по $n\geq -C'$, а потом по $k_j \underset{s,C'}{\ll} 1$, $j=\overline{1,s-1}$. Для оценки $\sum g_2$, мы сначала суммируем g_2 по целым n таким, что

$$n\leq\log_2(R/r^s)+(k_2+\ldots+k_{s-1})+C'-(s-1)m,$$

потом по $m\geq -C'$, а потом по $k_j \underset{s,C'}{\ll} 1$, $j=\overline{1,s-1}$. В результате, получаем

$$\sum_{(m,n,k)\in Y} g_l(m,n,k) \underset{s,C'}{\ll} (R/r^s)^s, \qquad l=1,2.$$

Следовательно,

$$\sum_{(m,n,k)\in Y}\operatorname{mes}\left(U_{m,n,k}\cap U(S,\epsilon)\right) \underset{S}{\ll} \epsilon\cdot r^{s^2-1}\cdot\sum_{(m,n,k)\in Y}\left(g_1(m,n,k)+g_2(m,n,k)\right) \underset{s,C'}{\ll} \epsilon\cdot R^s/r.$$

□

Следствие 1.2. *Пусть* $\epsilon, r\in\mathbb{R}_+$, *причем* $r>2(s-1)\cdot\epsilon$. *Определим*

$$W=\left\{X\in\Omega_{R,P}:\ \ \min\left\{|h_1(X)|,\rho_s(X)\right\}\geq r\right\}.$$

Тогда $\operatorname{mes} U(\partial W,\epsilon) \underset{\Omega}{\ll} \epsilon\cdot R^s/r.$

Доказательство. Используя ii) и условие $r > 2(s-1)\epsilon$, получаем, что любая матрица $X \in U(\partial W, \epsilon)$, удовлетворяет условиям

$$\rho_j(X) \ll \rho_{j+1}(X), \quad j = \overline{1, s-1}; \quad \max_{1\le j\le s} |h_j(X)| \ll |h_1(X)|; \tag{1.11}$$

$$|h_1(X)| \cdot \prod_{j=2}^{s} \rho_j(X) \le R, \quad \min\{|h_1(X)|, \rho_s(X)\} \gg r \tag{1.12}$$

(постоянные в оценках $O(\ldots)$ и $\ll$ зависят только от Ω).

Граница W содержится в объединении трех множеств: S, S_R и $\pi_{P,r}$, где

$$\begin{aligned} &S = \partial\Omega, \\ &S_R = \{X \in \mathrm{M}_s(\mathbb{R}) : |\det X| = R\}, \\ &\pi_{P,r} = \{X \in \mathrm{M}_s(\mathbb{R}) : \quad \rho_s(X) = P \text{ либо } \min\{|h_1(X)|, \rho_s(X)\} = r\}. \end{aligned}$$

Поэтому $U(\partial W, \epsilon) \subset U_1 \cup U_2 \cup U_3$, где

$$\begin{aligned} U_1 &= \{X \in U(S, \epsilon) : \text{ выполняются (1.11), (1.12)}\}, \\ U_2 &= \{X \in U(S_R, \epsilon) : \text{ выполняются (1.11), (1.12)}\}, \\ U_3 &= \{X \in U(\pi_{P,r}, \epsilon) : \text{ выполняются (1.11), (1.12)}\}. \end{aligned}$$

Используя лемму 1.5, получаем $\operatorname{mes} U_1 \ll \epsilon R^s / r$.

Множество S_R зависит от R. Чтобы преодолеть эту проблему рассмотрим множество $U' = R^{-1} \cdot U_2$. Оно состоит из $X \in U(S_1, R^{-1}\epsilon)$, удовлетворяющих (1.11) и

$$|h_1(X)| \cdot \prod_{j=2}^{s} \rho_j(X) \le R^{-(s-1)}, \quad \min\{|h_1(X)|, \rho_s(X)\} \gg r \cdot R^{-1}.$$

Множество $S_1 = \{X \in \mathrm{M}_s(\mathbb{R}) : |\det X| = 1\}$ не зависит от R, P, r. Следовательно, используя лемму 1.5, получаем

$$\operatorname{mes} U' \ll (\epsilon R^{-1}) \frac{(R^{-(s-1))^s}}{r R^{-1}} = \frac{\epsilon}{r R^{s(s-1)}} \quad \Longrightarrow \quad \operatorname{mes} U_2 = R^{s^s} \cdot \operatorname{mes} U' \ll \epsilon \frac{R^s}{r}.$$

Аналогичным образом доказывается, что $\operatorname{mes} U_3 \underset{R}{\ll} \epsilon R^s / r$. □

Лемма 1.6. *Пусть $P, R \in [1, +\infty)$, $C_{P,R} = \max\{1, \ln(P^{s-1}/R)\}$. Тогда количество целочисленных матриц в $\Omega_{R,P}$ равно*

$$\frac{R^s}{s}\left(\mu_c(\Omega) \cdot \ln P + O_\Omega(C_{P,R})\right).$$

Доказательство. Определим множество $\Omega' = \Omega'(R, P)$ по формуле

$$\Omega' = \left\{X \in \Omega_{R,P} : \ \min\{h_1(X), \rho_1(X)\} \ge 2(s-1)\right\}.$$

Рассмотрим множество $\Omega'' = \Omega_{R,P} \setminus \Omega'$, состоящее из таких матриц $X \in \Omega_{R,P}$, что

$$h_1(X) \le 2(s-1) \quad \text{ либо } \quad \rho_1(X)\} \le 2(s-1).$$

Нетрудно получить неравенство

$$\#(\Omega'' \cap \mathrm{M}_s(\mathbb{Z})) \ll R^s.$$

Здесь и далее в этом доказательстве постоянные в оценках $O(\ldots)$ и $\ll$ зависят только от Ω. Согласно лемме 1.3 количество целочисленных точек в Ω' равно $\operatorname{mes}\Omega' + O(\operatorname{mes} U(\partial\Omega', 1))$. Используя следствие 1.2, получаем, что $\operatorname{mes} U(\partial\Omega', 1) = O(R^s)$. Следовательно,

$$\#(\Omega_{R,P} \cap \mathrm{M}_s(\mathbb{Z})) = \#(\Omega' \cap \mathrm{M}_s(\mathbb{Z})) + \#(\Omega'' \cap \mathrm{M}_s(\mathbb{Z})) = \operatorname{mes}\Omega' + O(R^s).$$

Осталось доказать, что

$$\operatorname{mes}\Omega' = \frac{R^s}{s}\left(\mu_c(\Omega)\cdot \ln P + O_\Omega(C_{P,R})\right). \tag{1.13}$$

Для этого мы в интеграле $\operatorname{mes}\Omega' = \int_{\Omega'} dX$ сделаем замену

$$X = \operatorname{Diag}(\rho, h)\cdot X',$$

где $\rho = \rho_s(X)$, $h = h_1(X)$ и $X' \in \mathcal{S}$ (поверхность $\mathcal{S}$ определена в начале параграфа). Тогда

$$dX = (\rho^{s-1})^{s-1}\cdot \rho^{s-2}\cdot h^{s-1}\, d\rho\, dh\, d\mathcal{S}(X')$$

и, учитывая, что

$$|\det X| \in [1, R] \quad\Longleftrightarrow\quad \frac{1}{|\det X'|} \le \rho^{s-1}h \le \frac{R}{|\det X'|},$$

получаем

$$\operatorname{mes}\Omega' = \int_{\Omega_0}\left(\int_{Q(X')} \rho^{s(s-1)-1}h^{s-1}\, d\rho\, dh\right) d\mathcal{S}(X'),$$

где Ω_0 — множество, определенное в начале параграфа,

$$Q(X') = \left\{(\rho,h)\in\mathbb{R}^2_+ :\ \begin{array}{c} 2(s-1)\le\rho\le P,\quad 2(s-1)\le h<\infty,\\ \frac{1}{|\det X'|}\le\rho^{s-1}h\le\frac{R}{|\det X'|}.\end{array}\right\}$$

Для доказательства (1.13) осталось заметить, что

$$\int_{Q(X')} \rho^{s(s-1)-1}h^{s-1}\, d\rho\, dh = \frac{R^s}{s}\cdot\frac{\ln P}{|\det X'|^s} + O_s\left(C_{P,R}\cdot R^s\cdot\frac{1+|\ln|\det X'||}{|\det X'|^s}\right),$$
$$\int_{\Omega_0}\frac{d\mathcal{S}(X')}{|\det X'|^s} = \mu_c(\Omega),\quad \int_{\Omega_0}\frac{1+|\ln|\det X'||}{|\det X'|^s}\, d\mathcal{S}(X') < +\infty,$$

□

Доказательство леммы 1.1. Согласно условиям ii) существует положительная постоянная C_1, зависящая только от s и C, такая, что $\rho_s(X) \le C_1\cdot R^{1/(s-1)}$ для любой $X\in\Omega_R$. Осталось воспользоваться леммой 1.6, в которой $P = C_1\cdot R^{1/(s-1)}$. □

О количестве целочисленных матриц M с $d_t(M) = 1$

Используем следующее обозначение: если $G \subset \mathbb{R}^s$, $\epsilon \in \mathbb{R}_+$, то

$$B(G, \epsilon) = G \cap U(\partial G, s \cdot \epsilon) = \{x \in G : \rho_\infty(x, \partial G) \le s \cdot \epsilon\},$$

где

$$\rho_\infty(x, \partial G) = \inf_{y \in \partial G} |x - y|_\infty.$$

Лемма 1.7. *Пусть $\Gamma \in \mathcal{L}_s(\mathbb{Z}, D)$. Возьмем любое ограниченное измеримое по Лебегу множество G из $\mathbb{R}^s$. Тогда*

$$\#(\Gamma \cap G) = \frac{\#(\mathbb{Z}^s \cap G)}{D} + O\left(\xi_1 + \frac{\xi_2}{D}\right),$$

где ξ_1 — количество точек решетки Γ в $B(G, 2D)$, ξ_2 — количество целочисленных точек в $B(G, 2D)$.

Доказательство. Определим $G' = \{x \in G : \rho_\infty(x, \partial G) > sD\}$. Если $G' = \emptyset$, то утверждение следствия тривиально. Пусть $G' \ne \emptyset$. Тогда

$$G \setminus G' \subset B(G, D), \quad U(\partial G', sD) \subset B(G, 2D).$$

Следовательно,

$$\#(\Gamma \cap G) = \#(\Gamma \cap G') + O(\xi_1), \qquad \#(\mathbb{Z}^s \cap G') = \#(\mathbb{Z}^s \cap G) + O(\xi_2). \tag{1.14}$$

Применим соотношение (II.4.3) для вычисления количества точек множества $\Gamma \cap G'$ и (1.8) для выражения объема G' через количество целочисленных точек в G'. Учитывая, что $\upsilon(\Gamma) \le D$, получаем

$$\#(\Gamma \cap G') = \frac{\operatorname{mes} G'}{D} + O(\xi_1), \qquad \operatorname{mes} G' = \#(\mathbb{Z}^s \cap G') + O(\xi_2).$$

Из двух последних оценок и (1.14) вытекает утверждение леммы. □

Лемма 1.8. *Пусть Θ — ограниченное, измеримое по Лебегу множество из $\mathrm{M}_s(\mathbb{R})$, а $\Theta(\mathbb{Z})$ — множество целочисленных матриц из Θ. Определим*

$$\begin{aligned} g(0) &= \#\Theta(\mathbb{Z}), \\ g(t) &= \#\{M \in \Theta(\mathbb{Z}) : d_t(M) = 1\}, \quad t = \overline{1, s-1}. \end{aligned}$$

Тогда для любого $t \in \{0, \dots, s-2\}$ имеет место формула

$$g(t+1) = \frac{1}{\zeta(s-t)} \cdot g(t) + O\left(\sum_{k \in \mathbb{N}} \left(\xi_1(k) + \frac{\xi_2(k)}{k^{s-t}}\right)\right),$$

где $\xi_1(k)$ — количество целочисленных матриц $M \in B(\Theta, 2k^{s-t})$ таких, что

$$d_t(M) = 1, \quad d_{t+1}(M) \equiv 0 \pmod{k}, \tag{1.15}$$

а $\xi_2(k)$ — количество целочисленных матриц $M \in B(\Theta, 2k^{s-t})$ таких, что $d_t(M) = 1$.

Доказательство. Если $d_{t+1}(M) = 1$, то и $d_t(M) = 1$. Поэтому, используя свойства функции Мебиуса μ, получаем

$$g(t+1) = \sum_{k\in\mathbb{N}} \mu(k)\cdot g(t,k), \tag{1.16}$$

где $g(t,k)$ — количество матриц $M \in \Theta(\mathbb{Z})$, удовлетворяющих (1.15).

Пусть множество Θ' составлено из матриц, полученных из $X \in \Theta$, вычеркиванием $(t+1)$-й строки. Возьмем любую $X' \in \Theta'$ и $x \in \mathbb{R}^s$. Между t-й и $(t+1)$-й строкой X' вставим x в качестве еще одной строки и обозначим полученную матрицу через $\mathcal{M}_t(X', x) \in \mathrm{M}_s(\mathbb{R})$, то есть

$$\mathcal{M}_t(X',x) = \begin{pmatrix} x'_{11} & x'_{12} & x'_{13} & \dots & x'_{1s} \\ \vdots & \vdots & \vdots & & \vdots \\ x'_{t1} & x'_{t2} & x'_{t3} & \dots & x'_{ts} \\ x_1 & x_2 & x_3 & \dots & x_s \\ x'_{(t+1)1} & x'_{(t+1)2} & x'_{(t+1)3} & \dots & x'_{(t+1)s} \\ \vdots & \vdots & \vdots & & \vdots \\ x'_{(s-1)1} & x'_{(s-1)2} & x'_{(s-1)3} & \dots & x'_{(s-1)s} \end{pmatrix}.$$

Пусть $G(X') = \{x \in \mathbb{R}^s : \mathcal{M}_t(X', x) \in \Theta\}$. Тогда

$$\begin{aligned} \Theta &= \{\mathcal{M}_t(X',x) : \quad X' \in \Theta',\ x \in G(X')\}, \\ g(t,k) &= \sum_{M'\in\Theta'(\mathbb{Z}),\ d_t(M')=1} \#\left(\Gamma(M',k)\cap G(M')\right), \end{aligned} \tag{1.17}$$

где $\Gamma(M',k)$ — решетка, состоящая из решений $m \in \mathbb{Z}^s$ сравнения

$$d_{t+1}(\mathcal{M}_t(M',m)) \equiv 0 \pmod{k}.$$

Так как $d_t(M') = 1$, то по лемме II.3.2, $\det\Gamma(M',k) = k^{s-t}$. Применяя лемму 1.7, получаем

$$\#\left(\Gamma(M',k)\cap G(M')\right) = \frac{1}{k^{s-t}}\cdot\#(\mathbb{Z}^s\cap G(M')) + O\left(\eta_1(M',k) + \frac{\eta_2(M',k)}{k^{s-t}}\right), \tag{1.18}$$

где $\eta_1(M',k)$ — количество узлов решетки $\Gamma'(M',k)$ в $B(G(M'), 2k^{s-t})$, а $\eta_2(M',k)$ — количество целочисленных точек в $B(G(M'), 2k^{s-t})$.

Если $X = \mathcal{M}_t(X', x)$, причем $\rho_\infty(x, \partial G(X')) \le r$, то $\rho_\infty(X, \partial\Theta) \le r$. Поэтому

$$\sum_{M'\in\Theta'(\mathbb{Z}),\ d_t(M')=1} \eta_i(M',k) \le \xi_i(k), \quad i = 1,2. \tag{1.19}$$

Кроме того,

$$\sum_{M'\in\Theta'(\mathbb{Z}),\ d_t(M')=1} \#(\mathbb{Z}^s\cap G(M')) = g(t).$$

Используя (1.16), (1.17), (1.18), (1.19), получаем

$$\begin{aligned} g(t+1) &= \sum_{k\in\mathbb{N}}\mu(k) \sum_{\substack{M'\in\Theta'(\mathbb{Z}),\\ d_t(M')=1}} \#(\Gamma(M',k)\cap G(M')) = \\ &= \sum_{k\in\mathbb{N}}\mu(k)\left(\frac{g(t)}{k^{s-t}} + O\left(\xi_1(k) + \frac{\xi_2(k)}{k^{s-t}}\right)\right). \end{aligned}$$

Осталось заметить, что

$$\sum_{k\in\mathbb{N}} \frac{\mu(k)}{k^{s-t}} = \frac{1}{\zeta(s-t)}.$$

□

Количество целочисленных $M \in \Omega_{R,P}$ таких, что $d_{s-1}(M) = 1$

Чтобы применить лемму 1.8 к множеству $\Theta = \Omega_{R,P}$ нам понадобятся некоторые вспомогательные результаты, которые будут использоваться для оценки $\xi_1(k)$, $\xi_2(k)$.

Как и в главе II будем использовать множество $\mathrm{TM}_s(\mathbb{Z})$, состоящее из целочисленных невырожденных нижнетреугольных матриц $T = (\!(t_{ij})\!) \in \mathrm{M}_s(\mathbb{Z})$ таких, что для любого i

$$\begin{array}{ll} 0 < t_{ii}, & \\ 0 \le t_{ij} < t_{ii} & \text{при } j < i. \\ t_{ij} = 0 & \text{при } j > i, \end{array}$$

Лемма 1.9. *Пусть $r \in [1, +\infty)$, $d \in \mathbb{N}$, $t \in \{0, 1, \ldots, s-2\}$. Тогда количество целочисленных матриц $M \in \Omega_R$, удовлетворяющих условиям:*

$$d_{t+1}(M) \equiv 0 \pmod{d}; \tag{1.20}$$

$$\rho_1(M) \le r \text{ } \textit{либо} \text{ } h_1(M) \le r, \tag{1.21}$$

не больше, чем

$$O_\Omega\left(R^s \cdot \ln(r+1) \cdot \frac{\sigma_{-1}(d)}{d^{s-t}}\right).$$

Доказательство. Пусть

$$T(R,d) = \{T \in \mathrm{TM}_s(\mathbb{Z}) : \ \ d_{t+1}(T) \equiv 0 \pmod{d}, \ \ \det T \in [1,R]\}.$$

Согласно следствию II.2.1 и лемме II.2.1, любая матрица $M \in \mathrm{M}_s(\mathbb{Z})$ такая, что

$$|\det M| \in [1,R], \quad d_{t+1}(M) \equiv 0 \pmod{d},$$

единственным образом представима в виде: $M = T \cdot S$, где $T \in T(R,d)$, $S \in \mathrm{GL}_s(\mathbb{Z})$. Кроме того, $\Omega_R \cap \mathrm{M}_s(\mathbb{Z}) = \{M \in \Omega \cap \mathrm{M}_s(\mathbb{Z}) : \ \ |\det M| \in [1,R]\}$. Поэтому количество целочисленных матриц $M \in \Omega_R$, удовлетворяющих (1.20), (1.21), равно

$$\sum_{T\in T(R,d)} \#\{M \in \Omega \cap (T \cdot \mathrm{GL}_s(\mathbb{Z})) : \text{ выполняется (1.21)}\}.$$

Применяя условие iv), получаем что искомое количество оценивается величиной

$$O_\Omega\left(\ln(r+1) \cdot \#T(R,d)\right).$$

Осталось заметить (см. доказательство леммы II.2.3), что

$$\#T(R,d) \underset{s}{\ll} R^s \cdot \sigma_{-1}(d) \cdot d^{-(s-t)}.$$

□

Следствие 1.3. *Пусть* $t \in \{0, 1, \ldots, s-2\}$, $d \in \mathbb{N}$, $\epsilon \in [1, +\infty)$. *Пусть* $v = v(\Omega, R, d, \epsilon)$ *— количество целочисленных матриц* $M \in B(\Omega_{R,P}, \epsilon)$, *удовлетворяющих сравнению:* $d_{t+1}(M) \equiv 0 \pmod{d}$. *Тогда*

$$v \underset{\Omega}{\ll} R^s \cdot \frac{\sigma_{-1}(d) \cdot (1 + \ln(\epsilon \cdot d))}{d^{s-t}}.$$

Доказательство. Оценим v следующим образом: $v \le v_1 + v_2$, где v_1 — количество целочисленных матриц $M \in \Omega_R$, удовлетворяющих (1.20), (1.21), а v_2 — количество целочисленных матриц $M \in B(\Omega_{R,P}, \epsilon)$ таких, что $\min\{|h_1(M)|, \rho_1(M)\} \ge r$. Здесь $r = 2(s-1) \cdot (\epsilon + 1) \cdot d^{s-t}$. Применяя лемму 1.9 для оценки v_1 и лемму 1.5 для оценки v_2, получаем

$$v_1 \underset{\Omega}{\ll} R^s \cdot \frac{\sigma_{-1}(d) \cdot (1 + \ln(\epsilon \cdot d))}{d^{s-t}}, \quad v_2 \underset{\Omega}{\ll} \frac{R^s}{d^{s-t}}.$$

□

Всюду ниже до конца параграфа считаем, что

$$P, R \in [1, +\infty), \quad C_{P,R} = \max\{1, \ln(P^{s-1}/R)\}.$$

Лемма 1.10. *Пусть* $t \in \{0, 1, \ldots, s-2\}$ *и* $F(t+1)$ *— количество целочисленных матриц* $M \in \Omega_{R,P}$ *таких, что* $d_{t+1}(M) = 1$. *Тогда*

$$F(t+1) = \left(\prod_{k=s-t}^{s} \zeta(k) \right)^{-1} \cdot F(0) + O_\Omega(R^s),$$

где $F(0)$ *— количество целочисленных матриц* $M \in \Omega_{R,P}$.

Доказательство. Используем индукцию по $t = -1, 0, 1, 2, \ldots, s-2$.

При $t = -1$ утверждение леммы тривиально.

Индукционный переход от t к $t+1$. Согласно лемме 1.8

$$F(t+1) = \frac{1}{\zeta(s-t)} F(t) + O\left(\sum_{k \in \mathbb{N}} \left(\xi_1(k) + \frac{\xi_2(k)}{k^{s-t}} \right) \right), \tag{1.22}$$

где $\xi_1(k)$ — количество целочисленных матриц $M \in B(\Omega_{R,P}, 2k^{s-t})$ таких, что $d_{t+1}(M) \equiv 0 \pmod{k}$, а $\xi_2(k)$ — количество целочисленных матриц $M \in B(\Omega_R, 2k^{s-t})$.

Будем использовать следствие 1.3 для оценки $\xi_1(k)$ и $\xi_2(k)$ (выбираем $\epsilon = 2k^{s-t}$, $d = k$ для ξ_1 и $\epsilon = 2k^{s-t}$, $d = 1$ для ξ_2). В итоге, получаем

$$\begin{aligned}
&\xi_1(k) \underset{\Omega}{\ll} R^s \cdot \frac{\sigma_{-1}(k) \cdot (\ln k + 1)}{k^{s-t}}, \\
&\xi_2(k) \underset{\Omega}{\ll} R^s \cdot \sigma_{-1}(k) \cdot (\ln k + 1), \\
&\sum_{k \in \mathbb{N}} \left(\xi_1(k) + \frac{\xi_2(k)}{k^{s-t}} \right) \underset{\Omega}{\ll} R^s \cdot \sum_{k \in \mathbb{N}} \frac{\sigma_{-1}(k) \cdot (1 + \ln k)}{k^{s-t}} \ll R^s.
\end{aligned}$$

Осталось применить (1.22) и предположение индукции. □

Следствие 1.4. *Количество целочисленных матриц $M \in \Omega_{R,P}$, удовлетворяющих условию $d_{s-1}(M) = 1$, равно*

$$\frac{R^s}{s}\left(\frac{\mu_c(\Omega)}{\zeta(2)\cdot\ldots\cdot\zeta(s)}\cdot\ln P + O_\Omega(C_{P,R})\right). \tag{1.23}$$

Для доказательства достаточно воспользоваться леммами 1.10, 1.6.

Лемма 1.11. *Количество целочисленных матриц $M \in \Omega_R$ таких, что $\rho_1(M) \le P < \rho_s(M)$, не больше, чем $O_{s,C}(R^s)$.*

Доказательство. Используя условия ii), получаем, что искомое число, не превосходит $O(S(R,P,C,s))$, где

$$S(R,P,C,s) = \sum\left(h^{s-1}\cdot\prod_{i=1}^{s}\rho_i^{s-2}\right)$$

— сумма по всем целым $(\rho,h) = (\rho_1,\ldots,\rho_s,h) \in \mathbb{Z}_+^{s+1}$, удовлетворяющим условиям

$$\rho \in \Upsilon = \left\{\rho \in \mathbb{Z}_+^s : \ \rho_i \ll \rho_{i+1},\ \ i = \overline{1,s-1};\quad \rho_1 \ll P \ll \rho_s\right\},$$
$$h\cdot\prod_{i=2}^{s}\rho_i \ll R.$$

Здесь и далее в этом доказательстве постоянные в оценках $O(\ldots)$ и $\ll$ зависят только от s и C. Суммируя по $h \ll R/(\rho_2\cdot\ldots\cdot\rho_s)$, получаем

$$S(R,P,C,s) \ll R^s\sum_{\rho\in\Upsilon}\frac{\rho_1^{s-2}}{\rho_2^2\cdot\ldots\cdot\rho_s^2}$$

Множество Υ разобьем на части: $\Upsilon_1,\ldots,\Upsilon_{s-1}$ так, что

$$\forall\rho\in\Upsilon_l \quad \rho_l \ll P \ll \rho_{l+1}.$$

Возьмем любое $l \in \{1,\ldots,s-1\}$. Суммируя сначала по $\rho_i \gg P$, $i = \overline{l+1,s}$, а потом по $\rho_1 \ll \rho_2$, $\rho_2 \ll \rho_3,\ldots,\ \rho_{l-1} \ll \rho_l$, $\rho_l \ll P$, получаем

$$R^s\sum_{\rho\in\Upsilon_l}\frac{\rho_1^{s-2}}{\rho_2^2\cdot\ldots\cdot\rho_s^2} \ll \frac{R^s}{P^{s-l}}\sum\frac{\rho_1^{s-2}}{\rho_2^2\cdot\rho_3^2\cdot\ldots\cdot\rho_l^2} \ll$$
$$\ll \frac{R^s}{P^{s-l}}\sum\frac{\rho_2^{s-3}}{\rho_3^2\cdot\ldots\cdot\rho_l^2} \ll \ldots \ll \frac{R^s}{P^{s-l}}\sum_{1\le\rho_l\ll P}\rho_l^{s-l-1} \ll R^s.$$

В силу произвольности l, доказали, что $S(R,P,C,s) \ll R^s$. □

Доказательство леммы 1.2. Для доказательства утверждения а) достаточно воспользоваться леммой 1.11 и следствием 1.4.

Докажем б). Пусть M — целочисленная матрица из Ω, удовлетворяющая условиям (1.4) и не удовлетворяющая (1.6). Применяя ii), получаем

$$|\det M| \underset{C,s}{\ll} h_1(M)\cdot\prod_{j=2}^{s}\rho_j(M) \underset{C,s}{\ll} \left(|\det M|\cdot P^{-s}\right)\cdot(\rho_s(M))^{s-1}.$$

Следовательно, $\rho_s(M) \underset{C,s}{\gg} P$. Согласно лемме 1.11 таких матриц, не больше, чем $O_{C,s}(R^s)$. Используя утверждение а), приходим к требуемой формуле. □

§ 2. Приложение к главе VI

Пусть целые $s_0, s_1, \ldots, s_r$ удовлетворяют условиям:

$$0 = s_0 < s_1 < \ldots < s_r = s.$$

Для каждого $l \in \{1, \ldots, r\}$ определим

$$I_l = \{s_{l-1} + 1, \ldots, s_l\}, \quad t_l = s_l - s_{l-1}.$$

Тогда

$$\{1, \ldots, s\} = I_1 \cup \ldots \cup I_r; \quad I_l \cap I_j = \emptyset \text{ при } l \neq j; \quad \#I_l = t_l.$$

Положим

$$I = (I_1, \ldots, I_r).$$

Для любой матрицы $X = (\!(x_{ij})\!) \in \mathrm{M}_s(\mathbb{R})$ и номера $i \in I_l$, где $l \in \{1, \ldots, r\}$, определим

$$T_i(X) = \max\left\{\max_{1 \leq j \leq s} |x_{ij}|, \max_{k \in I_l} |x_{ki}|\right\}.$$

Пусть $\mathrm{D}_I(\mathbb{R}_+)$ — множество, состоящее из диагональных матриц $X \in \mathrm{GL}_s(\mathbb{R})$ с положительными элементами на главной диагонали таких, что, если i, j принадлежат одному и тому же набору I_l, то $x_{ii} = x_{jj}$.

Пусть Ω — связное множество из $\mathrm{GL}_s(\mathbb{R})$, удовлетворяющее следующим условиям:

j) Ω инвариантно относительно левого действия группы $\mathrm{D}_I(\mathbb{R}_+)$;

jj) существует такая постоянная $C = C(\Omega) > 0$, что для всех $X \in \Omega$

$$\prod_{i=1}^{s} T_i(X) \leq C \cdot |\det X|;$$

jjj) граница Ω является кусочно-дифференцируемой.

Целью настоящего раздела является получение асимптотической формулы для количества целочисленных матриц $M \in \Omega$ таких, что $|\det M| \in [1, R]$.

Лемма 2.1. *Пусть $P, C_1 \in [1, +\infty)$. Определим множество V_P, состоящее из таких матриц $X = (\!(x_{ij})\!) \in \mathrm{GL}_s(\mathbb{R})$, что*

$$\prod_{i=1}^{s} T_i(X) \leq P; \tag{2.1}$$

$$1 \leq T^{(l)}(X) = \max_{i \in I_l} T_i(X), \quad l = \overline{1, r}; \tag{2.2}$$

$$T_i(X) \leq C_1 |x_{ii}|, \quad i = \overline{1, s}. \tag{2.3}$$

Тогда $\operatorname{mes} V_P = O_{I, C_1}(P^s \ln^{r-1} P + 1)$.

Доказательство. Не умаляя общности считаем, что матрицы $X \in V_P$ удовлетворяют следующему дополнительному условию:

$$\max_{i \in I_l} |x_{ii}| = |x_{s_l s_l}|, \quad l = \overline{1,r}. \tag{2.4}$$

Пусть $X \in V_P$. Положим $y_i = |x_{ii}|$, $i = \overline{1,s}$. Тогда для всех $l \in \{1,\dots,r\}$, $i \in I_l \setminus \{s_l\}$

$$\begin{aligned} &|x_{ij}| \le C_1 \cdot y_i, \quad j \in \{1,\dots,s\} \setminus \{i\}; \\ &|x_{s_l i}| \le C_1 \cdot y_i; \\ &|x_{s_l j}| \le C_1 \cdot y_{s_l}, \quad j \in \{1,\dots,s\} \setminus I_l, \end{aligned}$$

Поэтому, интегрируя по x_{ij} с $i \ne j$, получаем

$$\operatorname{mes} V_P = \int_{V_P} dX \le (2C_1)^{s(s-1)} \int_Y f(y)\, dy,$$

где

$$f(y) = \prod_{l=1}^{r} \left(y_{s_l}^{s-t_l} \cdot \prod_{i \in I_l \setminus \{s_l\}} y_i^s \right),$$

$$Y = \left\{ y \in \mathbb{R}_+^s : \quad C_1^{-1} \le y_{s_l} = \max_{i \in I_l} y_i,\ l = \overline{1,r};\ \prod_{i=1}^{s} y_i \le P \right\}.$$

Сделаем замену:

$$y_i = z_i \cdot z_{s_l} \text{ при } i \in I_l \setminus \{s_l\}, \quad y_{s_l} = z_{s_l}, \quad l = \overline{1,r}.$$

Тогда

$$dy = \left(\prod_{l=1}^{r} z_{s_l}^{t_l - 1} \right) dz, \quad f(y) = \prod_{l=1}^{r} \left(z_{s_l}^{st_l - t_l} \cdot \prod_{i \in I_l \setminus \{s_l\}} z_i^s \right),$$

$$f(y)\, dy = g(z)\, dz, \qquad g(z) = \prod_{l=1}^{r} \left(z_{s_l}^{st_l - 1} \cdot \prod_{i \in I_l \setminus \{s_l\}} z_i^s \right),$$

$$\int_Y f(y)\, dy = \int_Z g(z)\, dz,$$

где Z состоит из точек $z \in \mathbb{R}_+^s$ таких, что

$$\begin{aligned} &z_i \le 1 \text{ при } i \in \{1,\dots,s\} \setminus \{s_1,\dots,s_r\}, \\ &C_1^{-1} \le z_{s_l}, \ \ l = \overline{1,r}, \\ &\left(\prod_{l=1}^{r} z_{s_l}^{t_l} \right) \cdot \prod_{\substack{1 \le i \le s, \\ i \notin \{s_1,\dots,s_r\}}} z_i \le P. \end{aligned}$$

Интегрируя по z_{s_r}, получаем

$$\int_Z g(z)\, dz \underset{I, C_1}{\ll} P^s \int_{Z'} \frac{dz_1\, dz_2 \dots dz_{s-1}}{z_{s_1} z_{s_2} \cdot \ldots \cdot z_{s_{r-1}}},$$

где Z' состоит из $z \in \mathbb{R}_+^{s-1}$ таких, что

$$z_i \le 1 \text{ при } i \in \{1,\dots,s-1\} \setminus \{s_1,\dots,s_{r-1}\},$$
$$C_1^{-1} \le z_{s_l}, \quad l = \overline{1, r-1},$$
$$\left(\prod_{l=1}^{r-1} z_{s_l}^{t_l}\right) \cdot \prod_{\substack{1\le i\le s,\\ i\notin\{s_1,\dots,s_r\}}} z_i \le C_1^{t_r} P.$$

Учитывая, что для любого $z \in Z'$, $l \in \{1,\dots,r-1\}$

$$z_{s_l} \ll P \cdot \left(\prod_{\substack{1\le i\le s-1,\\ i\notin\{s_1,\dots,s_r\}}} z_i\right)^{-1},$$

получаем

$$\int_{Z'} \frac{dz_1 \dots dz_{s_l-1}}{z_{s_1} \cdot \ldots \cdot z_{s_{l-1}}} \underset{s,r,C_1}{\ll} \prod_{l=1}^{r-1} \left(\ln P + \int_0^1 |\ln\tau|\, d\tau\right) = (\ln P + 1)^{r-1}.$$

□

Следствие 2.1. *Пусть* $C_1 \in [1,+\infty)$, $P \in [2,+\infty)$, $\epsilon \in \mathbb{R}_+$. *Определим множество* $V_{P,\epsilon}$, *состоящее из матриц* $X \in \mathrm{M}_s(\mathbb{R})$ *таких, что*

$$\prod_{i\in J} T_i(X) \le P \quad \text{при всех } J \subset \{1,\dots,s\}, \tag{2.5}$$
$$T_i(X) \le C_1 |x_{ii}|, \quad i = \overline{1,s}, \tag{2.6}$$
$$\exists (i,j) : |x_{ij}| \le \epsilon. \tag{2.7}$$

Тогда $\operatorname{mes} V_{P,\epsilon} \underset{C_1,I}{\ll} \epsilon \cdot P^s \cdot \ln^{r-2} P$.

Для доказательства достаточно повторить рассуждения, использованные при обосновании леммы 2.1.

Рассмотрим многообразие $\mathrm{P}_I(\mathbb{R}) = \mathrm{D}_I(\mathbb{R}_+)\backslash\mathrm{GL}_s(\mathbb{R})$, которое является проективизацией $\mathrm{GL}_s(\mathbb{R})$ относительно левого действия группы $\mathrm{D}_I(\mathbb{R}_+)$. Через $\mathcal{P}_I(\Omega)$ обозначаем образ $\Omega \subset \mathrm{GL}_s(\mathbb{R})$ при проективизации $\mathrm{GL}_s(\mathbb{R}) \to \mathrm{P}_I(\mathbb{R})$.

Пусть $k = ((k_1', k_1''), \dots, (k_r', k_r''))$ — набор пар номеров таких, что

$$k_l' \in I_l \text{ при } l \in I_l;$$
$$k_i'' \in \{1,\dots,s\}; \qquad k_i'' \ne k_j'' \quad \text{при } i \ne j.$$

Пусть $\theta = (\theta_1,\dots,\theta_r)$, $\theta_i = \pm 1$. Определим множества

$$\mathrm{GL}_I(\mathbb{R};k;\theta) = \{X \in \mathrm{GL}_s(\mathbb{R}) : \ x_{k_i'k_i''} = \theta_i, \ \ i = \overline{1,r}\},$$
$$\mathrm{P}_I(\mathbb{R};k;\theta) = \mathcal{P}_I(\mathrm{GL}_I(\mathbb{R};k;\theta)).$$

Множество $\mathrm{P}_I(\mathbb{R})$ содержится в объединении всех $\mathrm{P}_I(\mathbb{R},k,\theta)$. Кроме того, каждый элемент из $\mathrm{P}_s(\mathbb{R},k,\theta)$ имеет единственный прообраз при проективизации

$$\mathrm{GL}_I(\mathbb{R},k,\theta) \to \mathrm{P}_I(\mathbb{R},k,\theta). \tag{2.8}$$

Значит, множество всех $\mathrm{P}_I(\mathbb{R},k,\theta)$ образует атлас многообразия $\mathrm{P}_I(\mathbb{R})$, а матрицы из $\mathrm{GL}_I(\mathbb{R},k,\theta)$ являются координатами соответствующих элементов $\mathrm{P}_I(\mathbb{R},k,\theta)$.

Определим меру μ_I на (фиксированной) карте $\mathrm{P}_I(\mathbb{R};k;\theta)$ следующим образом:

$$\mu_I(w)=\int_W \frac{dL(X)}{|\det X|^s} \text{ при } w\subset \mathrm{P}_I(\mathbb{R};k;\theta),$$

где W — прообраз w при проективизации (2.8), $dL(X)$ — дифференциал (s^2-r)-мерной меры Лебега поверхности $L=\mathrm{GL}_I(\mathbb{R};k;\theta)$ в точке X. Также, как и в § II.1 проверяется, что мера μ_I не зависит от выбора карты и поэтому корректно определена на всем многообразии $\mathrm{P}_I(\mathbb{R})$. Достаточное условие μ_I-измеримости множества вытекает из следующей леммы.

Лемма 2.2. *Пусть W — ограниченное, измеримое по Лебегу множество, лежащее на поверхности $L=\{X\in \mathrm{GL}_s(\mathbb{R}):\quad x_{s_ls_l}=1,\ \ l=\overline{1,r}\}$, причем*

$$T_i(X)\underset{W}{\ll} x_{ii},\quad i=\overline{1,s};\qquad \prod_{i=1}^{s} x_{ii}\underset{W}{\ll}|\det X|.$$

Тогда интеграл Лебега

$$\nu(W)=\int_W \frac{|\ln|\det X||}{|\det X|^s}\,dL(X)$$

существует и конечен.

Доказательство. Из условий леммы вытекает, что для любой $X\in W$

$$T_{s_l}(X)\asymp 1,\ \ l=\overline{1,r};\quad |\det X|\asymp \prod_{i\in\Upsilon(I)} x_{ii},$$

где $\Upsilon(I)=\{1,\dots,s\}\setminus\{s_1,\dots,s_r\}$. Здесь и далее в этом доказательстве постоянные в оценках $O(\dots)$ и $\ll$ зависят только от W. Значит,

$$\nu(W)\ll\int_W \frac{\sum_{i\in\Upsilon(I)}\ln x_{ii}}{\prod_{i\in\Upsilon(I)} x_{ii}^s}\,dL(X).$$

Интегрируя по всем x_{ij} с $i\neq j$, учитывая, что при любом $l\in\{1,\dots,r\}$

$$\max\left\{|x_{s_li}|,\max_{j\neq i}|x_{ij}|\right\}\ll x_{ii},\ \ i\in I_l\setminus\{s_l\};$$
$$\max_{j\neq s_l}|x_{s_lj}|\ll 1,$$

получаем

$$\nu(W)\ll\prod_{i\in\Upsilon(I)}\int_{|x_{ii}|\ll 1}|\ln x_{ii}|\,dx_{ii}\ll\int_0^1|\ln t|\,dt=1.$$

□

Пусть

$$\Omega_R=\left\{X\in\Omega:\quad |\det X|\in[1,R],\ \ T^{(l)}(X)=\max_{i\in I_l}T_i(X)\geq 1,\ \ l=\overline{1,r}\right\}. \tag{2.9}$$

Лемма 2.3. *Пусть множество* $\Omega \subset \mathrm{GL}_s(\mathbb{R})$ *удовлетворяет условиям j), jj), jjj) и (2.3). Тогда множество* $\mathcal{P}_I(\Omega)$ *является* μ_I*-измеримым и для любого* $R \geq 2$ *справедлива асимптотическая формула*

$$\operatorname{mes}\Omega_R = \frac{1}{s \cdot t_1 \cdot \ldots \cdot t_r} \cdot \frac{R^s}{(r-1)!} \cdot \ln^{r-1} R \cdot \left(\mu_I(\mathcal{P}_I(\Omega)) + O_{\Omega,I}\left(\ln^{-1} R\right).\right). \tag{2.10}$$

Доказательство. Согласно лемме 2.2 множество $\mathcal{P}_I(\Omega)$ является μ_I-измеримым . Не умаляя общности считаем, что дополнительно выполняются следующие условия:

$$\max_{i \in I_l} |x_{ii}| = x_{s_l s_l}, \quad l = \overline{1,r}. \tag{2.11}$$

Сделаем в интеграле $\operatorname{mes}\Omega_R = \int_{\Omega_R} dX$ замену

$$\begin{aligned} &x_{s_l s_l} = y_l, \\ &x_{ij} = y_{ij} \cdot y_l, \qquad j \in \{1,\ldots,s\} \setminus \{s_l\}, \;\; i \in I_l, \end{aligned} \tag{2.12}$$

где $l = \overline{1,r}$. Преобразование переменных (2.12) можно записать также в виде

$$X = S \cdot Y,$$

где S — матрица из $\mathrm{D}_I(\mathbb{R})$ с $s_{ii} = y_l$ при $i \in I_l$, а Y — матрица из L, где L — поверхность из леммы 2.2. Тогда

$$dX = \left(y_1^{t_1 s-1} \cdot \ldots \cdot y_r^{t_r r-1}\right)\, dy_1 \cdot \ldots \cdot dy_r \prod_{\substack{1 \leq i,j \leq s, \\ (i,j) \neq (s_l, s_l)}} dy_{ij}, \tag{2.13}$$

причем

$$1 \leq |\det X| \leq R \qquad \Longleftrightarrow \qquad \frac{1}{|\det Y|} \leq y_1^{t_1} \cdot \ldots \cdot y_r^{t_r} \leq \frac{R}{|\det Y|}. \tag{2.14}$$

Согласно j), (2.3), (2.11) существует ограниченное множество $W \subset L$ такое, что $\mathcal{P}_I(\Omega) = \mathcal{P}_I(W)$. Пусть

$$H(R,Y) = \left\{ y \in \mathbb{R}^r : \quad \frac{1}{|\det Y|} \leq y_1^{t_1} \cdot \ldots \cdot y_r^{t_r} \leq \frac{R}{|\det Y|}, \quad \frac{1}{C_1} \leq y_l, \; l = \overline{1,r} \right\}.$$

Используя (2.13), (2.14), получаем

$$\operatorname{mes}\Omega_R = \int_{\Omega_R} dX = \int_W \left(\int_{H(R,Y)} y_1^{t_1 s-1} \cdot \ldots \cdot y_r^{t_r s-1} dy \right) dL(Y). \tag{2.15}$$

Сделаем еще одну замену: $z_l = y_l^{t_l s}$, $l = \overline{1,r}$. Тогда

$$\int_{H(R,Y)} y_1^{t_1 s-1} \cdot \ldots \cdot y_r^{t_r s-1} dy = \left(s^r \cdot \prod_{l=1}^{r} t_l \right)^{-1} \int_{H'(R,Y)} dz, \tag{2.16}$$

$$H'(R,Y) = \left\{ z \in \mathbb{R}^r : \quad \frac{1}{|\det Y|^s} \leq z_1 \cdot \ldots \cdot z_r \leq \frac{R^s}{|\det Y|^s}, \quad C_1^{-t_l s} \leq z_l, \; l = \overline{1,r} \right\}.$$

Нетрудно проверить, что

$$\int_{H'(R,Y)} dz = \frac{R^s}{|\det Y|^s} \cdot \frac{\ln^{r-1} R^s}{(r-1)!} + O_{r,C,C_1}\left(\frac{R^s \ln^{r-2} R + |\ln|\det Y||}{|\det Y|^s}\right).$$

Из последней формулы, а также (2.15), (2.16) вытекает соотношение

$$\begin{aligned}\operatorname{mes}\Omega_R &= \frac{1}{s\cdot t_1\cdot\ldots\cdot t_r}\cdot\frac{R^s}{(r-1)!}\cdot\ln^{r-1}R\cdot\left(\int_W \frac{dL(Y)}{|\det Y|^s} + \right.\\ &\left. + O_{r,C,C_1}\left(\ln^{-1}R\cdot\int_W \frac{1+|\ln|\det Y||}{|\det Y|^s}dL(Y)\right)\right).\end{aligned}$$

Осталось заметить, что

$$\int_W \frac{dL(Y)}{|\det Y|^s} = \mu_I(\mathcal{P}_I(\Omega)), \quad \int_W \frac{1+|\ln|\det Y||}{|\det Y|^s}\,dL(Y) < \infty.$$

□

Замечание 2.1. Пусть $L \in \mathbb{N}$, $m_0 \in \mathbb{Z}_+$. Пусть

$$S(L, m_0) = \sum\left(\frac{1}{2^{m_1}}\prod_{l=1}^{r} 2^{m_l t_l s}\right),$$

где суммирование введется по всем $(m_1, \ldots, m_r) \in \mathbb{Z}_+^r$, удовлетворяющим условиям:

$$m_1 t_1 + \ldots + m_r t_r \le L, \quad m_1 \ge m_0.$$

Тогда, суммируя сначала по m_r, а потом по оставшимся m_i, получаем

$$S(L, m_0) \underset{r}{\ll} 2^{Ls} \sum_{\substack{m_1 \ge m_0 \\ m_i \le L}} \frac{1}{2^{m_1}} \ll \frac{2^{Ls}}{2^{m_0}} \cdot L^{r-2}.$$

Пусть $P, p \in \mathbb{R}_+$, $P > p$. Определим множество $G(P,p)$, состоящее из матриц $X \in \mathrm{M}_s(\mathbb{R})$, для которых выполняются неравенства (2.1) и $p \le T_i(X)$, $i = \overline{1,s}$. Обозначение $U(S,\epsilon)$ введено на стр. 139.

Лемма 2.4. *Пусть S — кусочно-дифференцируемая поверхность из $\mathrm{M}_s(\mathbb{R})$, которая либо ограниченная, либо является конусом. Пусть $P, p \in \mathbb{R}_+$, $P > p^s$; $\epsilon \in \mathbb{R}_+$. Тогда*

$$\operatorname{mes}\left(U(S,\epsilon) \cap G(P,p)\right) \underset{S,I}{\ll} \epsilon \cdot \frac{P^s}{p} \cdot \ln^{r-2}(P/p^s).$$

Доказательство. Не умаляя общности считаем, что для любого $X \in G(P,p)$

$$T_{s_l}(X) = \max_{i \in I_l} T_i(X), \quad l = \overline{1,r}.$$

Определим множество K, состоящее из наборов $k = (k_1, \ldots, k_s) \in \mathbb{Z}_+^s$ таких, что

$$\max_{i \in I_l} k_i = k_{s_l}, \quad l = \overline{1, r};$$
$$k_1 + \ldots + k_s \leq s + \log_2 (P/p^s).$$

Для каждого $k \in K$ положим

$$G_k = \left\{ X \in \mathrm{M}_s(\mathbb{R}) : \quad T_i(X) \leq p \cdot 2^{k_i},\ i = \overline{1, s} \right\}.$$

Тогда $G(P, p) \subset \bigcup_{k \in K} G_k$ и поэтому

$$\operatorname{mes} \left(U(S, \epsilon) \cap G(P, p) \right) \leq \sum_{k \in K} \operatorname{mes} \left(U(S, \epsilon) \cap G_k \right).$$

Каждое G_k содержится в параллелепипеде Π_k, состоящем из $X \in \mathrm{M}_s(\mathbb{R})$ таких, что

$$\max \left\{ \max_{1 \leq j \leq s} |x_{ij}|,\ |x_{s_l i}| \right\} \leq p \cdot 2^{k_j} \quad \text{при } i \in I_l \setminus \{s_l\},$$
$$|x_{s_l j}| \leq p \cdot 2^{k_{s_l}} \quad \text{при } j \in \{1, \ldots, s\} \setminus (I_l \setminus \{s_l\}),\ \ l \in \{1, \ldots, r\}.$$

Очевидно, что

$$\operatorname{mes} \Pi_k \underset{I}{=} (2p)^{s^2} \cdot \prod_{l=1}^{r} \left(\left(2^{k_{s_l}}\right)^{s - t_l + 1} \cdot \prod_{i \in I_l \setminus \{s_l\}} \left(2^{k_i}\right)^{s+1} \right).$$

Используя лемму 1.4 и следствие 1.1, получаем

$$\operatorname{mes} \left(U(S, \epsilon) \cap G_k \right) \underset{S}{\ll} \operatorname{mes} \left(U(S, \epsilon) \cap \Pi_k \right) \leq \epsilon \cdot \operatorname{mes} \Pi_k \cdot \sum_{j=1}^{s} \frac{1}{p \cdot 2^{k_j}}.$$

$$\operatorname{mes} \left(U(S, \epsilon) \cap G(P, p) \right) \underset{S}{\ll} \epsilon \cdot p^{s^2 - 1} \cdot \sum_{j=1}^{s} \theta_j,$$

$$\theta_j = \sum_{k \in K} \frac{1}{2^{k_j}} \cdot \prod_{l=1}^{r} \left(\left(2^{k_{s_l}}\right)^{s - t_l + 1} \cdot \prod_{i \in I_l \setminus \{s_l\}} \left(2^{k_i}\right)^{s+1} \right).$$

Осталось доказать, что

$$\theta_j \underset{I}{\ll} \frac{P^s}{p^{s^2}} \cdot \ln^{r-2}(P/p^s). \tag{2.17}$$

Достаточно рассмотреть случай $j = 1$. Положим

$$n_i = k_{s_l} - k_i, \quad i \in I_l \setminus \{s_l\},$$
$$n_{s_l} = k_{s_l},$$
$$\Upsilon(I) = \{1, \ldots, s\} \setminus \{s_1, \ldots, s_r\}.$$

Тогда

$$\theta_1 = \sum_{n \in K'} \left(\frac{2^{n_1}}{2^{n_{s_1}}} \prod_{l=1}^{r} 2^{n_{s_l} t_l s} \cdot \prod_{i \in \Upsilon(I)} \frac{1}{2^{n_i (s+1)}} \right),$$

$$K' = \left\{ n \in \mathbb{Z}_+^s : \quad \begin{array}{l} n_{s_l} \geq n_i \text{ при } i \in I_l,\ \ l \in \{1, \ldots, r\}, \\ \displaystyle\sum_{l=1}^{r} t_{s_l} n_{s_l} \leq \log_2(P/p^s) + s + \sum_{i \in \Upsilon(I)} n_i. \end{array} \right\}$$

Суммируя по $n_{s_1}, \ldots, n_{s_r}$, используя замечание 2.1, в котором

$$m_i = n_{s_i},\ i = \overline{1,s}; \quad m_0 = n_1; \quad L = \log_2(P/p^s) + s + \sum_{i \in \Upsilon(I)} n_i,$$

получаем

$$\theta_1 \underset{I}{\ll} \left(\frac{P}{p^s}\right)^s \cdot \sum_{\substack{n_i \in \mathbb{Z}_+, \\ i \in \Upsilon(I)}} \left(\log_2(P/p^s) + s + \sum_{i \in \Upsilon(I)} n_i\right)^{r-2} \cdot \prod_{i \in \Upsilon(I)} \frac{1}{2^{n_i}} \underset{I}{\ll} \frac{P^s}{p^{s^2}} \cdot \log_2^{r-2}(P/p^s).$$

Неравенство (2.17) доказано. □

Лемма 2.5. *Пусть выполняются условия j), jj), jjj) и (2.3). Тогда для любого $R \geq 2$ количество целочисленных $M \in \Omega$, удовлетворяющих условию $|\det M| \in [1, R]$, равно*

$$\frac{1}{s \cdot t_1 \cdot \ldots \cdot t_r} \cdot \frac{R^s}{(r-1)!} \cdot \ln^{r-1} R \cdot \Big(\mu_I(\mathcal{P}_I(\Omega)) + O_\Omega(\ln^{-1} R)\Big).$$

Доказательство. Используя формулу (1.7) для подсчета целочисленных точек в Ω_R и применяя лемму 2.3 для нахождения $\operatorname{mes} \Omega_R$, получаем, что искомое число равно

$$\frac{1}{s \cdot t_1 \cdot \ldots \cdot t_r} \cdot \frac{R^s}{(r-1)!} \cdot \mu_I(\mathcal{P}_I(\Omega)) \cdot \ln^{r-1} R + O(R^s \cdot \ln^{r-2} R + \xi),$$

где $\xi = \operatorname{mes} U(\partial\Omega_R, 1)$. Здесь и далее в этом доказательстве постоянные в оценках $\ll$ и $O(\ldots)$ зависят только от Ω и I. Осталось оценить ξ.

Любая матрица $X \in U(\partial\Omega_R, 1)$ удовлетворяет условиям

$$\prod_{i \in J} T_i(X) \ll R \quad \text{при всех } J \subset \{1, \ldots, s\}. \tag{2.18}$$

Поэтому $U(\partial\Omega_R, 1) \subset U^{(1)} \cup U^{(2)} \cup U^{(3)}$, где

$U^{(1)}$ состоит из матриц $X \in \mathrm{M}_s(\mathbb{R})$, для которых выполняются (2.3), (2.18) и существует такой номер $l \in \{1, \ldots, r\}$, что $T^{(l)}(X) \leq 1$;

$U^{(2)}$ состоит из $X \in U(\partial\Omega, 1)$, удовлетворяющих (2.3), (2.18), причем $T_i(X) \geq 1$, $i = \overline{1,s}$;

$U^{(3)}$ состоит из $X \in U(S_R, 1)$, удовлетворяющих (2.3), (2.18), причем $T_i(X) \geq 1$, $i = \overline{1,s}$.

Здесь $S_R = \{X \in \mathrm{M}_s(\mathbb{R}) : |\det X| = R\}$.

Согласно следствию 2.1

$$\operatorname{mes} U^{(1)} \ll R^s \cdot \ln^{r-2} R.$$

Для оценки $\operatorname{mes} U^{(2)}$ используем лемму 2.4, в которой $P = O(R)$, $p = 1$, $\epsilon = 1$. Получаем

$$\operatorname{mes} U^{(2)} \ll R^s \cdot \ln^{r-2} R.$$

Оценим $\operatorname{mes} U^{(3)}$. Рассмотрим множество $U' = R^{-1/s} \cdot U^{(3)}$. Оно состоит из матриц $X \in U(S_1, \epsilon)$ ($\epsilon = R^{-1/s}$), удовлетворяющих условиям

$$R^{-1/s} \le T_i(X), \quad i = \overline{1,s}; \quad \prod_{i=1}^{s} T_i(X) \ll 1.$$

Применяя лемму 2.4, в которой $P = O(1)$, $p = \epsilon = R^{-1/s}$, получаем

$$\operatorname{mes} U' \ll \ln^{r-2} R \quad \Longrightarrow \quad \operatorname{mes} U^{(3)} = R^s \cdot \operatorname{mes} U' \ll R^s \cdot \ln^{r-2} R.$$

Таким образом, $\xi \ll R^s \cdot \ln^{r-2} R$. □

Лемма 2.6. *Пусть $X \in \mathrm{GL}_s(\mathbb{R})$, причем*

$$\prod_{i=1}^{s} T_i(X) \le C \cdot |\det X|. \tag{2.19}$$

Тогда существует перестановка $(n_1, \ldots, n_s)$ из $\{1, \ldots, s\}$ такая, что

$$T_i(X) \le (C \cdot s!) \cdot |x_{in_i}|, \quad i = \overline{1,s}.$$

Доказательство. Предположим противное: существует матрица $X \in \mathrm{GL}_s(\mathbb{R})$, удовлетворяющая (2.19), причем для любой перестановки $(n_1, \ldots, n_s)$ найдется такой номер n_k, что

$$T_{n_k}(X) > (C \cdot s!) \cdot |x_{kn_k}|.$$

Тогда для любой перестановки $(n_1, \ldots, n_s)$

$$\prod_{i=1}^{s} T_i(X) > (C \cdot s!) \cdot \prod_{i=1}^{s} |x_{in_i}| \iff \prod_{i=1}^{s} |x_{in_i}| < \frac{1}{C \cdot s!} \prod_{i=1}^{s} T_i(X)$$

Следовательно,

$$|\det X| < s! \cdot \frac{1}{C \cdot s!} \prod_{i=1}^{s} T_i(X) = \frac{1}{C} \prod_{i=1}^{s} T_i(X).$$

Получили противоречие с (2.19). □

Лемма 2.7. *Пусть выполняются условиям j), jj), jjj). Тогда для любого $R \ge 2$ количество целочисленных матриц $M \in \Omega$, удовлетворяющих условию $|\det M| \in [1, R]$, равно*

$$\frac{1}{s \cdot t_1 \cdot \ldots \cdot t_r} \cdot \frac{R^s}{(r-1)!} \cdot \ln^{r-1} R \cdot \left(\mu_I(\mathcal{P}_I(\Omega)) + O_{\Omega,I}(\ln^{-1} R) \right).$$

Доказательство. Согласно лемме 2.6 множество Ω можно разбить на фиксированное число непересекающихся частей так, что каждая часть после действия некоторого преобразования, меняющего нумерацию столбцов, удовлетворяет условиям j), jj), jjj), (2.3), в которых $C_1 = C \cdot s!$. Применяя лемму 2.5 для подсчета количества целочисленных точек в каждой части, получаем требуемую формулу. □

Литература

[1] М. О. Авдеева, "О нижних оценках количества локальных минимумов целочисленных решеток", *Фундамент. и прикл. матем.*, **11**:6 (2005), 9–14.

[2] М. О. Авдеева, В. А. Быковский, "Верхние и нижние оценки константы Вороного-Минковского", *Матем. заметки*, **87**:4 (2010), 483–491.

[3] В. И. Арнольд, *Задачи Арнольда*, М.: Фазис, 2000.

[4] В. И. Арнольд, *Цепные дроби*, М.: МЦНМО, 2001.

[5] З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, М.: Наука, 1972. 496 с.

[6] А. Брёнстед, *Введение в теорию выпуклых многогранников*, М.: Мир, 1988. 240 с.

[7] А. Д. Брюно, В. И. Парусников, "Многогранники Клейна для двух кубических форм Давенпорта", *Матем. заметки*, **56**:4 (1994), 9–27.

[8] А. В. Быковская, "О многомерном обобщении теоремы Лагранжа о цепных дробях", *Матем. заметки*, **92**:3 (2012), 343–360.

[9] А. В. Быковская, "Критерий целочисленной эквивалентности двух обобщенных выпуклых целочисленных многогранников", *Матем. заметки*, **94**:5 (2013), 648–660.

[10] В. А. Быковский, "О погрешности теоретико-числовых квадратурных формул", *ДАН*, **382**:2 (2003), 154–155.

[11] В. А. Быковский, "О погрешности теоретико-числовых квадратурных формул", *Чебышевский сб.*, Тула, **3**:2 (2002), 27–33.

[12] В. А. Быковский, "Алгоритм вычисления локальных минимумов решеток", *ДАН*, **399**:5 (2004), 587–589.

[13] В. А. Быковский, "Относительные минимумы решеток и вершины многогранников Клейна", *Функц. анализ и его прил.*, **40**:1 (2006), 69–71.

[14] В. А. Быковский, "Теорема Валена для двумерных подходящих дробей", *Матем. заметки*, **66**:1 (1999), 30–37.

[15] В. А. Быковский, "Отклонения сеток Коробова", *Изв. РАН. Сер. матем.,* **76**:3 (2012), 19–38.

[16] В. А. Быковский, С. В. Гассан, "О параметре оптимальности параллелепипедальных сеток Коробова для квадратурных формул", *Журн. выч. матем. и матем. физ.*, **51**:8 (2011), 1363–1369.

[17] В. А. Быковский, С. В. Гассан, "Алгоритм вычисления локальных минимумов решеток и его приложения", *Вестник Тихоокеанского государственного университета*, 1 (2011), 39–48.

[18] В. А. Быковский, О. А. Горкуша, "Минимальные базисы трехмерных полных решеток", *Матем. сб.*, **192**:2 (2001), 57–66.

[19] Г. Ф. Вороной, *Об одном обобщении алгорифма непрерывных дробей.* Типография Варшавского Учебного Округа, Варшава, 1896.

[20] Г. Ф. Вороной, *Собрание сочинений в 3-х томах.* Т. 1. Киев: Изд-во АН УССР, 1952.

[21] С. В. Гассан, "Структура областей Валена для трехмерных решеток", *Чебышевский сб.*, **6**:3 (2005), 51–84.

[22] О. Н. Герман, "Паруса и базисы Гильберта", *Тр. МИАН*, **239** (2002), 98–105.

[23] О. Н. Герман, "Паруса и норменные минимумы решеток", *Матем. сб.*, **196**:3 (2005), 31–60.

[24] О. Н. Герман, "Полиэдры Клейна и относительные минимумы решеток", *Матем. заметки.*, **79**:4 (2006), 546–552.

[25] О. Н. Герман, Е. Л. Лакштанов, "О многомерном обобщении теоремы Лагранжа для цепных дробей", *Изв. РАН. Сер. матем.*, **72**:1 (2008), 51–66.

[26] О. А. Горкуша, "Минимальные базисы трехмерных полных решеток", *Матем. заметки*, **69**:3 (2001), 353–362.

[27] О. А. Горкуша, "Критерий конечности множества локальных минимумов решетки", *Чебышевский сб.*, **5**:3 (2004), 15–17.

[28] О. А. Горкуша, Н. М. Добровольский, "Об оценках гиперболической дзета-функции решеток", *Чебышевский сб.*, **6**:2 (2005).

[29] П. М. Грубер, К. Г. Леккеркеркер, *Геометрия чисел*, М.: Наука, 2008, 727 с.

[30] Л. Даунер, Б. Грюнбаум, В. Кли, *Теорема Хелли*, М.: Мир, 1968, 160 с.

[31] Б. Н. Делоне, *Петербургская школа теории чисел*, Изд-во АН СССР, М.-Л., 1947.

[32] Б. Н. Делоне, Д. К. Фаддеев, *Теория иррациональностей третьей степени*, Тр. МИАН, **11** (1940), Изд-во АН СССР, М.-Л., 3–340.

[33] Г. Дэвенпорт, *Высшая арифметика. Введение в теорию чисел,* М.: Наука, 1968, 176 с.

[34] А. А. Илларионов, "Оценка количества относительных минимумов неполных целочисленных решеток", *Чебышевский сб.*, **7**:4 (2006), 92–98.

[35] А. А. Илларионов, "Оценка количества относительных минимумов неполных целочисленных решеток произвольного ранга", *ДАН*, **418**:2 (2008), 155–158.

[36] А. А. Илларионов, "Оценки количества относительных минимумов решеток", *Матем. заметки*, **89**:2 (2011), 249–259.

[37] А. А. Илларионов, "Среднее количество относительных минимумов трехмерных целочисленных решеток", *Алгебра и анализ*, **23**:3 (2011), 189–215.

[38] А. А. Илларионов, "О цилиндрических минимумах трехмерных решеток", *Дальневост. матем. журн.*, **11**:1 (2011), 37–47.

[39] А. А. Илларионов, Д. А. Слинкин, "О количестве вершин многогранников Клейна целочисленных решеток в среднем", *Дальневост. матем. журн.*, **11**:1 (2011), 48–55.

[40] А. А. Илларионов, Ю. А. Сойка, "О количестве относительных минимумов целочисленных решеток", *Дальневост. матем. журн.*, **11**:2 (2011), 149–154.

[41] А. А. Илларионов, "О цилиндрических минимумах целочисленных решеток", *Алгебра и анализ*, **24**:2 (2012), 154–170.

[42] А. А. Илларионов, "Среднее количество относительных минимумов трехмерных целочисленных решеток фиксированного определителя", *Изв. РАН. Сер. матем.*, **76**:3 (2012), 111–138.

[43] А. А. Илларионов, “О статистических свойствах локальных минимумов целочисленных решеток”, *Дальневост. матем. журн.*, **12**:2 (2012), 201–230.

[44] А. А. Илларионов, “О статистических свойствах многогранников Клейна трехмерных целочисленных решеток”, *Матем. сб.*, **204**:6 (2013), 23–46.

[45] А. А. Илларионов, “Многомерное обобщение теоремы Хейльбронна о средней длине конечной непрерывной дроби”, *Матем. сб.*, **205**:3 (2014)

[46] А. А. Илларионов, “О среднем количестве наилучших приближений линейных форм”, *Изв. РАН. Сер. матем.*, **78**:2 (2014), 61–86

[47] А. М. Истамов, “Асимптотическое распределение целочисленных матриц n-го порядка, принадлежащих заданному классу вычетов”, *Аналитическая теория чисел и теория функций. 4, Зап. научн. сем. ЛОМИ*, **112** (1981), 85–11

[48] О. Н. Карпенков, “О триангуляциях торов, связанных с двумерными цепными дробями кубических иррациональностей”, *Функц. анализ и его прил.*, **38**:2 (2004), 28–37.

[49] О. Н. Карпенков, “О двумерных цепных дробях целочисленных гиперболических матриц с небольшой нормой”, *УМН*, **59**:5 (2004), 149–150

[50] О. Н. Карпенков, “Классификация трехмерных многоэтажных вполне пустых выпуклых отмеченных пирамид”, *УМН*, **60**:1 (2005), 169–170

[51] О. Н. Карпенков, “Об инвариантной мере Мебиуса и распределении граней Гаусса–Кузьмина”, *Тр. МИАН*, **258** (2007), 79–92.

[52] Дж. В. Касселс, *Введение в теорию диофантовых приближений*, М.: ИЛ, 1961, 213 с.

[53] Дж. В. Касселс, *Рациональные квадратичные формы*, М.: Мир, 1982. 440 с.

[54] Дж. В. Касселс, *Введение в геометрию чисел*, М.: Мир, 1995.

[55] Д. Е. Кнут, *Искусство программирования. Т.2*, М.: Изд. дом «Вильямс», 2001.

[56] Е. И. Коркина, “Двумерные цепные дроби. Самые простые примеры”, *Тр. МИАН*, **209** (1995), 143–166.

[57] Н. М. Коробов, *Теоретико-числовые методы в приближенном анализе*, М.: МЦНМО, 2004.

[58] Ж.-О. Муссафир, “Паруса и базисы Гильберта”, *Функц. анализ и его прил.*, **34**:2 (2000), 43–49.

[59] Ю. В. Линник, *Эргодические свойства алгебраических полей*, Л.: Изд-во Ленинградского университета, 1967. 208 с.

[60] Ю. В. Линник, Б. Ф. Скубенко, “Асимптотическое распределение целочисленных матриц третьего порядка”, *Вестник ЛГУ*, № 13 (1964), 25–36.

[61] Н. Г. Мощевитин, “Сингулярные диофантовы системы А. Я. Хинчина и их применение”, *УМН*, **65**:3 (2010), 43–126.

[62] В. И. Парусников, “Многогранники Клейна для четвертой экстремальной кубической формы”, *Матем. заметки*, **67**:1 (2000), 110–128.

[63] В. И. Парусников, “Многогранники Клейна для трех экстремальных кубических форм”, *Матем. заметки*, **77**:4 (2005), 566–583.

[64] Б. Ф. Скубенко, “К распределению целочисленных матриц и вычислению объема фундаментальной области унимодулярной группы матриц”, *Тр. МИАН СССР*, **80** (1965), 129–144.

[65] Б. Ф. Скубенко, "Минимумы разложимой кубической формы от трех переменных", Аналитическая теория чисел и теория функций. 9, *Записки научн. сем. ЛОМИ*, **168** (1988), 125–139.

[66] Б. Ф. Скубенко , "Минимумы разложимых форм степени n от n переменных при $n > 3$", Модулярные функции и квадратичные формы. 1, *Записки научн. сем. ЛОМИ*, **183** (1990), 142–154.

[67] В. Г. Спринджук, *Метрическая теория диофантовых приближений*, М.: Наука, 1977.

[68] В. А. Тиморин, *Комбинаторика выпуклых многогранников*, М.: МЦНМО, 2002. 16 с.

[69] А. В. Устинов, "Вычисление дисперсии в одной задаче из теории цепных дробей", *Матем. сб.*, **198**:6 (2007), 139–158

[70] А. В. Устинов,"О числе решений сравнения $xy \equiv l \pmod q$ под графиком дважды непрерывно дифференцируемой функции", *Алгебра и анализ*, **20**:5 (2008), 186–216.

[71] А. В. Устинов, "К теореме Вороного о цилиндрических минимумах трехмерных решеток", *Дальневост. матем. журн.*, **11**:2 (2011), 213–221.

[72] А. В. Устинов, "Минимальные системы векторов в трехмерных решетках и аналог теоремы Валена для трехмерных цепных дробей Минковского", *Математика и информатика, 1*, К 75-летию со дня рождения Анатолия Алексеевича Карацубы, Совр. пробл. матем., 16, МИАН, М., 2012, 103–128.

[73] Д. М. Ушанов, "Теорема Быковского и обобщение теоремы Ларчера", *Матем. заметки*, **91**:5 (2012), 795–798

[74] Д. А. Фроленков, "Асимптотическое поведение первого момента для числа шагов в алгоритме Евклида по избытку и недостатку", *Матем. сб.*, **203**:2 (2012), 143–160.

[75] Г. Хассе, *Лекции по теории чисел*, М.: Издательство иностранной литературы, 1953, 527 с.

[76] А. Я. Хинчин, *Цепные дроби*, М.: ГИФИЗМАТЛИТ, 1961.

[77] В. Ярник, "К теории однородных линейных диофантовых приближений", *Чехослов. матем. журн.*, **4** (1954), 330–353

[78] V. I. Arnold, "A-Graded Algebras and continued fractions", *Commun. Pure Appl. Math.*, **142** (1989), 993–1000.

[79] V. I. Arnold, "Higher dimensional continued fractions", *Регулярная и хаотическая динамика*, **3**:3 (1998), 10–17.

[80] V. I. Arnold, "Preface", *Amer. Math. Soc. Transl.*, **197**:2 (1999), ix-xii.

[81] L. Clozel, H. Oh, E. Ullmo, "Hecke operators and equidistribution of Hecke points", *Invent. math.*, **144**:2 (2001), 327–351.

[82] A. J. Brentjes, *Multidimensional continued fraction algorithms*, Mathematical Centre Tracts, 145. Mathematisch Centrum, Amsterdam, 1981, 183 pp.

[83] J. Buchmann, "A generalization of Voronoi's unit algorithm. I", *J. Number Theory*, **20**:2 (1985), 177–191.

[84] J. Buchmann, "A generalization of Voronoi's unit algorithm. II", *J. Number Theory*, **20**:2 (1985), 192–209.

[85] J. Buchmann, "The generalized Voronoi-algorithm in totally real algebraic number fields", EUROCAL'85, **2** (Linz, 1985), 479–486, Lecture Notes in Comput. Sci., 204, Springer, Berlin, 1985.

[86] J. Buchmann, "The computation of the Fundamental Unit of Totally Complex Quartic Orders", *Math. Comp.*, **48**:177 (1987), 39–54.

[87] J. Buchmann, "On the computation of unit and class number by a generalization og Lagrange's algorithm", *J. Number Theory*, **26**:1 (1987), 8–30.

[88] J. Buchmann, "On the period length of the generalized Lagrange algoritm", *J. Number Theory*, **26**:1 (1987), 31–38.

[89] J. Buchmann, "On generalized continued fraction expansions of short period length", *Publ.Math. Debrecen*, **37**:1–2 (1990), 109–114.

[90] J. Buchmann, M. Pohst, J. v. Schmettow, "On the computation of unit group and class groups of totally real quartic fields", *Math. Comp.*, **53**:187 (1989), 387–397.

[91] Y. Bugeaud, M. Laurent, "On exponents of homogeneous and inhomogeneous Diophantine approximation", *Mosc. Math. J.*, **5**:4 (2005), 747–766.

[92] N. Chevallier, "Meilleures approximations diophantiennes simultanées et théoréme de Lévy", *Ann. Inst. Fourier (Grenoble)*, **55**:5 (2005), 1635-1657.

[93] N. Chevallier, "Best simultaneous Diophantine approximations and multidimensional continued fraction expansions", *Moscow Journal of Combinatorics and Number Theory*, **3**:1 (2013), 3–56

[94] L. Euler, *De relatione inter ternas pluresve quantitates instituenda*, Leonhardi Euleri Commentationes arithmeticae collectae, т. II, С.-Петербург, 1849, с. 99

[95] Ph. Furtwängler, M. Zeisel, "Zur Minkowskischen Parallelepiped approximation", *Motatsh. f. Math.*, **30** (1920), 177–198.

[96] O. N. German, "Klein polyhedra and lattices with positive norm minima", *J. Theor. Nombres Bordeaux*, **19**:1 (2007), 175–190.

[97] H. Hancock, *Development of the Minkowski geometry of numbers.* Vol. 1-2, Dover Publications Inc., 1964.

[98] H. Heilbronn, "On the average length of a class of finite continued fractions", *Abhandlungen aus Zahlentheorie und Analysis*, Berlin, VEB (1968), 89–96.

[99] A. A. Illarionov, "On the Asymptotic Distribution of Integer Matrices", *Moscow Journal of Combinatorics and Number Theory*, **1**:4 (2011), 301–345.

[100] V. Jarník, "Zum Khintchineschen 'Übertragungssatz", *Acad. Sci. URSS*, **3**, Trav. Inst. math, Tbilissi, 1938, 193–216

[101] V. Jarník, "On linear inhomogeneous Diophintine approximations", *Rozpravy II. Tridy Ceske Akad.*, **51**:29 (1941)

[102] V. Jarník, "Eine Bemerkung über diophantische Approximationen", *Math. Z.*, **72**:1 (1959), 187-191

[103] O. N. Karpenkov, "Three exapmles of three-dimensional continued fractions in the sense of Klein", *C. R. Acad. Sci. Paris.* **343**:1 (2006), 5–7.

[104] O. N. Karpenkov, "Completely empty pyramids on integer lattices and two-dimensional faces of multidimensional continued fractions", *Monatsh. Math.*, **152**:3 (2007), 217–249.

[105] O. N. Karpenkov, "Constructing multidimensional periodic continued fractions in the sense of Klein", *Math. Comp.* **78**:267 (2009), 1687–1711.

[106] O. N. Karpenkov, *Geometry of Continued Fractions*, Algorithms and Computation in Mathematics, **26**, Springer-Verlag, Berlin Heidelberg, 2013, 405 p.

[107] D. E. Knuth, "Evalution of Porter's Constant", *Comp. and Math. with Appl.*, 2 (1976), 137–139.

[108] M. L. Kontsevich, Yu. M. Suhov, "Statistics of Klein polyhedra and multidimensional continued fractions", *Amer. Math. Soc. Trasl.*, **197**:2 (1999), 9–27.

[109] E. I. Korkina, "La périodicité des fractions continues multidimensionnelles", *C. R. Acad. Sci. Paris Ser. I Math.*, **319**:8 (1994), 777–780.

[110] E. I. Korkina, "The simplest 2-dimensional continued fraction", *J. Math. Sci.*, **82**:5 (1996), 3680–3685.

[111] F. Klein, "Ueber die geometrische Auffassung der gewohlichen Kettenbruchentwichlung", *Nachr. Ges. Wiss. Göttingem*, № 3 (1895), 357–359.

[112] F. Klein, "Sur une representation geometrique de development en fraction continue ordinaire", *Nouv. Ann. Math.*, № 3 (1896), 327–331.

[113] F. Klein, Ausgewählte Kapitel der Zahlentheorie. Bd I. Einleitung. Vorlesungen 1895/1896 herausgegeben von A. Sommerfeld. Göttingen, 1896.

[114] G. Lachaud, "Polyédre d'Arnol'd et voile d'un cône simplicial: analogues du théoréme de Lagrange [The Arnold polyhedron and the sail of a simplicial cone: analogues of the Lagrange theorem]", *C. R. Acad. Sci. Paris Ser. I Math.*, **317**:8 (1993), 711–716.

[115] G. Lachaud, "Sails and Klein polyhedra", Number theory, Proceedings of the international conference on discrete mathematics and number theory (Tiruchirapalli, 1996), *Contemp. Math.*, ed. V. K. Murty, **210** (1998), 373–385.

[116] G. Lachaud, *Voiles et Polyèdres de Klein*, Act. Sci. Ind., Hermann, Paris, 2002.

[117] J. C. Lagarias, "Some new results in simultaneous Diophantine approximation", Proc. Queens's University Number Theory Conference 1979, (P. Ribenboim, Ed.), Queen's Papers in Pure and Applied Math. No. 54, Queen's University, 1980, 453–474

[118] J. C. Lagarias, "Best simultaneous Diophantine approximations. I. Growth rates of best approximation denominators", *Trans. Amer. Math. Soc.*, **272**:2 (1982), 545–554

[119] J. C. Lagarias, "Best simultaneous Diophantine approximations. II. Behavior of consecutive best approximations", *Pacific J. Math.*, **102**:1 (1982), 61–88

[120] J. C. Lagarias, "Best Diophantine approximations to a set of linear forms", *J. Austral. Math. Soc. Ser. A*, **34**:1 (1983), 114–122.

[121] J. C. Lagarias, "The computational complexity of simultaneous Diophantine approximation problems", *SIAM J. Comput.*, **14**:1 (1985), 196–209

[122] G. Lochs, "Statistik der Teilnenner der zu den echten Brüchen gehörigen regelmässigen Kettenbrüche", *Monatsh. Math.*, **65** (1961), 27–52.

[123] P. McMullen, "The maximum numbers of faces of a convex polytope", *Mathematika*, 1970, № 6, 179–184.

[124] H. Minkowski, "Zur Theorie der Kettenbruche", *Annales de l'Ecole Normale Superieure*, **13**:3 (1894).

[125] H. Minkowski, "Generalisation de la theorie des fraction continues", *Ann. Sci. École Norm. Sup.* Ser. 3. **13**:2 (1896), 41–60.

[126] H. Minkowski, *Zur Theorie der Kettenbrúche*, Gesammelte Abhandlungen, Leipzig, 1911, 278–292.

[127] N. Moshchevitin, *On some open problems in Diophantine approximation*, arXiv:1202.4539.

[128] J.-O. Moussafir, "Convex hulls of integral points", Теория представлений, динамические системы, комбинаторные и алгоритмические методы. V, *Зап. научн. сем. ПОМИ*, **266**, ПОМИ, СПб., 2000, 188–217

[129] J.-O. Moussafir, *Voiles et polyèdres de Klein: Géométrie, algorithmes et statistiques*, Doc. Sci. Thése, Univ. Paris IX–Dauphine, 2000.

[130] P.M. Pepper, "Une application de la géométrie des nombres á une généralisation d'une fractiion continue", *Annales scientifiques de l'É.N.S.*, 3 séries, **56** (1939), 1–70.

[131] M.E. Pohst, "Three principal tasks of computational algebraic number theory", Number theory and applications (Banff, AB, 1988), 123–133, NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., 265, Kluwer Acad. Publ., Dordrecht, 1989

[132] J. W. Porter, "On a theorem of Heilbronn", *Mathematika*, **22**: 1 (1975), 20–28.

[133] H. Tsuchihashi, "Higher dimensional analogues of periodic continued fractions and cusp singularities", *Tohoku Math. J.*, **35** (1983), 176–193.

[134] L. Ya. Vulakh, "Units in some families of algebraic number fields", *Trans. Amer. Math. Soc.* **356**:4 (2004), 2325–2348.