УДК 512.54

В. Г. Бардаков

Построение ортогональных базисов некоторых решеток [1]

Аннотация

В работе рассматривается вопрос о существовании ортогонального базиса в некоторых решетках. Для $\mathbf{Z}$–решетки в евклидовом пространстве $V = \mathbf{R}^n$ выписывается система диофантовых уравнений и доказывается, что ее разрешимость равносильна существованию ортогонального базиса соответствующей решетки. При этом, разрешимость этой системы эффективно проверяется за конечное число шагов. В последнем параграфе рассматривается вопрос (сформулированый в "Коуровской тетради"(вопрос 9.45)) о существовании ортогонального базиса решетки $S(a) = \{ka + b \mid k \in \mathbf{Z}, b \in \mathbf{Z}^n\}$, где $a \in \mathbf{Q}^n$, в пространстве $V = \mathbf{Q}^n$.

Пусть V — векторное пространство над полем k, I — некоторое подкольцо в k. Если a_1, a_2, $\ldots$, a_m — система векторов из V, то *I–решеткой* называется совокупность всех векторов вида

$$\alpha_1 a_1 + \alpha_2 a_2 + \ldots + \alpha_m a_m, \qquad \alpha_i \in I.$$

Будем обозначать эту решетку символом $L = \mathcal{L}_I(a_1, a_2, \ldots, a_m)$. Другими словами, L является I–модулем, порожденным векторами $a_1, a_2 \ldots, a_m$.

В евклидовом пространстве $V = \mathbf{R}^n$, $n \in \mathbf{N}$, $\mathbf{Z}$–решетки изучались в теории чисел такими математиками, как Эрмит, Минковский, Воронов и др. (см. [1; 2, гл. 2, § 3]). В случае, когда I — дедекиндово кольцо, а k — его поле частных, базисы I–решеток исследовались в работах Дедекинда, Штейница, Д. К. Фаддеева (см. [3] и цитированную там литературу).

В предлагаемой работе рассматривается вопрос о существовании ортогонального базиса в некоторых решетках. Если на n–мерном векторном пространстве V задана симметрическая билинейная форма φ, то V обладает ортогональным базисом [4, с. 29], т. е. таким базисом $e_1, e_2 \ldots, e_n$, что $\varphi(e_i, e_j) = 0$ при $i \neq j$. Возникает естественный вопрос: если L — некоторая I–решетка в V, то при каких условиях она обладает ортогональным базисом? В работе этот вопрос исследуется для формы φ, определяющей евклидово скалярное произведение в пространстве V.

В § 1 напоминаются общие свойства решеток и, в частности, отмечается, что задача о построении ортогонального базиса I–решетки L равносильна задаче о I–эквивалентности квадратичной формы, построенной по L, диагональной форме. Там же рассматриваются решетки в векторных пространствах над полем p–адических чисел $\mathbf{Q}^{(p)}$. Доказывается, что если p — нечетное простое число, то всякая $\mathbf{Z}^{(p)}$–решетка, где $\mathbf{Z}^{(p)}$ — кольцо целых p–адических чисел, обладает ортогональным базисом.

[1] Работа выполнена при финансовой поддержке РФФИ.

В оставшейся части работы рассматриваются $\mathbf{Z}$–решетки в евклидовом пространстве $V = \mathbf{R}^n$. Отметим, что для двумерных рациональных решеток критерий существования ортогонального базиса известен (см. [5], [6]).

В § 2 устанавливается, что если $\mathbf{Z}$–решетке L соответствует положительно определенная квадратичная форма, приведенная по Минковскому, то существует эффективный алгоритм, позволяющий проверить: обладает ли решетка L ортогональным базисом. К сожалению, в общем случае не существует эффективной процедуры, позволяющей от произвольной положительно определенной квадратичной формы перейти к эквивалетной и являющейся приведенной по Минковскому. Для решеток, лежащих в пространствах небольшой размерности, в частности, в размерности 2 и 3, такие алгоритмы существуют. Поэтому для двумерных и трехмерных решеток можно указать критерий существования ортогонального базиса в терминах теории приведения. Отметим, что такие решетки находят применение в кристаллографии (см. [7]).

Далее предлагается другой способ проверить: обладает ли целочисленная решетка ортогональным базисом. Для этого выписывается система диофантовых уравнений и доказывается (теорема 1), что ее разрешимость равносильна существованию ортогонального базиса соответствующей решетки. При этом, разрешимость этой системы эффективно проверяется за конечное число шагов. В заключение этого параграфа будет установлено, что всякая целая квадратичная форма $\mathbf{Z}$–эквивалентна форме, имеющей трехдиагональную матрицу.

В § 3 рассматривается вопрос о существовании ортогонального базиса решетки $S(a) = \{ka + b \mid k \in \mathbf{Z}, b \in \mathbf{Z}^n\}$, где $a \in \mathbf{Q}^n$, в пространстве $V = \mathbf{Q}^n$. Вначале будет построен некоторый ступенчатый базис этой решетки, а затем будет установлено, что решетка $S(a)$ обладает ортогональным базисом тогда и только тогда, когда разрешима некоторая система диофантовых уравнений. При этом разрешимость этой системы эффективно проверяется за конечное число шагов. Вопрос о существовании ортогонального базиса решетки $S(a)$ сформулирован в [8] (вопрос 9.45).

Благодарю всех участников семинара “Эварист Галуа” за полезнные замечания и предложения.

§ 1. Общие свойства решеток

Пусть V — n–мерное векторное пространство над полем k. В V определено скалярное произведение

$$x \cdot y = \sum_{i=1}^{n} x^i y^i.$$

где $x = \sum_{i=1}^n x^i e_i$, $y = \sum_{i=1}^n y^i e_i$ — векторы из V, разложенные по базису $e_1, e_2, \ldots, e_n$ пространства V.

Если I — подкольцо поля k, а M — некоторая матрица с элементами из k, то I–элементарными преобразованиями строк матрицы M называются следующие два типа преобразований: умножение строки на обратимый элемент кольца I; умножение некоторой строки на элемент из I и прибавление к другой строке. Аналогично определяются элементарные преобразования столбцов матрицы M.

Со всякой I–решеткой L, порожденной векторами $a_1, a_2, \ldots, a_m$, можем связать матрицу $A = (a_{ij}) \in \mathbf{M}_{m,n}(k)$, $i = 1, \ldots, m$, $j = 1, \ldots, n$, строками которой являются координаты векторов $a_1, a_2, \ldots, a_m$. Верно и обратное, — всякой матрице из $\mathbf{M}_{m,n}(k)$ соответствует решетка, порожденная строками этой матрицы. Если кольцо I является евклидовым, то используя I–элементарные преобразования строк матрицы, легко показать, что всякая I–решетка обладает базисом. Аналогичное утверждение справедливо и для некоторых других колец, в частности для дедекиндовых [3].

Легко проверить, что две линейно независимые системы векторов $f_1, f_2, \ldots, f_m$ и $g_1, g_2, \ldots, g_m$ из V определяют одну и ту же I–решетку тогда и только тогда, когда найдется матрица $T = (\alpha_{ij}) \in \mathbf{GL}_m(I)$ такая, что

$$g_i = \sum_{j=1}^{m} \alpha_{ij} f_j, \qquad i = 1, \ldots, m. \tag{1}$$

Если векторы $f_1, f_2, \ldots, f_m$ образуют базис I–решетки L, то *матрицей Грама* этого базиса называется симметрическая матрица $F = (f_i \cdot f_j) \in \mathbf{GL}_m(k)$. При переходе к новому базису по формулам (1) матрица Грама базиса $g_1, g_2, \ldots, g_m$ будет иметь вид $G = TFT^t$, где символ t означает транспонирование. Очевидно, если $g_1, g_2, \ldots, g_m$ — ортогональный базис, то матрица G является диагональной. Таким образом, справедлива

Лемма 1. *Пусть F — матрица Грама некоторого базиса I–решетки L. Решетка L обладает ортогональным базисом тогда и только тогда, когда найдется матрица T из $\mathbf{GL}_m(I)$ такая, что TFT^t — диагональная матрица.*

С другой стороны, так как матрица Грама F является симметрической, то мы можем сопоставить ей квадратичную форму

$$\psi_L(x) = \sum_{i,j=1}^{m} (f_i \cdot f_j) x_i x_j, \quad x = (x_1, x_2, \ldots, x_m), \tag{2}$$

с матрицей F. При этом, если в форме $\psi_L(x)$ перейти к другим переменным $y = (y_1, \ldots, y_m)$ по формулам

$$x_i = \sum_{j=1}^{m} \alpha_{ij} y_j, \quad i = 1, \ldots, m,$$

где $T = (\alpha_{ij})$ — некоторая матрица из $\mathbf{GL}_m(I)$, то в новых переменных форма $\psi_L(y) = \psi_L(xT) = yTFT^t y^t$ будет иметь матрицу TFT^t. Из этого замечания и леммы 1 легко вытекает

Лемма 2. *Пусть L —некоторая m–мерная I–решетка в пространстве V, F — матрица Грама некоторого базиса решетки L. Решетка L обладает ортогональным базисом тогда и только тогда, когда квадратичная форма $\psi_L(x) = xFx^t$ I–эквивалентна некоторой диагональной квадратичной форме.*

Рассмотрим в качестве поля k поле p–адических чисел $\mathbf{Q}^{(p)}$, а в качестве кольца I — кольцо целых p–адических чисел $\mathbf{Z}^{(p)}$. В этом случае справедливо

Предложение 1. *Пусть p —нечетное простое число. Тогда всякая $\mathbf{Z}^{(p)}$–решетка L векторного пространства V над полем $\mathbf{Q}^{(p)}$ обладает ортогональным базисом.*

Доказательство. Предположим, что решетка L задана некоторым своим базисом и $A = (a_{ij}) \in \mathbf{GL}_m(\mathbf{Q}^{(p)})$ — матрица Грама этого базиса. Ввиду леммы 2 решетка L обладает ортогональным базисом тогда и только тогда, когда квадратичная форма

$$\psi_L(x) = \sum_{i,j=1}^{m} a_{ij}x_ix_j, \quad a_{ij} \in \mathbf{Q}^{(p)},$$

$\mathbf{Z}^{(p)}$–эквивалентна диагональной форме. Выберем натуральное число d так, что все коэффициенты формы представимы в виде $a_{ij} = p^{-d}b_{ij}$, где b_{ij}, $i, j = 1, \ldots, m$, — целые p–адические числа. Тогда форма $\psi_L(x)$ представима в виде $\psi_L(x) = p^{-d}\xi(x)$, где $\xi(x) = \sum_{i,j=1}^{m} b_{ij}x_ix_j$ — p–адически целочисленная форма. Так как форма $\xi(x)$ может быть диагонализирована посредством p–адически целочисленного преобразования (т. е. преобразования из $\mathbf{GL}_m(\mathbf{Z}^{(p)})$) [9, с. 465], то и форма $\psi_L(x)$ может быть диагонализирована при помощи преобразования из $\mathbf{GL}_m(\mathbf{Z}^{(p)})$. Предложение доказано.

§ 2. Решетки в евклидовом пространстве

В этом параграфе мы считаем, что $k = \mathbf{R}$ — поле вещественных чисел, а $I = \mathbf{Z}$ — кольцо целых чисел. Вместо терминов "$\mathbf{Z}$–решетка", "$\mathbf{Z}$–эквивалентность" будем употреблять термины "решетка", "эквивалентность".

Решетку L из V будем называть *рациональной* (*целочисленной*), если координаты всех векторов из L являются рациональными (соответственно, целыми) числами. Для рациональных решеток справедлива

Лемма 3 ([6, лемма 2]). *Для всякой рациональной решетки L существует изоморфная ей целочисленная решетка M такая, что L обладает ортогональным базисом в точности тогда, когда ортогональным базисом обладает решетка M.*

Ввиду леммы 2 задача о построении ортогонального базиса свелась к задаче о диагонализируемости соответствующей квадратичной формы. Поэтому далее будем рассматривать положительно определенную вещественную квадратичную форму

$$\psi(x) = \sum_{i=1}^{m} a_{ij}x_ix_j, \quad a_{ij} = a_{ji}, \quad a_{ji} \in \mathbf{R}. \tag{3}$$

Напомним, что форма $\psi(x)$ называется *целой*, если все коэффициенты a_{ij} являются целыми числами, *определителем* $\det\psi$ формы ψ называется определитель $\det A$ матрицы $A = (a_{ij})$.

Наша задача — найти критерий эквивалентности формы $\psi(x)$ некоторой диагональной форме. Заметим, что если форма ψ эквивалентна диагональной форме $\xi(y) = d_1y_1^2 + d_2y_2^2 + \ldots + d_my_m^2$,

$d_i \in \mathbf{R}$, то, не уменьшая общности, будем считать, что коэффициенты этой формы связаны системой неравенств: $0 < d_1 \le d_2 \le \ldots \le d_m$. Так как определители эквивалентных форм равны, то $\det\psi = d_1 d_2 \ldots d_m$.

Напомним (см. [4, с. 276]), что форма $\psi(x)$ называется *приведенной по Минковскому*, если для любого j, $1 \le j \le m$, выполняются неравенства

$$\psi(e_j) \le \psi(v), \tag{4}$$

где $e_j = (0, \ldots, 0, 1, 0, \ldots, 0)$ (1 стоит на j–м месте), а v пробегает все такие целочисленные векторы, что $e_1, e_2, \ldots, e_{j-1}, v$ можно продолжить до базиса решетки $\mathcal{L}_{\mathbf{Z}}(e_1, e_2, \ldots, e_m)$. Иначе условие (4) может быть записано так:

$$a_{jj} = \psi(e_j) \le \psi(b_1, \ldots, b_m),$$

где $b_1, \ldots, b_m$ — такие целые числа, что НОД$(b_j, b_{j+1} \ldots, b_m)$=1.

Так как всякая положительно определенная форма эквивалентна по меньшей мере одной и не более чем конечному числу приведенных форм [4, с. 277], то не уменьшая общности, будем считать, что рассматриваемая нами форма $\psi(x)$ является приведенной. Справедливо

Предложение 2. *Пусть $A \in \mathbf{GL}_m(\mathbf{R})$ — матрица положительно определенной, приведенной по Минковскому формы $\psi(x)$. Существует постоянная C, зависящая только от числа переменных m такая, что форма $\psi(x)$ эквивалентна диагональной форме тогда и только тогда, когда множество $\mathcal{M} = \{TAT^t \mid T = (t_{ij}) \in \mathbf{GL}_m(\mathbf{Z}), |t_{ij}| \le C, \quad при \quad всех\, i, j = 1, \ldots, m\}$ содержит диагональную матрицу.*

Доказательство. Предположим, что форма $\psi(x)$ эквивалентна диагональной форме. Не уменьшая общности, можно считать, что, ввиду положительной определенности, матрица D этой диагональной формы имеет вид $D = \mathrm{diag}(d_1, \ldots, d_m)$, $0 < d_1 \le d_2 \le \ldots \le d_m$. Очевидно, диагональная форма приведена. Из теории приведенных форм [4, с. 277] известно, что если формы $\psi(x)$ и $\psi(xQ)$ приведены, причем $Q = (q_{ij}) \in \mathbf{GL}_m(\mathbf{Z})$, то $|q_{ij}| \le C$, где C — постоянная, зависящая только от m. Взяв это значение C и, построив по нему множество $\mathcal{M}$, видим, что матрицы всех приведенных форм, эквивалентных форме ψ, содержатся в этом множестве. Отсюда и следует требуемое утверждение.

Таким образом, вопрос об эквивалентности положительно определенной формы некоторой диагональной форме, а вместе с ним и вопрос о существовании ортогонального базиса произвольной $\mathbf{Z}$–решетки, имеет эффективное решение в рамках теории приведения Минковского.

К сожалению, в общем случае мне не известен алгоритм, позволяющий по форме $\psi(x)$ построить эквивалентную ей приведенную форму. Тем не менее, для малых значений m, в частности для $m = 2, 3, 4$, такие алгоритмы существуют. Рассмотрим их более подробно, опираясь на результаты работы [10].

Положительно определенная бинарная квадратичная форма

$$\psi(x, y) = ax^2 + 2bxy + cy^2, \quad a, b, c \in \mathbf{R},$$

называется *приведенной по Лагранжу* если ее коэффициенты удовлетворяют неравенствам

$$0 \leq 2b \leq a \leq c.$$

Существуе эффективная процедура [10, § 3], позволяющая по произвольной положительно определенной бинарной квадратичной форме построить эквивалентную ей приведенную по Лагранжу форму. При этом приведенная форма определяется единственным образом. Следовательно, мы имеем

Предложение 3. *Положительно определенная бинарная квадратичная форма*

$$\psi(x, y) = ax^2 + 2bxy + cy^2, \quad a, b, c \in \mathbf{R},$$

эквивалентна диагональной форме тогда и только тогда, когда приведенная по Лагранжу форма, соответствующая $\psi(x, y)$ имеет диагональный вид.

Можно дать и геометрическую интерпретацию этого предложения. Рассматривая двумерную решетку $L \subseteq \mathbf{R}^2$ как множество точек, являющихся концами векторов из L, получим параллепепидальную систему [10, § 5]. С каждой точкой O этой параллепепидальной системы можно связать область Дирихле, состоящую из множества всех точек плоскости $\mathbf{R}^2$, которые отстоят от точки O не далее, чем от любой другой точки этой параллепепидальной системы. Для двумерной параллепепидальной системы область Дирихле является либо шестиугольником, либо прямоугольником. Используя связь между двумерными решетками и бинарными квадратичными формами, из предложения 3 легко вывести

Следствие. *Двумерная решетка обладает ортогональным базисом тогда и только тогда, когда соответствующая ей область Дирихле является прямоугольником.*

Рассмотрим далее трехмерные решетки. Если трехмерная решетка L обладает базой v_1, v_2, v_3, то выберем вектор u такой, что $v_1 + v_2 + v_3 + u = 0$. Векторы v_1, v_2, v_3, u определяют четырехсторонник Зеллинга [10, § 8]. Перейдем от решетки L к квадратичной форме

$$\psi(x, y, z) = ax^2 + by^2 + cz^2 + 2kxy + 2hxz + 2gyz, \quad a, b, c, k, h, g \in \mathbf{R},$$

где $a = v_1 \cdot v_1$, $b = v_2 \cdot v_2$, $c = v_3 \cdot v_3$, $k = v_1 \cdot v_2$, $h = v_1 \cdot v_3$, $g = v_2 \cdot v_3$, — коэффициенты матрицы Грама. По этим коэффициентам из системы

$$a + k + h + l = 0, \quad k + b + g + m = 0, \quad h + g + c + n = 0,$$

найдем значения l, m, n. Далее, по коэффициентам g, h, k, l, m, n, построим тетраэдрический символ Делоне и используем алгоритм приведения [10, § 38]. При этом будем применять алгоритм приведения не только к положительным параметрам символа Делоне, но и к нулевым. В результате получим конечное множество приведенных символов Делоне каждому из которых соответствует квадратичная форма эквивалентная исходной. Поэтому справедливо

Предложение 4. *Трехмерная решетка L в пространстве $\mathbf{R}^3$ обладает ортогональным базисом тогда и только тогда, когда среди приведенных символов Делоне, соответствующих решетке L, найдется символ, которому соответствует диагональная квадратичная форма.*

Аналогичное предложение можно сформулировать и для четырехмерных решеток, если вместо тетраэдрического символа использовать пятиугольный символ [10, § 51].

В общем же случае справедлива

Теорема 1. *Целая положительно определенная форма $\psi(x) = \sum_{i,j=1}^{m} a_{ij}x_ix_j$, зависящая от m переменных $x = (x_1, x_2, \ldots, x_m)$ эквивалентна диагональной форме тогда и только тогда, когда найдутся целые числа $d_1, d_2, \ldots, d_m$ такие, что $1 \le d_1 \le d_2 \le \ldots \le d_m$, $d_1d_2 \ldots d_m = \det\psi$, и матрица $T = (t_{ij}) \in \mathbf{SL}_m(\mathbf{Z})$ элементы которой удовлетворяют следующей системе*

$$\sum_{k=1}^{m} d_k t_{ik}^2 = a_{ii}, \quad \sum_{k=1}^{m} d_k t_{ik}t_{jk} = a_{ij}, \quad 1 \le i < j \le m.$$

Доказательство. Предположим, что форма $\psi(x)$ эквивалентна диагональной форме $\xi(y) = yDy^t$, $D = \mathrm{diag}(d_1, d_2, \ldots, d_m)$. Не уменьшая общности, будем считать, что $1 \le d_1 \le \ldots \le d_m$. Кроме того, так как определители эквивалентных форм равны, то $d_1d_2 \ldots d_m = \det\psi$. Из определения эквивалентных форм следует существование матрицы $T = (t_{ij}) \in \mathbf{GL}_m(\mathbf{Z})$ такой, что $y = xT$ и $\psi(x) = \xi(xT)$. Распишем последнее равенство в развернутом виде:

$$\sum_{i,j=1}^{m} a_{ij}x_ix_j = \sum_{k=1}^{m} d_k(x_1t_{1k} + x_2t_{2k} + \ldots x_mt_{mk})^2.$$

Раскрывая скобки в правой части и приводя подобные слагаемые, получим

$$\sum_{i,j=1}^{m} a_{ij}x_ix_j = \sum_{i,j=1}^{m} \left(\sum_{k=1}^{m} d_k t_{ik}t_{jk} \right) x_ix_j.$$

Приравнивая коэффициенты при одинаковых мономах, получим m^2 равенств

$$\sum_{k=1}^{m} d_k t_{ik}t_{jk} = a_{ij}, \quad i, j = 1, 2, \ldots, m.$$

Так как матрица $A = (a_{ij})$ симметрическая, то среди этих равенств будет $m(m+1)/2$ различных:

$$\sum_{k=1}^{m} d_k t_{ik}^2 = a_{ii}, \quad i = 1, 2, \ldots, m, \tag{5}$$

$$\sum_{k=1}^{m} d_k t_{ik}t_{jk} = a_{ij}, \quad 1 \le i < j \le m. \tag{6}$$

Добавим к этим равенствам условие того, что определитель матрицы T равен 1:

$$\det T = 1 \tag{7}$$

(легко показать, что если существует матрица $Q \in \mathbf{GL}_m(\mathbf{Z})$ такая, что QAQ^t — диагональная матрица, то существует матрица $Q_1 \in \mathbf{SL}_m(\mathbf{Z})$ такая, что $Q_1AQ_1^t$ также диагональная матрица). Теорема доказана.

Отметим, что эта теорема дает и практический способ построения матрицы T. Действительно, непосредственно из системы видим, что коэффициенты t_{ij} удовлетворяют неравенствам $|t_{ij}| \le \sqrt{a_{ii}/d_j}$, а потому нам надо рассмотреть лишь конечное число таких матриц.

Будем рассматривать систему (5)–(7) как систему диофантовых уравнений. Найти ее общее решение для произвольного m по–видимому довольно сложно. Первым шагом в этом направлении является следующее утверждение, поэволяющее найти первый столбец матрицы T.

Предложение 5. *Целая положительно определенная форма*

$$\psi(x) = \sum_{i,j=1}^{m} a_{ij}x_ix_j$$

эквивалентна диагональной форме тогда и только тогда, когда найдутся целые числа $\varepsilon = \pm 1$, $d_1, d_2, \ldots, d_m$, t_{ij}, $i = 2, 3, \ldots, m$, $j = 1, 2, \ldots, m$, *такие, что* $1 \le d_1 \le \ldots \le d_m$, $d_1d_2 \ldots d_m = \det\psi$, $|t_{ij}| \le \sqrt{a_{ii}/d_j}$,

$$(a_{1j} - \sum_{k=2}^{m} d_kt_{1k}t_{jk})^2 + (a_{11} - \sum_{k=2}^{m} d_kt_{1k}^2)(\sum_{k=2}^{m} d_kt_{jk}^2 - a_{jj}) = 0, \quad j = 2, \ldots, m,$$

$$(a_{1i} - \sum_{k=2}^{m} d_kt_{1k}t_{ik})(a_{1j} - \sum_{k=2}^{m} d_kt_{1k}t_{jk}) + (a_{11} - \sum_{k=2}^{m} d_kt_{1k}^2)(\sum_{k=2}^{m} d_kt_{ik}t_{jk} - a_{ij}) = 0,$$
$$2 \le i < j \le m,$$

$$(a_{11} - \sum_{k=2}^{m} d_kt_{1k}^2) + \sum_{j=2}^{m}(a_{1j} - \sum_{k=2}^{m} d_kt_{1k}t_{jk})T_{j1} = \varepsilon\sqrt{d_1(a_{11} - \sum_{k=2}^{m} d_kt_{1k}^2)},$$

где T_{j1} *— алгебраическое дополнение элемента* t_{j1} *матрицы* (t_{ij})*; и целые числа* $t_{11}, t_{21}, \ldots, t_{m1}$, *удовлетворяющие равенствам*:

$$t_{11} = \varepsilon\sqrt{(a_{11} - \sum_{k=2}^{m} d_kt_{1k}^2)/d_1}, \quad t_{j1} = \frac{a_{1j} - \sum_{k=2}^{m} d_kt_{1k}t_{jk}}{\varepsilon\sqrt{d_1(a_{11} - \sum_{k=2}^{m} d_kt_{1k}^2)}}, \quad j = 2, 3, \ldots, m.$$

Доказательство. Рассмотрим систему (6). Зафиксировав $i = 1$, выделим из этой системы $m - 1$ уравнение:

$$\sum_{k=1}^{m} d_kt_{1k}t_{jk} = a_{1j}, \quad j = 2, 3, \ldots, m.$$

Представим их в таком виде

$$d_1t_{11}t_{j1} + \sum_{k=2}^{m} d_kt_{1k}t_{jk} = a_{1j}, \quad j = 2, 3, \ldots, m.$$

Выражая отсюда t_{j1}, получим

$$t_{j1} = (a_{1j} - \sum_{k=2}^{m} d_k t_{1k} t_{jk})/(d_1 t_{11}), \quad j = 2, 3, \ldots, m. \tag{8}$$

Представим выражение из (5) в таком виде

$$d_1 t_{i1}^2 + \sum_{k=2}^{m} d_k t_{ik}^2 = a_{ii}, \quad i = 1, 2, \ldots, m.$$

Первое уравнение этой системы оставим без изменений, а в остальные подставим выражение для t_{i1} из (8). После несложных преобразований получим систему

$$d_1 t_{11}^2 + \sum_{k=2}^{m} d_k t_{1k}^2 = a_{11}, \tag{9}$$

$$(a_{1j} - \sum_{k=2}^{m} d_k t_{1k} t_{jk})^2 + d_1 t_{11}^2 (\sum_{k=2}^{m} d_k t_{jk}^2 - a_{jj}) = 0, \quad j = 2, 3, \ldots, m. \tag{10}$$

Из (9) находим:

$$t_{11} = \varepsilon \sqrt{(a_{11} - \sum_{k=2}^{m} d_k t_{1k}^2)/d_1}, \quad \varepsilon = \pm 1. \tag{11}$$

Тогда для t_{j1} из (8) имеем выражение

$$t_{j1} = \frac{a_{1j} - \sum_{k=2}^{m} d_k t_{1k} t_{jk}}{\varepsilon \sqrt{d_1 (a_{11} - \sum_{k=2}^{m} d_k t_{1k}^2)}}, \quad j = 2, 3, \ldots, m. \tag{12}$$

а систему (10) представим в таком виде:

$$(a_{1j} - \sum_{k=2}^{m} d_k t_{1k} t_{jk})^2 + (a_{11} - \sum_{k=2}^{m} d_k t_{1k}^2)(\sum_{k=2}^{m} d_k t_{jk}^2 - a_{jj}) = 0, \quad j = 2, 3, \ldots, m. \tag{13}$$

В системе (6) у нас остались уравнения

$$d_1 t_{i1} t_{j1} + \sum_{k=2}^{m} d_k t_{ik} t_{jk} = a_{ij}, \quad 2 \le i < j \le m.$$

Воспользовавшись равенством (12), представим эту систему в виде

$$(a_{1i} - \sum_{k=2}^{m} d_k t_{1k} t_{ik})(a_{1j} - \sum_{k=2}^{m} d_k t_{1k} t_{jk}) + (a_{11} - \sum_{k=2}^{m} d_k t_{1k}^2)(\sum_{k=2}^{m} d_k t_{ik} t_{jk} - a_{ij}) = 0,$$

$$2 \le i < j \le m. \tag{14}$$

Рассмотрим, наконец, уравнение (7). Разложим определитель матрицы T по первому столбцу:

$$\sum_{j=1}^{m} t_{j1}T_{j1} = 1,$$

где T_{j1} — алгебраическое дополнение элемента t_{j1}. Воспользовавшись равенствами (11)–(12), перепишем последнее равенство в таком виде

$$(a_{11} - \sum_{k=2}^{m} d_k t_{1k}^2) + \sum_{j=2}^{m}(a_{1j} - \sum_{k=2}^{m} d_k t_{1k}t_{jk})T_{j1} = \varepsilon\sqrt{d_1(a_{11} - \sum_{k=2}^{m} d_k t_{1k}^2)}. \tag{15}$$

Следовательно, из системы (5)–(7) мы исключили переменные t_{j1}, $j = 1, \ldots, m$. При этом остались уравнения (13)–(17) Предложение доказано.

Заметим, что системы, входящие в теорему и предложение можно упростить, если воспользоваться следующим утверждением

Предложение 6. *Всякая целая форма $\psi(x)$ от $m \geq 3$ переменных $x = (x_1, x_2, \ldots, x_m)$ эквивалентна форме имеющей трехдиагональную матрицу.*

Доказательство проведем индукцией по m. Пусть $\psi(x) = xAx^t$, где $A \in \mathbf{M}_m(\mathbf{Z})$. Так как всякая форма $\varphi(y)$ эквивалентная форме $\psi(x)$ имеет вид $\varphi(y) = yTAT^ty^t$, то достаточно показать, что можно так подобрать матрицу $T \in \mathbf{GL}_m(\mathbf{Z})$, что матрица TAT^t является трехдиагональной.

Определим семейство отображений

$$f_{ij}^{\lambda} : \mathbf{M}_m(\mathbf{Z}) \longrightarrow \mathbf{M}_m(\mathbf{Z}), \quad 1 \leq i, j \leq m, \quad i \neq j, \quad \lambda \in \mathbf{Z},$$

действующих по правилу: $f_{ij}^{\lambda}(C) = e_{ij}(\lambda)Ce_{ji}(\lambda)$, $C \in \mathbf{M}_m(\mathbf{Z})$, где $e_{ij}(\lambda)$ — элементарная трансвекция, т. е. матрица у которой на месте (i, j) стоит λ, на главной диагонали 1, а на остальных местах — нули. Ограничивая отображение f_{ij}^{λ} на множество симметрических матриц, можем рассматривать его как отображение, определенное на множестве квадратичных форм и переводящее всякую форму в эквивалентную. Заметим далее, что матрица $e_{ij}(\lambda)C$ получается из матрицы C умножением j–й строки на λ и прибавлением к i–й строке. Матрица $e_{ij}(\lambda)Ce_{ji}(\lambda)$ получается из матрицы $e_{ij}(\lambda)C$ умножением j–го столбца на λ и прибавлением к i–му столбцу. Таким образом, отображение f_{ij}^{λ} меняет только i–ю строку и j–й столбец матрицы C. Кроме того, очевидно, матрица $f_{ij}^{\lambda}(C)$ является симметрической, если таковой была матрица C. Применяя алгоритм Евклида к элементам $a_{1,m-1}$, $a_{1,m}$ матрицы A, подберем целые числа $\alpha_1, \alpha_2, \ldots, \alpha_p$ такие, что в матрице $A_1 = f_{m,m-1}^{\alpha_p} f_{m-1,m}^{\alpha_{p-1}} \ldots f_{m,m-1}^{\alpha_1}(A)$ на месте $(1, m)$, а значит и на месте $(m, 1)$ стоят нули. Если $m = 3$, то предложение доказано и квадратичная форма с матрицей A_1 эквивалентна форме φ и имеет требуемый вид. Если $m > 3$, то рассмотрим элементы матрицы A_1 стоящие на местах $(1, m-2)$ и $(1, m-1)$. Применяя к ним алгоритм Евклида, подберем целые числа $\beta_1, \beta_2, \ldots, \beta_q$ так, что в матрице $A_2 = f_{m-1,m-2}^{\beta_1} f_{m-2,m-1}^{\beta_2} \ldots f_{m-1,m-2}^{\beta_q}(A_1)$ на местах $(1, m-1)$ и $(1, m)$ стоят нули. Продолжая в том же духе, на $m-2$–м шаге получим матрицу A_{m-2}

у которой в первой строке и в первом столбце отличными от нуля могут быть только первые два элемента. Таким образом, у матрицы A_{m-2} первые строка и столбец имеют требуемый вид. Воспользовавшись предположением индукции, получим требуемое утверждение.

В следующем параграфе мы применим полученные результаты к решетке $S(a)$.

§ 3. Ортогональный базис решетки $S(a)$

В этом параграфе для фиксированного вектора a из $\mathbf{Q}^n$ рассматривается решетка

$$S(a) = \{ka + b \mid k \in \mathbf{Z}, b \in \mathbf{Z}^n\}$$

в евклидовом пространстве $\mathbf{R}^n$. Очевидно, она порождается векторами $a, e_1, e_2, \ldots, e_n$. Не уменьшая общности, можно считать, что все компоненты вектора a отличны от нуля. Действительно, если i–я компонента равна нулю, то положим $a' = a + e_i$. Очевидно, решетка $S(a')$ совпадает с решеткой $S(a)$ и в векторе a' i–я компонента равна 1. Следовательно, мы можем считать, что вектор a имеет вид

$$a = \left(\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}\right), \quad p_i \in \mathbf{Z} \setminus \{0\}, q_i \in \mathbf{N}.$$

Определим по этому вектору совокупность целых чисел $\delta_0, \delta_1, \ldots, \delta_{n-1}$:

$$\delta_0 = 1, \quad \delta_i = \left(\frac{q_1}{\delta_0}, \frac{q_2}{\delta_1}, \ldots, \frac{q_i}{\delta_{i-1}}, q_{i+1}\right), \quad i = 1, \ldots, n-1;$$

совокупность целых чисел $\check{q}_1, \check{q}_2, \ldots, \check{q}_n$:

$$\check{q}_1 = 1, \quad \check{q}_i = \prod_{k=1}^{i-1} \frac{q_k}{\delta_{k-1}}, \quad i = 2, 3, \ldots, n,$$

а также совокупность пар целых чисел (u_i, v_i), удовлетворяющих соотношениям

$$p_i \check{q}_i u_i + q_i v_i = \delta_{i-1}, \quad i = 1, \ldots, n.$$

В этих обозначениях справедлива

Лемма 4. *Следующие векторы из* $\mathbf{Q}^n$ *образуют базис решетки* $S(a)$:

$$
\begin{array}{lccccc}
b_1 = (\dfrac{\delta_0}{q_1}, & \dfrac{p_2}{q_2}\check{q}_1u_1, & \dfrac{p_3}{q_3}\check{q}_1u_1, & \ldots, & \dfrac{p_{n-1}}{q_{n-1}}\check{q}_1u_1, & \dfrac{p_n}{q_n}\check{q}_1u_1), \\
b_2 = (0, & \dfrac{\delta_1}{q_2}, & \dfrac{p_3}{q_3}\check{q}_2u_2, & \ldots, & \dfrac{p_{n-1}}{q_{n-1}}\check{q}_2u_2, & \dfrac{p_n}{q_n}\check{q}_2u_2), \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
b_i = (0, & \ldots, 0, \dfrac{\delta_{i-1}}{q_i}, & \dfrac{p_{i+1}}{q_{i+1}}\check{q}_iu_i, & \ldots, & \dfrac{p_{n-1}}{q_{n-1}}\check{q}_iu_i, & \dfrac{p_n}{q_n}\check{q}_iu_i), \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
b_n = (0, & \ldots & \ldots & \ldots, & 0, & \dfrac{\delta_{n-1}}{q_n}).
\end{array}
$$

Доказательство. Рассмотрим матрицу

$$
A = \begin{pmatrix}
\dfrac{p_1}{q_1} & \dfrac{p_2}{q_2} & \ldots & \dfrac{p_{n-1}}{q_{n-1}} & \dfrac{p_n}{q_n} \\
1 & 0 & \ldots & 0 & 0 \\
0 & 1 & \ldots & 0 & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & \ldots & 0 & 1 \\
0 & 0 & \ldots & 0 & 0
\end{pmatrix},
$$

строки которой порождают решетку $S(a)$. Используя $\mathbf{Z}$–элементарные преобразования строк этой матрицы, приведем ее к ступенчатому виду.

Так как числа p_1 и q_1 взаимно просты, то найдутся целые числа u_1 и v_1 такие, что $p_1u_1 + q_1v_1 = 1$. Умножим первую строку матрицы A на u_1 и прибавим к последней строке, вторую строку умножим на v_1 и также прибавим к последней строке. В полученной матрице умножим последнюю строку на $-p_1$ и прибавим к первой, а затем — умножим последнюю строку на $-q_1$ и прибавим ко второй строке. Получим матрицу

$$
\begin{pmatrix}
0 & \dfrac{p_2}{q_2}q_1v_1 & \dfrac{p_3}{q_3}q_1v_1 & \ldots & \dfrac{p_n}{q_n}q_1v_1 \\
0 & -\dfrac{p_2}{q_2}q_1u_1 & -\dfrac{p_3}{q_3}q_1u_1 & \ldots & -\dfrac{p_n}{q_n}q_1u_1 \\
0 & 1 & 0 & \ldots & 0 \\
\ldots & \ldots & \ldots & \ldots & \ldots \\
0 & 0 & 0 & \ldots & 1 \\
\dfrac{1}{q_1} & \dfrac{p_2}{q_2}u_1 & \dfrac{p_3}{q_3}u_1 & \ldots & \dfrac{p_n}{q_n}u_1
\end{pmatrix}
$$

строки которой порождают решетку $S(a)$. Видим, что последняя строка этой матрицы линейно независима от остальных и совпадает с вектором b_1. Удалим из полученной матрицы первый столбец и последнюю строку и добавив нулевую строку, получим матрицу

$$A_1 = \begin{pmatrix} \frac{p_2}{q_2}q_1v_1 & \frac{p_3}{q_3}q_1v_1 & \dots & \frac{p_n}{q_n}q_1v_1 \\ -\frac{p_2}{q_2}q_1u_1 & -\frac{p_3}{q_3}q_1u_1 & \dots & -\frac{p_n}{q_n}q_1u_1 \\ 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \\ 0 & 0 & \dots & 0 \end{pmatrix}.$$

Умножим первую строку этой матрицы на q_1 и прибавим к последней, вторую строку умножим на $-p_1$ и также прибавим к последней. В полученной матрице умножим последнюю строку на $-v_1$ и прибавим к первой строке, а затем последнюю строку умножим на u_1 и прибавим ко второй строке. В результате получим матрицу у которой первые две строки нулевые, а оставшиеся имеют вид

$$A_2 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \\ \frac{p_2}{q_2}q_1 & \frac{p_3}{q_3}q_1 & \dots & \frac{p_n}{q_n}q_1 \end{pmatrix}.$$

Если обозначить последнюю строку матрицы A_2 символом a_1, то строки этой матрицы порождают решетку $S(a_1)$. Воспользоваться непосредственно индуктивным предположением мы не можем так как дроби $\frac{p_i}{q_i}q_1$ могут быть сократимыми. Поэтому положим δ_1=НОД(q_1, q_2). Тогда найдутся целые числа u_2 и v_2 такие, что $p_2q_1u_2 + q_2v_2 = \delta_1$. Далее, для построения базиса решетки $S(a_1)$ проводим те же рассуждения, что и для решетки $S(a)$. Затем переходим к подрешетке меньшей размерности и т. д., пока не получим базу решетки $S(a)$. Лемма доказана.

Для чисел, входящих в компоненты вектора a положим

$$q = \prod_{i=1}^{n} q_i, \quad \hat{q}_i = \frac{q}{q_i}, \quad i = 1, \dots, n.$$

Следующая теорема позволяет эффективно проверить: обладает ли решетка $S(a)$ ортогональным базисом

Теорема 2. *Решетка $S(a)$ обладает ортогональным базисом относительно стандартного скалярного произведения пространства $\mathbf{R}^n$ тогда и только тогда, когда найдутся целые числа $d_1, d_2, \dots, d_n$ такие, что $1 \le d_1 \le \dots \le d_n$, $d_1d_2 \dots d_n = (\prod_{i=1}^{n} \hat{q}_i\delta_{i-1})^2$ и для которых система*

$$\sum_{k=1}^{n} d_k y_{ik}^2 = (\hat{q}_i\delta_{i-1})^2 + (\check{q}_iu_i)^2 \sum_{l=i+1}^{n} (\hat{q}_lp_l)^2, \quad i = 1, \dots, n, \tag{1}$$

$$\sum_{k=1}^{n} d_k y_{ik} y_{jk} = \check{q}_i u_i \left(\hat{q}_j^2 p_j \delta_{j-1} + \check{q}_j u_j \sum_{l=j+1}^{n} (\hat{q}_l p_l)^2 \right), \quad 1 \le i < j \le n, \tag{2}$$

$$\det(y_{ij}) = 1 \tag{3}$$

имеет целочисленные решения относительно переменных y_{ij}, $i, j = 1, \ldots, n$.

Доказательство. Ввиду леммы 4 решетка $S(a)$ порождается векторами b_1, b_2, …, b_n. Рассмотрим векторы $f_1 = qb_1, f_2 = qb_2, \ldots, f_n = qb_n$, Очевидно, решетка $R(a) = \mathcal{L}_{\mathbf{Z}}(f_1, f_2, \ldots, f_n)$ порожденная векторами $f_1, f_2, \ldots, f_n$ является целочисленной и ввиду леммы 3 обладает ортогональным базисом тогда и только тогда, когда ортогональным базисом обладает решетка $S(a)$. Обозначим символом F матрицу, строками которой являются векторы $f_1, f_2, \ldots, f_n$. Тогда матрицей Грама решетки $R(a)$ будет матрица $G = (g_{ij}) = FF^t$ с элементами

$$g_{ij} = \begin{cases} (\hat{q}_i \delta_{i-1})^2 + (\check{q}_i u_i)^2 \sum_{l=i+1}^{n} (\hat{q}_l p_l)^2, & \text{если } i = j, \\ \check{q}_i u_i \left(\hat{q}_j^2 p_j \delta_{j-1} + \check{q}_j u_j \sum_{l=j+1}^{n} (\hat{q}_l p_l)^2 \right), & \text{если } i < j, \\ g_{ji}, & \text{если } j < i. \end{cases}$$

Очевидно, определитель матрицы G равен $(\prod_{i=1}^{n} \hat{q}_i \delta_{i-1})^2$. Сопоставим решетке $R(a)$ положительно определенную квадратичную форму $\psi(x) = xGx^t$, $x = (x_1, x_2, \ldots, x_n)$. Теперь для завершения доказательства остается воспользоваться теоремой 1.

Отметим, что эта теорема позволяет для всякого вектора $a \in \mathbf{Q}^n$ эффективно проверить: обладает ли решетка $S(a)$ ортогональным базисом, а если ответ утвердительный, то — построить такой базис. Действительно, существует лишь конечное число целочисленных матриц вида $\mathrm{diag}(d_1, d_2, \ldots, d_n)$ таких, что $1 \le d_1 \le \ldots \le d_n$, $d_1 d_2 \ldots d_n = (\prod_{i=1}^{n} \hat{q}_i \delta_{i-1})^2$. Для каждой такой матрицы существует лишь конечное число целочисленных матриц $Y = (y_{ij})$, удовлетворяющих подсистеме (1). Если среди них найдется такая, которая удовлетворяет системе (2)–(3), то решетка $S(a)$ обладает ортогональным баисом. Таким образом, перебрав все возможные варианты, либо найдем ортогональный базис решетки $S(a)$, либо докажем, что такого базиса не существует.

ЛИТЕРАТУРА

1. Касселс Дж. Введение в геометрию чисел. М.: Мир, 1965.
2. Боревич З. И., Шафаревич И. Р. Теория чисел. М.: Наука, 1972.
3. Фаддеев Д. К. Об обобщенных целочисленных представлениях над дедекиндовыми кольцами. Зап. научн. семин. ПОМИ, 227, 1995, 113–118.
4. Касселс Дж. Рациональные квадратичные формы. М.: Мир, 1982.

5. Протасов И. В. Циклические измерения и решетки. Математика сегодня. Научно методический сборник. 26–39. Киев.: Вища школа, 1992.

6. Бардаков В. Г. Об ортогональных базисах рациональных решеток. Сиб. матем. жур., 39, №6 (1998), 1236–1250.

7. Делоне Б., Падуров Н., Александров. Математические основы структурного анализа кристаллов, ОНТИ, ГТТИ, 1934.

8. Коуровская тетрадь: Нерешённые вопросы теории групп. 14–е изд. Новосибирск, ИМ СО РАН, 1999.

9. Конвей Дж., Слоэн Н. Упаковки шаров, решётки и группы. М.: Мир, 1990.

10. Делоне Б. Н., Геометрия положительных квадратичных форм, Успехи мат. наук, 3, (1937) 16–62; 4, (1938) 102–164.

РОССИЯ,

Бардаков Валерий Георгиевич,

630090, г. Новосибирск, 90,

пр. Ак. Коптюга, д. 4,

ИМ СО РАН,

E–mail: bardakov@math.nsc.ru.