Math-Net.Ru

Общероссийский математический портал

В. А. Быковский, О. А. Горкуша, Минимальные базисы трехмерных полных решеток, *Матем. сб.*, 2001, том 192, номер 2, 57–66

DOI: <https://doi.org/10.4213/sm542>

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

Параметры загрузки:

IP: 18.209.158.208

26 апреля 2023 г., 11:26:44

УДК 511.36+511.9

В. А. Быковский, О. А. Горкуша

Минимальные базисы трехмерных полных решеток

Изучены базисы Минковского для трехмерных решеток.
Библиография: 5 названий.

Обозначим через $\mathfrak{L}_s(\mathbb{R})$ ($s = 2, 3, \dots$) множество всех полных решеток в $\mathbb{R}^s$. Каждая матрица $M \in GL_s(\mathbb{R})$ определяет решетку $\Gamma(M) \in \mathfrak{L}_s(\mathbb{R})$, которая порождается базисными узлами $\gamma^{(1)}, \dots, \gamma^{(s)}$, составленными из столбцов M . При этом $\Gamma(M) = \Gamma(M')$ тогда и только тогда, когда $M' = MU$ для некоторой унимодулярной матрицы U . При построении многомерных аналогов алгоритма цепных дробей в рамках теории “относительных минимумов” Г. Ф. Вороного [1] и Г. Минковского [2] среди всех возможных базисов (соответственно матриц) естественным образом выделяются так называемые *минимальные базисы* (*минимальные матрицы*). В настоящей работе изучается структура минимальных базисов трехмерных решеток из $\mathfrak{L}_3^*(\mathbb{R})$, где

$$\mathfrak{L}_s^*(\mathbb{R}) = \{\Gamma \in \mathfrak{L}_s(\mathbb{R}) : \forall (\gamma_1, \dots, \gamma_s) \in \Gamma' \gamma_1 \neq 0, \dots, \gamma_s \neq 0\}.$$

Здесь $\Gamma' = \Gamma \setminus \{(0, \dots, 0)\}$. Для решеток $\Gamma \in \mathfrak{L}_s^*(\mathbb{R})$ справедливо следующее важное

ЗАМЕЧАНИЕ 1. Пусть $\gamma \neq \pm\gamma'$ — узлы из Γ' . Тогда $|\gamma_i| \neq |\gamma'_i|$ при всех $i = 1, \dots, s$.

Для непустого конечного $T \subset \mathbb{R}^s$ и $i = 1, \dots, s$ положим

$$|T|_i = \max\{|x_i| : (x_1, \dots, x_i, \dots, x_s) \in T\}.$$

Следуя [2] и [3], для $\Gamma \in \mathfrak{L}_s^*(\mathbb{R})$ назовем $S = \{\gamma^{(1)}, \dots, \gamma^{(t)}\} \subset \Gamma'$ *минимальным*, если:

- а) $\gamma^{(i)} \neq \pm\gamma^{(j)}$ при всех $1 \leq i < j \leq t$;
- б) не существует $\tilde{\gamma} \in \Gamma'$ с $|\tilde{\gamma}_i| < |S|_i$ при всех $i = 1, \dots, s$.

Если S состоит из одного элемента, то мы приходим к понятию “относительный минимум” (в дальнейшем просто минимум) из [1]. Справедливо

Работа выполнена при финансовой поддержке ФЦП “Интеграция” (проект № К 0560).

ЗАМЕЧАНИЕ 2. Любое непустое подмножество минимального множества S также минимально. В частности, все элементы S минимумы.

Согласно [1] и [3] минимумы γ и γ' , для которых множество $\{\gamma, \gamma'\}$ минимально, называются *смежными*. Базис $\gamma^{(1)}, \dots, \gamma^{(s)}$ решетки $\Gamma \in \mathfrak{L}_s^*(\mathbb{R})$, составляющий минимальное множество, назовем *минимальным базисом*. Решетки из $\mathfrak{L}_s^*(\mathbb{R})$ определяются матрицами соответствующего подмножества $GL_s^*(\mathbb{R})$ в $GL_s(\mathbb{R})$. Назовем матрицу $M \in GL_s^*(\mathbb{R})$ *минимальной*, если $\gamma^{(1)}(M), \dots, \gamma^{(s)}(M)$ (столбцы M) составляют минимальный базис в $\Gamma(M)$.

Обозначим через $\mathfrak{F}_s$ семейство всех отображений

$$F: GL_s(\mathbb{R}) \rightarrow GL_s(\mathbb{R}),$$

состоящее из композиций преобразований $GL_s(\mathbb{R})$ в себя вида: а) перестановки строк и столбцов; б) одновременное изменение знака у всех элементов некоторых строк и столбцов.

Очевидно, что множество $GL_s^*(\mathbb{R})$ и его подмножество минимальных матриц инвариантны относительно действия преобразований из $\mathfrak{F}_s$.

Пусть $\gamma^{(1)}, \gamma^{(2)}$ – базис $\Gamma \in \mathfrak{L}_2^*(\mathbb{R})$ и $M \in GL_2^*(\mathbb{R})$ – соответствующая ему матрица, столбцы которой составлены из $\gamma^{(1)}$ и $\gamma^{(2)}$. Легко проверить, что если для некоторого преобразования $F \in \mathfrak{F}_2$

$$F(M) = \begin{pmatrix} a_1 & -b_1 \\ a_2 & b_2 \end{pmatrix} \quad (0.1)$$

с $0 < a_1 < b_1$ и $0 < b_2 < a_2$, то множество $\{\gamma^{(1)}, \gamma^{(2)}\}$ минимально и M – минимальная матрица. Вороной [1] доказал обратное утверждение в следующем виде. Пусть $\{\gamma^{(1)}, \gamma^{(2)}\}$ – минимальное множество для $\Gamma \in \mathfrak{L}_2^*(\mathbb{R})$. Тогда $\gamma^{(1)}, \gamma^{(2)}$ составляют базис Γ , а для соответствующей ему матрицы M выполнено (0.1) с некоторым $F \in \mathfrak{F}_2$.

В настоящей работе мы изучаем эти вопросы для трехмерных решеток и доказываем следующие утверждения.

ТЕОРЕМА 1. Пусть $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$ – базис $\Gamma \in \mathfrak{L}_3^*(\mathbb{R})$ и $M \in GL_3^*(\mathbb{R})$ – соответствующая ему матрица. Предположим, что для некоторого преобразования $F \in \mathfrak{F}_3$ матрица $F(M)$ имеет один из следующих двух видов:

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & -b_2 & -c_2 \\ a_3 & -b_3 & c_3 \end{pmatrix}, \quad \begin{pmatrix} a_1 & b_1 & -c_1 \\ a_2 & -b_2 & -c_2 \\ a_3 & -b_3 & c_3 \end{pmatrix} \quad (0.2)$$

с положительными a_i, b_i, c_i , у которых в обоих случаях $a_1 < b_1, c_1 < b_1, b_2 < a_2, c_2 < a_2, a_3 < c_3, b_3 < c_3$, и в первом случае выполняется хотя бы одно из неравенств $c_1 < a_1, b_2 < c_2$, а во втором оба неравенства $b_2 + c_2 > a_2, b_3 < a_3$. Тогда множество $\{\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}\}$ минимально.

ТЕОРЕМА 2. Пусть $\{\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}\}$ – минимальное множество в $\Gamma \in \mathfrak{L}_3^*(\mathbb{R})$ с линейно независимыми узлами. Тогда:

- а) $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$ составляют базис Γ ;
- б) для соответствующей матрицы M найдется преобразование $F \in \mathfrak{F}_3$, для которого матрица $F(M)$ имеет один из двух видов в (0.2).

Ранее Минковский в работе [2] доказал утверждение а) теоремы другим методом.

Вороной [1] установил (см. также [4]), что любую пару смежных минимумов $\gamma^{(1)}, \gamma^{(2)}$ решетки $\Gamma \in \mathfrak{L}_3^*(\mathbb{R})$ можно дополнить третьим узлом $\gamma^{(3)}$ до базиса. Очевидно, что в качестве $\gamma^{(3)}$ может фигурировать любой другой узел вида $\pm(\gamma^{(3)} + m_1\gamma^{(1)} + m_2\gamma^{(2)})$ с произвольными целыми m_1 и m_2 . Мы доказываем более сильное утверждение.

ТЕОРЕМА 3. Любую пару $\gamma^{(1)}, \gamma^{(2)}$ смежных минимумов решетки $\Gamma \in \mathfrak{L}_3^*(\mathbb{R})$ можно дополнить третьим узлом $\gamma^{(3)}$ до минимального базиса.

Ранее в [5] было доказано, что в качестве $\gamma^{(3)}$ можно выбрать минимум решетки Γ .

§ 1. Достаточные условия минимальности базиса

Напомним, что решетка в $\mathbb{R}^3$ – множество целочисленных комбинаций

$$\Gamma = \{m_1\gamma^{(1)} + m_2\gamma^{(2)} + m_3\gamma^{(3)} : m_1, m_2, m_3 \in \mathbb{Z}\},$$

где $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$ – линейно независимые векторы из $\mathbb{R}^3$. Как уже отмечалось во введении, мы будем иметь дело только с решетками из $\mathfrak{L}_3^*(\mathbb{R})$. Положим для любого $x \in \mathbb{R}^3$

$$\Gamma'(x) = \{\gamma \in \Gamma' : |\gamma_i| \leq |x_i|, i = 1, 2, 3\}.$$

ЛЕММА 1. Пусть $\Gamma \in \mathfrak{L}_3^*(\mathbb{R})$ – решетка, порожденная базисными узлами

$$\begin{aligned} \gamma^{(1)} &= (a_1, a_2, a_3), \\ \gamma^{(2)} &= (b_1, -b_2, -b_3), \\ \gamma^{(3)} &= (c_1, -c_2, c_3) \end{aligned} \tag{1.1}$$

с положительными a_i, b_i, c_i , для которых выполнены условия:

- 1) $\max(a_1; c_1) < b_1, \max(b_2; c_2) < a_2, \max(a_3; b_3) < c_3$;
- 2) справедливо хотя бы одно из неравенств

$$c_1 < a_1, \quad b_2 < c_2.$$

Тогда $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$ – минимальный базис.

ДОКАЗАТЕЛЬСТВО. Ввиду условий 1) достаточно показать, что

$$\Gamma'(b_1, a_2, c_3) = \{\pm\gamma^{(1)}, \pm\gamma^{(2)}, \pm\gamma^{(3)}\}. \quad (1.2)$$

Любой узел $\gamma \in \Gamma'$ имеет вид

$$\begin{aligned} \gamma &= m_1\gamma^{(1)} + m_2\gamma^{(2)} + m_3\gamma^{(3)} \\ &= (m_1a_1 + m_2b_1 + m_3c_1, m_1a_2 - m_2b_2 - m_3c_2, m_1a_3 - m_2b_3 + m_3c_3), \end{aligned} \quad (1.3)$$

где m_1, m_2, m_3 — целые числа, одновременно не равные нулю. Если в разложении (1.3) два числа из m_1, m_2, m_3 равны нулю, то $\gamma = m_i\gamma^{(i)}$. Из всех таких узлов только $\pm\gamma^{(i)} \in \Gamma'(b_1, a_2, c_3)$.

Рассмотрим теперь те узлы в Γ' , у которых в разложении (1.3) хотя бы два числа из m_1, m_2, m_3 отличны от нуля. Без ограничения общности можно считать, что $m_1 \geq 0$. Тогда:

а) для $m_2 > 0$ и $m_3 \geq 0$

$$\gamma_1 = m_1a_1 + m_2b_1 + m_3c_1 > b_1;$$

б) для $m_2 \leq 0$ и $m_3 > 0$

$$\gamma_3 = m_1a_3 + |m_2|b_3 + m_3c_3 > c_3;$$

в) для $m_2 \leq 0$ и $m_3 \leq 0$ в случае $m_1 > 0$

$$\gamma_2 = m_1a_2 + |m_2|b_2 + |m_3|c_2 > a_2,$$

а в случае $m_1 = 0$

$$\gamma_1 = -|m_2|b_1 - |m_3|c_1 < -b_1.$$

Пусть теперь $m_2 > 0$ и $m_3 < 0$.

Согласно условию 2) леммы должно выполняться хотя бы одно из неравенств: $c_1 < a_1, c_2 > b_2$.

Для $c_1 < a_1$ находим:

а) при $|m_3| \geq m_1 + 1$

$$\begin{aligned} \gamma_3 &= m_1a_3 - m_2b_3 - |m_3|c_3 \leq m_1a_3 - m_2b_3 - (m_1 + 1)c_3 \\ &= -c_3 + m_1(a_3 - c_3) - m_2b_3 < -c_3; \end{aligned}$$

б) при $|m_3| \leq m_1$

$$\begin{aligned} \gamma_1 &= m_1a_1 + m_2b_1 - |m_3|c_1 > m_1c_1 + m_2b_1 - |m_3|c_1 \\ &= (m_1 - |m_3|)c_1 + m_2b_1 \geq b_1. \end{aligned}$$

Для $b_2 < c_2$ получаем:

а) при $|m_3| \leq m_2 - 1$

$$\begin{aligned}\gamma_1 &= m_1 a_1 + m_2 b_1 - |m_3| c_1 \geq m_1 a_1 + (|m_3| + 1) b_1 - |m_3| c_1 \\ &= b_1 + m_1 a_1 + |m_3| (b_1 - c_1) > b_1;\end{aligned}$$

б) при $|m_3| \geq m_2$ и $m_1 > 0$

$$\begin{aligned}\gamma_2 &= m_1 a_2 - m_2 b_2 + |m_3| c_2 \geq m_1 a_2 - m_2 b_2 + m_2 c_2 \\ &= m_1 a_2 + m_2 (c_2 - b_2) > a_2;\end{aligned}$$

в) при $m_1 = 0$

$$\gamma_3 = -m_2 b_3 - |m_3| c_3 < -c_3.$$

Таким образом, для решетки $\Gamma \in \mathfrak{L}_3^*(\mathbb{R})$ с базисными векторами (1.1)

$$\Gamma'(b_1, a_2, c_3) = \{\pm\gamma^{(1)}, \pm\gamma^{(2)}, \pm\gamma^{(3)}\}.$$

Следовательно, $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$ составляют минимальный базис. Лемма 1 доказана.

ЛЕММА 2. Пусть $\Gamma \in \mathfrak{L}_3^*(\mathbb{R})$ – решетка, порожденная базисными узлами

$$\begin{aligned}\gamma^{(1)} &= (a_1, a_2, a_3), \\ \gamma^{(2)} &= (b_1, -b_2, -b_3), \\ \gamma^{(3)} &= (-c_1, -c_2, c_3)\end{aligned}\tag{1.4}$$

с положительными a_i, b_i, c_i , для которых выполнено условие 1) леммы 1 и при этом $a_2 < b_2 + c_2$, $b_3 < a_3$. Тогда $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$ – минимальный базис.

ДОКАЗАТЕЛЬСТВО. Достаточно показать, что

$$\Gamma'(b_1, a_2, c_3) = \{\pm\gamma^{(1)}, \pm\gamma^{(2)}, \pm\gamma^{(3)}\}.$$

Так как $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$ – базис решетки, то для любого узла $\gamma \in \Gamma'$ найдутся целые числа m_1, m_2, m_3 , для которых

$$\begin{aligned}\gamma &= m_1 \gamma^{(1)} + m_2 \gamma^{(2)} + m_3 \gamma^{(3)} \\ &= (m_1 a_1 + m_2 b_1 - m_3 c_1, m_1 a_2 - m_2 b_2 - m_3 c_2, m_1 a_3 - m_2 b_3 + m_3 c_3).\end{aligned}\tag{1.5}$$

Достаточно ограничиться случаем, когда хотя бы два числа из m_1, m_2, m_3 отличны от нуля (см. начало доказательства леммы 1) и $m_1 \geq 0$. Тогда:

а) для $m_2 > 0$ и $m_3 \leq 0$

$$\gamma_1 = m_1 a_1 + m_2 b_1 + |m_3| c_1 > b_1;$$

б) для $m_2 \leq 0$ и $m_3 > 0$

$$\gamma_3 = m_1 a_3 + |m_2| b_3 + m_3 c_3 > c_3;$$

в) для $m_2 \leq 0$ и $m_3 \leq 0$ при $m_1 > 0$

$$\gamma_2 = m_1 a_2 + |m_2| b_2 + |m_3| c_2 > a_2,$$

а при $m_1 = 0$

$$\gamma_2 = |m_2| b_2 + |m_3| c_2 \geq c_2 + b_2 > a_2.$$

Пусть теперь $m_2 > 0$ и $m_3 > 0$. Тогда:

а) при $m_3 \leq m_2 - 1$

$$\begin{aligned}\gamma_1 &= m_1 a_1 + m_2 b_1 - m_3 c_1 \geq m_1 a_1 + (m_3 + 1)b_1 - m_3 c_1 \\ &= b_1 + m_1 a_1 + m_3(b_1 - c_1) > b_1;\end{aligned}$$

б) при $m_3 \geq m_2$ и $m_1 > 0$, учитывая что $b_3 < a_3$, находим

$$\begin{aligned}\gamma_3 &= m_1 a_3 - m_2 b_3 + m_3 c_3 \geq m_1 a_3 - m_2 b_3 + m_2 c_3 \\ &= m_1 a_3 + m_2(c_3 - b_3) \geq a_3 - b_3 + c_3 > c_3.\end{aligned}$$

Таким образом, для решетки $\Gamma \in \mathfrak{L}_3^*(\mathbb{R})$ с базисными узлами (1.4)

$$\Gamma'(b_1, a_2, c_3) = \{\pm\gamma^{(1)}, \pm\gamma^{(2)}, \pm\gamma^{(3)}\}.$$

Следовательно, узлы $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$ составляют минимальный базис. Лемма 2 доказана.

Из лемм 1 и 2 непосредственно следует теорема 1, сформулированная во введении.

§ 2. Доказательство теорем 2 и 3

Определим $F_1, F_2 \in \mathfrak{F}_3$ из равенств

$$\begin{aligned}F_1 \begin{pmatrix} \gamma_1^{(1)} & \gamma_1^{(2)} & \gamma_1^{(3)} \\ \gamma_2^{(1)} & \gamma_2^{(2)} & \gamma_2^{(3)} \\ \gamma_3^{(1)} & \gamma_3^{(2)} & \gamma_3^{(3)} \end{pmatrix} &= \begin{pmatrix} -\gamma_2^{(3)} & \gamma_2^{(1)} & -\gamma_2^{(2)} \\ \gamma_3^{(3)} & -\gamma_3^{(1)} & \gamma_3^{(2)} \\ \gamma_1^{(3)} & -\gamma_1^{(1)} & \gamma_1^{(2)} \end{pmatrix}, \\ F_2 \begin{pmatrix} \gamma_1^{(1)} & \gamma_1^{(2)} & \gamma_1^{(3)} \\ \gamma_2^{(1)} & \gamma_2^{(2)} & \gamma_2^{(3)} \\ \gamma_3^{(1)} & \gamma_3^{(2)} & \gamma_3^{(3)} \end{pmatrix} &= \begin{pmatrix} \gamma_3^{(1)} & \gamma_3^{(3)} & \gamma_3^{(2)} \\ \gamma_2^{(1)} & \gamma_2^{(3)} & \gamma_2^{(2)} \\ \gamma_1^{(1)} & \gamma_1^{(3)} & \gamma_1^{(2)} \end{pmatrix}.\end{aligned}$$

ЛЕММА 3. Пусть матрица

$$M = \begin{pmatrix} a_1 & b_1 & \varepsilon c_1 \\ a_2 & -b_2 & -c_2 \\ a_3 & -b_3 & c_3 \end{pmatrix} \quad (2.1)$$

из $GL_3^*(\mathbb{R})$ минимальна, $\varepsilon \in \{-1, 1\}$ и a_i, b_i, c_i — положительные числа, для которых b_1, a_2, c_3 — максимальные по модулю числа в строках. Тогда:

- а) для $\varepsilon = 1$ хотя бы одна из матриц $M, F_1(M)$ принадлежит к первому типу из (0.2);
- б) для $\varepsilon = -1$ хотя бы одна из матриц $M, F_2(M)$ принадлежит ко второму типу из (0.2).

ДОКАЗАТЕЛЬСТВО. Легко заметить, что $F_1(M)$ при $\varepsilon = 1$ и $F_2(M)$ при $\varepsilon = -1$ опять имеют вид (2.1).

Пусть $\varepsilon = 1$. Если $c_1 > a_1$ и $b_2 > c_2$, то $b_3 > a_3$, поскольку узел

$$\gamma^{(1)} + \gamma^{(2)} - \gamma^{(3)} = (a_1 + b_1 - c_1, a_2 - b_2 + c_2, a_3 - b_3 - c_3)$$

не лежит в $\Gamma'(b_1, a_2, c_3)$. Тогда для матрицы $F_1(M)$ условие $b_3 > a_3$ эквивалентно условию $c'_2 > b'_2$, где b'_2, c'_2 — соответствующие элементы матрицы $F_1(M)$. Таким образом, M или $F_1(M)$ принадлежит к первому типу из (0.2).

Пусть $\varepsilon = -1$. Если $a_2 > b_2 + c_2$, то узел

$$\gamma^{(2)} + \gamma^{(3)} = (b_1 - c_1, -b_2 - c_2, -b_3 + c_3)$$

лежит в $\Gamma'(b_1, a_2, c_3)$, что противоречит минимальности матрицы M . Следовательно, $a_2 < b_2 + c_2$ для всех M вида (2.1) с $\varepsilon = -1$.

Если $b_3 > a_3$, то $a_1 > c_1$, поскольку узел

$$\gamma^{(1)} + \gamma^{(2)} + \gamma^{(3)} = (a_1 + b_1 - c_1, a_2 - b_2 - c_2, a_3 - b_3 + c_3)$$

не лежит в $\Gamma'(b_1, a_2, c_3)$. Но тогда для матрицы $F_2(M)$ условие $a_1 > c_1$ эквивалентно неравенству $b''_3 < a''_3$ для соответствующих элементов матрицы $F_2(M)$. Таким образом, хотя бы одна из матриц $M, F_2(M)$ принадлежит ко второму типу из (0.2). Лемма 3 доказана.

Пусть γ, γ' — минимумы Γ и $i \in \{1, 2, 3\}$. Следуя [1], назовем γ' смежным с γ по координате i , если выполнены условия:

- 1) $|\gamma'_i| > |\gamma_i|$; $|\gamma'_j| < |\gamma_j|$ для всех $j \neq i$;
- 2) $\Gamma'(x) = \{\pm\gamma, \pm\gamma'\}$ с $x_i = \gamma'_i$ и $x_j = \gamma_j$ для всех $j \neq i$.

Очевидно, что для любой пары смежных минимумов один из них смежен с другим по некоторой координате. Для $i \in \{1, 2, 3\}$ обозначим через π_i проекцию $\mathbb{R}^3$ в $\mathbb{R}^2$ вдоль координаты с индексом i . При этом

$$\pi_1(x_1, x_2, x_3) = (x_2, x_3), \quad \pi_2(x_1, x_2, x_3) = (x_1, x_3), \quad \pi_3(x_1, x_2, x_3) = (x_1, x_2).$$

Легко показать (см. [4]), что для любой пары смежных минимумов γ и γ' найдется координата j , для которой $\eta^{(j)} = \pi_j(\gamma)$ и $\xi^{(j)} = \pi_j(\gamma')$ составляют минимальный базис порожденной ими двумерной решетки. Такую координату назовем *регулярной* для пары смежных минимумов γ, γ' . Из определения непосредственно следует

ЗАМЕЧАНИЕ 3. Пусть γ' смежен с γ по координате i . Тогда координата i не является регулярной, а среди остальных координат регулярна по крайней мере одна.

Пусть $S = \{\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}\}$ — минимальное множество $\Gamma \in \mathfrak{L}_3^*(\mathbb{R})$. Переставляя в случае необходимости узлы, мы можем считать, что для $i = 1, 2, 3$

$$|\gamma_i^{(i)}| = \max\{|\gamma_i^{(1)}|; |\gamma_i^{(2)}|; |\gamma_i^{(3)}|\} = |S|_i. \quad (2.2)$$

Справедливо следующее утверждение.

ЛЕММА 4. Если узлы из S линейно независимы, то найдется координата с индексом i , которая регулярна относительно пары узлов из S , отличных от $\gamma^{(i)}$.

ДОКАЗАТЕЛЬСТВО. Предположим, что утверждение леммы 4 неверно. Обозначим через M матрицу из $GL_3^*(\mathbb{R})$, соответствующую узлам $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$. Для некоторого преобразования $F \in \mathfrak{F}_3$ положим $\widetilde{M} = F(M)$, а $\widetilde{\gamma}^{(1)}, \widetilde{\gamma}^{(2)}, \widetilde{\gamma}^{(3)}$ — соответствующий $\widetilde{M}$ базис решетки $\Gamma(\widetilde{M}) = \widetilde{\Gamma}$.

Из нерегулярности всех координат относительно соответствующей пары узлов из $\{\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}\}$ следует, что знаки в каждой паре произведений $\gamma_i^{(i)}\gamma_j^{(j)}$ и $\gamma_j^{(i)}\gamma_i^{(j)}$ для $(i, j) \in \{(2, 3), (1, 3), (1, 2)\}$ одинаковые. Поэтому можно выбрать F (речь идет только о перемене знаков) таким, что

$$\widetilde{\gamma}^{(1)} = (a_1, \varepsilon_1 a_2, \varepsilon_2 a_3), \quad \widetilde{\gamma}^{(2)} = (\varepsilon_1 b_1, b_2, \varepsilon_3 b_3), \quad \widetilde{\gamma}^{(3)} = (\varepsilon_2 c_1, \varepsilon_3 c_2, c_3)$$

с $\varepsilon_1, \varepsilon_2, \varepsilon_3 \in \{-1, 1\}$ и положительными a_i, b_i, c_i . Заметим, что

$$\widetilde{\gamma}^{(2)} = \varepsilon_1 (b_1, \varepsilon_1 b_2, \varepsilon_1 \varepsilon_3 b_3).$$

Поскольку $\widetilde{\gamma}^{(1)}$ и $\widetilde{\gamma}^{(2)}$ — смежные минимумы, то $\varepsilon_2 = -\varepsilon_1 \varepsilon_3$. Соответствующая множеству $\{\widetilde{\gamma}^{(1)}, \widetilde{\gamma}^{(2)}, \widetilde{\gamma}^{(3)}\}$ минимальная матрица имеет вид

$$\begin{pmatrix} a_1 & \varepsilon_1 b_1 & \varepsilon_2 c_1 \\ \varepsilon_1 a_2 & b_2 & -\varepsilon_1 \varepsilon_2 c_2 \\ \varepsilon_2 a_3 & -\varepsilon_1 \varepsilon_2 b_3 & c_3 \end{pmatrix}. \quad (2.3)$$

Умножим вторую и третью строки матрицы соответственно на $\varepsilon_1, \varepsilon_2$, а затем умножим второй и третий столбец на $\varepsilon_1, \varepsilon_2$. Тогда (2.3) преобразуется в минимальную матрицу

$$\begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & -c_2 \\ a_3 & -b_3 & c_3 \end{pmatrix}. \quad (2.4)$$

Заметим, что у узла

$$(a_1, a_2, a_3) - (b_1, b_2, -b_3) = (a_1 - b_1, a_2 - b_2, a_3 + b_3)$$

первые две координаты по абсолютной величине не превосходят a_1, b_2 соответственно. Тогда из минимальности матрицы следует, что $a_3 + b_3 > c_3$. Далее, у узла

$$\begin{aligned} & (a_1, a_2, a_3) - (b_1, b_2, -b_3) - (c_1, -c_2, c_3) \\ &= (a_1 - b_1 - c_1, a_2 - b_2 + c_2, a_3 + b_3 - c_3) \end{aligned}$$

абсолютные величины всех трех координат не превосходят a_1, b_2, c_3 соответственно. Поэтому по причине минимальности (2.4) третий столбец равен разности первого и второго. А это противоречит линейной независимости узлов $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$. Лемма 4 доказана.

ЗАМЕЧАНИЕ 4. При доказательстве леммы 4 мы попутно установили, что если узлы $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$ линейно зависимы (над $\mathbb{R}$) и составляют минимальное подмножество решетки, то один из них равен сумме двух остальных.

Теперь докажем теоремы 2 и 3.

Воспользовавшись в случае необходимости преобразованием из $\mathfrak{F}_3$, на основании леммы 4 мы можем считать, что

$$\gamma^{(1)} = (a_1, a_2, a_3), \quad \gamma^{(2)} = (\pm b_1, b_2, \pm b_3), \quad \gamma^{(3)} = (\pm c_1, \pm c_2, c_3)$$

с положительными a_i, b_i, c_i , для которых выполнено (2.2), и $\gamma^{(2)}$ с $\gamma^{(3)}$ образуют регулярную по первой координате пару. Тогда матрица M , определяемая узлами $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$, имеет один из двух видов:

$$M_1 = \begin{pmatrix} a_1 & -b_1 & \pm c_1 \\ a_2 & b_2 & -c_2 \\ a_3 & b_3 & c_3 \end{pmatrix}, \quad M_2 = \begin{pmatrix} a_1 & \pm b_1 & -c_1 \\ a_2 & b_2 & c_2 \\ a_3 & -b_3 & c_3 \end{pmatrix}$$

с положительными a_i, b_i, c_i . Применяя преобразования из $\mathfrak{F}_3$ вида

$$M_1 \rightarrow \begin{pmatrix} b_1 & a_1 & \pm c_1 \\ b_2 & -a_2 & -c_2 \\ b_3 & -a_3 & c_3 \end{pmatrix}, \quad M_2 \rightarrow \begin{pmatrix} c_1 & a_1 & \pm b_1 \\ c_3 & -a_3 & -b_3 \\ c_2 & -a_2 & b_2 \end{pmatrix},$$

мы попадаем в условия леммы 3.

Таким образом, мы показали, что если $\{\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}\}$ – минимальное множество и $\gamma^{(1)}, \gamma^{(2)}, \gamma^{(3)}$ – линейно независимые узлы решетки, то найдется преобразование F из $\mathfrak{F}_3$, переводящее матрицу M в матрицу $\widetilde{M} = F(M)$, где

$$M = \begin{pmatrix} \gamma_1^{(1)} & \gamma_1^{(2)} & \gamma_1^{(3)} \\ \gamma_2^{(1)} & \gamma_2^{(2)} & \gamma_2^{(3)} \\ \gamma_3^{(1)} & \gamma_3^{(2)} & \gamma_3^{(3)} \end{pmatrix},$$

$$\widetilde{M} = \begin{pmatrix} \widetilde{\gamma}_1^{(1)} & \widetilde{\gamma}_1^{(2)} & \widetilde{\gamma}_1^{(3)} \\ \widetilde{\gamma}_2^{(1)} & \widetilde{\gamma}_2^{(2)} & \widetilde{\gamma}_2^{(3)} \\ \widetilde{\gamma}_3^{(1)} & \widetilde{\gamma}_3^{(2)} & \widetilde{\gamma}_3^{(3)} \end{pmatrix} = \begin{pmatrix} a_1 & b_1 & \varepsilon c_1 \\ a_2 & -b_2 & -c_2 \\ a_3 & -b_3 & c_3 \end{pmatrix}$$

с ограничениями:

- 1) a_i, b_i, c_i – положительные числа;
- 2) $b_1 = \max(a_1; b_1; c_1)$, $a_2 = \max(a_2; b_2; c_2)$, $c_3 = \max(a_3; b_3; c_3)$;
- 3) если $\varepsilon = 1$, то выполняется хотя бы одно из неравенств $c_1 < a_1$, $b_2 < c_2$, а если $\varepsilon = -1$, то $a_2 < b_2 + c_2$ и $b_3 < a_3$.

Следуя работе [3], дополним $\widetilde{\gamma}^{(1)}, \widetilde{\gamma}^{(2)}$ до базиса решетки $\widetilde{\Gamma}$ третьим узлом γ с $|\gamma_1| < b_1$, $|\gamma_2| < a_2$ и минимальным $|\gamma_3|$. При этом γ можно выбрать в виде

$$\gamma = (\pm c'_1, -c'_2, c'_3)$$

с положительными c'_1, c'_2, c'_3 и для матрицы, составленной из $\widetilde{\gamma}^{(1)}, \widetilde{\gamma}^{(2)}, \gamma$, выполнены условия леммы 3. Поэтому множества $\{\widetilde{\gamma}^{(1)}, \widetilde{\gamma}^{(2)}, \widetilde{\gamma}^{(3)}\}$ и $\{\widetilde{\gamma}^{(1)}, \widetilde{\gamma}^{(2)}, \gamma\}$ одновременно минимальны. А это возможно только для $\widetilde{\gamma}^{(3)} = \gamma$. Теоремы 2 и 3 полностью доказаны.

Список литературы

1. *Вороной Г. Ф.* Собрание сочинений. Т. 1. Киев, 1952.
2. *Minkowski H.* Zur Theorie der Kettenbrüche // Gesammelte Abhandlungen. Leipzig, 1911. P. 278–292.
3. *Buchmann J.* On the Computation of units and class numbers by a generalization of Lagrange's algorithm // Journal Number Theory. 1987. V. 26. P. 8–30.
4. *Быковский В. А.* Теорема Валена для двумерных подходящих дробей // Матем. заметки. 1999. Т. 66. № 1. С. 30–37.
5. *Горкуша О. А.* Приведение базисов трехмерных решеток // Препринт. ИПМ ДВО РАН. Владивосток: Дальнаука, 1998.

Хабаровское отделение
Института прикладной математики ДВО РАН
E-mail: vab@iam.khv.ru, gorkusha@iam.khv.ru

Поступила в редакцию
24.06.1999