Math-Net.Ru

Общероссийский математический портал

С. А. Кулешов, Изометрии полуортогональной формы на $\mathbb{Z}$ -модуле ранга 3, *Изв. РАН. Сер. матем.*, 2013, том 77, выпуск 1, 49–90

DOI: <https://doi.org/10.4213/im7940>

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: 35.173.137.237

26 апреля 2023 г., 12:33:25

УДК 511.515+512.64

С. А. Кулешов

Изометрии полуортогональной формы на $\mathbb{Z}$ -модуле ранга 3

Исследуются группы изометрий полуортогональных форм на $\mathbb{Z}$ -модуле ранга 3, т. е. таких форм, матрица Грама которых в некотором базисе имеет верхнетреугольный вид с единицами на диагонали. Дискретным параметром таких форм служит высота – след дуализирующего оператора $+3$. Доказано, что группа таких изометрий представляет собой $\mathbb{Z}$ или $\mathbb{Z}_2 \times \mathbb{Z}$, причем перечислены все случаи, когда имеет место прямое произведение, и описана образующая второго порядка. Образующая группы изометрий бесконечного порядка описана для большого числа частных случаев высоты.

Библиография: 8 наименований.

Ключевые слова: квадратичные формы на модулях над кольцами.

DOI: 10.4213/im7940

§ 1. Введение

Одним из объектов, использующихся при описании многообразия модулей векторных расслоений на многообразиях Фано, являются так называемые исключительные векторные расслоения [1]–[5]. С одной стороны, многообразие модулей таких расслоений нульмерно, а с другой – из исключительных расслоений можно формировать базисы производных категорий когерентных пучков. На таких базисах возникает действие группы кос, и один из интереснейших вопросов – это вопрос о числе орбит такого действия, ответить на который с точки зрения геометрии оказывается довольно сложно. Полный ответ на него дан в случаях плоскости $\mathbb{P}^2$ [4] и поверхностей Дель Пеццо [3].

Однако вопрос о числе орбит действия группы кос можно исследовать и с точки зрения линейной алгебры над кольцом целых чисел. На группе K_0 от алгебраического многообразия X , которую можно рассматривать как $\mathbb{Z}$ -модуль, возникает естественная билинейная форма

$$\chi(E, F) = \sum_i \dim \operatorname{Ext}^i(E, F),$$

где E и F – пучки на X . При этом если $E_1, \dots, E_n$ – базис производной категории, составленный из исключительных расслоений, то матрица Грама формы χ будет верхнетреугольной с единицами на главной диагонали. Будем называть такие базисы *полуортонормированными*. Группа кос действует и на полуортонормированных базисах, и вопрос о числе орбит этого действия очень важен. В работе [6] доказывается транзитивность такого действия в случаях $\mathbb{P}^3$ и рациональных линейчатых поверхностей.

Работа выполнена при поддержке Лаборатории алгебраической геометрии ГУ-ВШЭ (грант Правительства РФ, договор 11.G34.31.0023).

В связи с этим можно сформулировать общую задачу.

Рассмотрим свободный $\mathbb{Z}$ -модуль V конечного ранга, на котором задана целозначная билинейная форма $\chi: V \times V \rightarrow \mathbb{Z}$.

Будем называть форму χ *полуортогональной*, если существует такой базис $\varepsilon = (e_1, \dots, e_n)$ в V , что матрица Грама формы χ в этом базисе имеет верхнетреугольный вид с единицами на диагонали:

$$G = \begin{pmatrix} 1 & g_{12} & \dots & g_{1,n-1} & g_{1n} \\ 0 & 1 & \dots & g_{2,n-1} & g_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}, \quad \text{или} \quad \chi(e_i, e_j) = \begin{cases} 0 & \text{при } i > j, \\ 1 & \text{при } i = j. \end{cases}$$

ПРЕДЛОЖЕНИЕ 1.1. Если $\varepsilon = (e_1, \dots, e_n)$ – полуортонормированный базис, то можно построить базисы $\mathcal{R}_i \varepsilon$ и $\mathcal{L}_i \varepsilon$, $1 \leq i < n$, по правилу

$$\begin{aligned} \mathcal{R}_i(\dots, e_i, e_{i+1}, \dots) &= (\dots, e_{i+1}, e'_i, \dots), \\ \mathcal{L}_i(\dots, e_i, e_{i+1}, \dots) &= (\dots, e'_i, e_{i+1}, \dots), \end{aligned}$$

где $e'_i = \chi(e_i, e_{i+1})e_{i+1} - e_i$, $e'_{i+1} = \chi(e_i, e_{i+1})e_i - e_{i+1}$. Тогда:

- 1) базисы $\mathcal{R}_i \varepsilon$ и $\mathcal{L}_i \varepsilon$ полуортонормированы;
- 2) перестройки $\mathcal{R}_1, \mathcal{R}_2, \dots, \mathcal{R}_{n-1}$ задают действие группы кос на полуортонормированных базисах и матрицах Грама формы χ .

Например, если матрица Грама формы имеет вид¹

$$G = M(a, b, c) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad (1.1)$$

то

$$\mathcal{R}_1 G = \begin{pmatrix} 1 & a & c \\ 0 & 1 & ac - b \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{R}_2 G = \begin{pmatrix} 1 & b & bc - a \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad (1.2)$$

$$\mathcal{L}_1 G = \begin{pmatrix} 1 & a & ab - c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix}, \quad \mathcal{L}_2 G = \begin{pmatrix} 1 & ac - b & a \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}. \quad (1.3)$$

В связи с действием группы кос можно сформулировать три основных вопроса.

1. (Орбиты на базисах.) Пусть даны полуортогональная целозначная форма χ и полуортонормированный относительно нее базис ε^0 . Можно ли перейти от другого полуортонормированного базиса ε той же ориентации² к ε^0 действием группы кос? (Сколько орбит существует на множестве всех ориентированных базисах $\text{Bases}(\chi)$?)

2. (Орбиты на матрицах.) Пусть G – матрица Грама целозначной формы в полуортонормированном базисе ε^0 и $\tilde{G}$ – матрица той же формы в другом полуортонормированном базисе. Можно ли, используя действие группы кос,

¹Обозначение $M(a, b, c)$ для матриц такого вида будет постоянно использоваться в настоящей работе.

²Базисы имеют одинаковую ориентацию, если определитель соответствующей матрицы перехода положителен.

перейти к базису ε , в котором матрица формы будет равна $\tilde{G}$? (Сколько орбит существует на множестве матриц Грама $\text{Matr}(\chi)$?)

3. Пусть в полуортонормированных базисах ε_1 и ε_2 одинаковой ориентации форма имеет одну и ту же матрицу G . Можно ли утверждать, что базисы ε_1 и ε_2 лежат в одной орбите действия группы кос?

ЗАМЕЧАНИЕ 1.2. При положительном ответе на третий вопрос первые два становятся равносильными.

Вопросы 1–3 связаны следующим образом. Пусть $\text{Isom}(\chi)$ – группа изометрий формы χ , а B_2 – соответствующая группа кос. Обе эти группы действуют на множестве всех полуортогональных базисов $\text{Bases}(\chi)$, поэтому можно рассмотреть их пересечение в группе перестановок множества $\text{Bases}(\chi)$. Очевидно, что $\text{Bases}(\chi)$ является главным $\text{Isom}(\chi)$ -расслоением над $\text{Matr}(\chi)$, причем отображение

$$\text{Bases}(\chi) \longrightarrow \text{Matr}(\chi)$$

эквивариантно относительно действия группы кос, поэтому возникает отображение множеств орбит

$$\text{Bases}(\chi)/B_2 \longrightarrow \text{Matr}(\chi)/B_2.$$

Ответ на вопрос 1 в случае $\mathbb{Z}$ -модуля ранга 3 дан в работе [7]. Далее сформулируем основные результаты последней работы.

ОПРЕДЕЛЕНИЕ 1.3. По билинейной несимметричной форме χ однозначно определен *дуализирующий оператор* $\varkappa$, удовлетворяющий соотношению $\chi(u, v) = \chi(v, \varkappa u)$ для всех векторов u и v .

ЗАМЕЧАНИЕ 1.4. Матрица K дуализирующего оператора $\varkappa$ вычисляется по формуле $K = G^{-1}G^t$, где G – матрица Грама формы χ , причем если $G = M(a, b, c)$, то

$$K = \begin{pmatrix} 1 + c^2 - m & b'c - a & b' \\ a - cb & 1 - c^2 & -c \\ b & c & 1 \end{pmatrix}, \quad b' = ac - b. \quad (1.4)$$

Очевидно, что коэффициенты характеристического многочлена дуализирующего оператора являются инвариантами полуортогональной формы.

ЛЕММА 1.5. *Характеристический многочлен дуализирующего оператора $\varkappa$ формы χ на $\mathbb{Z}$ -модуле ранга 3 с матрицей Грама $G = M(a, b, c)$ в полуортонормированном базисе имеет вид*

$$P_{K_\chi}(\lambda) = -\lambda^3 - \lambda^2(a^2 + b^2 + c^2 - abc - 3) + \lambda(a^2 + b^2 + c^2 - abc - 3) + 1.$$

ОПРЕДЕЛЕНИЕ 1.6. Инвариант $a^2 + b^2 + c^2 - abc = m$ полуортогональной формы χ , т. е. след дуализирующего оператора + 3, будем называть ее *высотой*.

ЗАМЕЧАНИЕ 1.7. Если существует целозначная полуортогональная форма высоты m , то:

- 1) $m \not\equiv -1 \pmod{4}$;
- 2) если $m \equiv 0 \pmod{3}$, то $m \equiv 0 \pmod{9}$.

Матрица Грама полуортогональной формы в полуортонормированном базисе $\mathbb{Z}$ -модуля ранга 3 определяется упорядоченной тройкой целых чисел (a, b, c) . Поэтому перестройки (1.2), (1.3) матриц удобно изображать схематически:

$$\begin{array}{ccc}
 (a, c', b) & & (b, a', c) \\
 & \swarrow L_1 \quad \searrow R_2 & \\
 & (a, b, c) & \\
 & \swarrow L_2 \quad \searrow R_1 & \\
 (b', a, c) & & (a, c, b')
 \end{array} \tag{1.5}$$

где $a' = bc - a$, $b' = ac - b$, $c' = ab - c$.

Заметим, что перестройки (1.5) являются в точности перестройками решений диофантова уравнения

$$a^2 + b^2 + c^2 - abc = m. \tag{1.6}$$

Поэтому орбиты действия группы кос на матрицах Грама взаимно однозначно соответствуют орбитам действия той же группы на множестве решений уравнения (1.6).

При исследовании орбит действия группы кос на множестве решений уравнения (1.6) активно использовалось следующее наблюдение, принадлежащее Маркову.

ЗАМЕЧАНИЕ 1.8. Рассмотрим диофантово уравнение относительно x_i

$$\sum_{i=1}^n x_i^2 - a \prod_{i=1}^n x_i - m = 0.$$

На множестве его решений действуют перестройки $\mathcal{R}_i$ и $\mathcal{L}_n$, которые определяются по правилам

$$\begin{aligned}
 \mathcal{R}_i(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n) &= (x_1, \dots, x_{i-1}, x_{i+1}, x'_i, \dots, x_n), \\
 \mathcal{L}_n(x_1, \dots, x_n) &= (x_1, \dots, x'_n, x_{n-1}),
 \end{aligned}$$

где

$$x'_i = \frac{a \prod_{j=1}^n x_j - x_i^2}{x_i}.$$

Здесь x_i и x'_i — корни многочлена $f_i(t) = t^2 + \sum_{j=1}^n x_j^2 - x_i^2 - at(\prod_{j=1}^n x_j)/x_i - m$.

Данные перестройки определяют действие группы кос B_{n-1} на множестве решений уравнения. Для подсчета числа орбит действия удобно поступать следующим образом. Предположим, что для какого-то решения $(x_1, \dots, x_n)$ выполнено неравенство $x_1 \geq x_2 > 0$, и рассмотрим многочлен $f_1(t)$, корнями которого являются x_1 и x'_1 . Если $f_1(x_2) < 0$, то $x'_1 < x_2$. Этот прием позволяет выбрать перестройку, уменьшающую общий вес решения $\sum x_i$, и обеспечить тем самым описание некоторой «фундаментальной» области в множестве всех решений. Поэтому подсчет числа орбит сводится к поиску решений в фундаментальной области. Заметим также, что если в фундаментальной области нет решений, то можно утверждать, что данное уравнение вообще не имеет решений.

Основным результатом работы [7] является следующая теорема.

ТЕОРЕМА 1.9. *Число орбит действия группы кос на матрицах Грама высоты m конечно при $m \neq 4$, а при $m = 4$ – бесконечно.*

Кроме того, по результатам работы [7] можно сформулировать еще одну теорему, которая нам потребуется в дальнейшем.

ТЕОРЕМА 1.10. *Для полуортогональной формы $\chi^{(m)}$ высоты m на $\mathbb{Z}$ -модуле ранга 3 найдется такой базис, в котором матрица Грама формы равна $M(a, b, c)$, причем:*

- 1) если $m \geq 0$, $m \neq 4$, то выполнено одно из условий:
 - a) $\min(|a|, |b|, |c|) \leq 1$;
 - b) $\text{sign } a \cdot \text{sign } b \cdot \text{sign } c = -1$;
 - c) $|a| = |b| = |c| = 3$ (при $m = 0$);
- 2) если $m = 4$, то $a = c$, $b = 2$;
- 3) если $m < 0$, то $c^2(|c| - 3) \leq |m|$ и $(|c| - 2)|b|^2 \leq |m - c^2|$.

Настоящая работа посвящена исследованию вопроса 3, а именно вопросу об изометриях полуортогональной формы на $\mathbb{Z}$ -модуле ранга 3.

§ 2. Метод исследования и основной результат

Прежде всего заметим, что бывают собственные изометрии (с положительным определителем) $\mathbb{Z}$ -модуля V , на котором задана форма χ , и несобственные (с отрицательным). Поскольку любая несобственная изометрия получается как композиция собственной и $-\text{Id}_V$, то достаточно исследовать группу собственных изометрий полуортогональной формы χ , которую будем обозначать через $\text{Isom}^+(\chi)$.

Основная идея исследования группы $\text{Isom}^+(\chi)$ основана на следующем замечании.

ЗАМЕЧАНИЕ 2.1. Дуализирующий оператор $\varkappa$ является изометрией формы χ , и произвольная изометрия A коммутирует с $\varkappa$.

Согласно замечанию 2.1 для описания группы $\text{Isom}^+(\chi)$ достаточно привести $\varkappa$ к жордановой нормальной форме, найти все матрицы, которые с ней коммутируют, и выбрать из них матрицы изометрий.

Отметим, что дуализирующий оператор принадлежит группе кос B_2 , поскольку $\varkappa = (\mathcal{R}_1 \mathcal{R}_2)^{-3}$.

ЗАМЕЧАНИЕ 2.2. Если $m \notin \{0, 4\}$, то дуализирующий оператор $\varkappa$ диагонализуется над полем $\mathbb{Q}[\sqrt{m^2 - 4m}]$ с собственными числами

$$1, \quad \lambda = 1 - \frac{m}{2} + \frac{1}{2}\sqrt{m^2 - 4m}, \quad \lambda^{-1} = 1 - \frac{m}{2} - \frac{1}{2}\sqrt{m^2 - 4m},$$

причем $\sqrt{m^2 - 4m} \in \mathbb{R} \setminus \mathbb{Q}$ при $m \neq 1, 2$ и $\sqrt{m^2 - 4m} \in \mathbb{C}$ при $m = 1, 2$.

В случаях $m = 0$ и $m = 4$ жорданова нормальная форма $\varkappa$ равна соответственно

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}.$$

В связи с замечанием 2.2 можно сформулировать план исследований. Сначала будет описана группа изометрий $\text{Isom}^+(\chi^{(0)})$ формы высоты 0, т. е. формы Маркова (§ 3), затем группа $\text{Isom}^+(\chi^{(4)})$ (§ 4). После этого мы опишем группу изометрий полуортогональных форм ($m \neq 0, 4$) над полем $\mathbb{Q}$ (§ 5). Группы $\text{Isom}^+(\chi^{(1)})$ и $\text{Isom}^+(\chi^{(2)})$ описываются в § 7. Остальные параграфы посвящены рассмотрению общего случая.

Основной результат настоящей работы заключается в следующем.

ТЕОРЕМА 2.3. Пусть $\chi^{(m)}$ – полуортогональная форма высоты m на $\mathbb{Z}$ -модуле ранга 3. Если соответствующая высота не приведена в табл. 1 или форма не обладает матрицей Грама, указанной в этой таблице, то группа $\text{Isom}^+(\chi^{(m)})$ порождается дуализирующим оператором $\varkappa$. Особые случаи сведены в табл. 1, где $\mathcal{I}^2 = \text{Id}$, а порядок $\mathcal{A}$ бесконечен, причем образующая $\mathcal{A}$ принадлежит группе кос всегда, кроме случая матрицы Грама $M(n, 0, 0)$, когда $\mathcal{A}$ не лежит в группе кос, и случая матрицы Грама $M(2b+1, 2, 2b+1)$, $b \neq 0$, когда ответ на этот вопрос нам не известен. Не известно также, лежит ли $\mathcal{I}$ в группе кос.

ТАБЛИЦА 1

Высота формы m	Матрица Грама	Образующие группы $\text{Isom}^+(\chi^{(m)})$	Ссылка
$-(n-2)(n+1)^2, n > 5$	$M(n+1, n+1, n+1)$	$\mathcal{A}: \mathcal{A}^3 = \varkappa$	предл. 9.1
$4w^2(2-w^2), w > 2$	$M(2w^2, 2w, 2w)$	$\mathcal{A}: \mathcal{A}^2 = \varkappa$	предл. 10.1
–50	$M(5, 5, 5)$	$\mathcal{I}, \mathcal{A}: \mathcal{A}^3 = \varkappa$	предл. 6.1, 9.1
–16	$M(4, 4, 4)$		
–32	$M(8, 4, 4)$	$\mathcal{I}, \mathcal{A}: \mathcal{A}^2 = \varkappa$	предл. 6.1, 10.1
–2	$M(3, 4, 3)$	$\mathcal{I}, \varkappa$	предл. 6.1
0	$M(3, 3, 3)$	$\mathcal{A}: \mathcal{A}^3 = \varkappa$	предл. 3.1
4	$M(2, 2, 2)$ $M(-2b, 2, -2b), b \neq 1$ $M(-2b-1, 2, -2b-1)$	$\mathcal{R}_1, \mathcal{R}_2$ из (1.2) $\mathcal{I}, \mathcal{A}: \mathcal{I}\mathcal{A}^{2-2b^2} = \varkappa$ $\mathcal{A}: \mathcal{A}^{3-4b^2-4b} = \varkappa$	предл. 4.3 предл. 4.1 предл. 4.1
1	$M(1, 1, 0)$	$\varkappa, \mathcal{A}^4 = \text{Id}$	предл. 7.1
2	$M(1, 0, 0)$	$\varkappa, \mathcal{A}^6 = \text{Id}$	предл. 7.1
$n^2, n \geq 2$	$M(n, 0, 0)$	$\mathcal{I}, \mathcal{A}: \mathcal{A}^2 = \varkappa$	предл. 6.1, 10.21
$2n^2, n \geq 2$	$M(n, n, 0)$	$\mathcal{I}, \varkappa$	предл. 6.1, 7.1
$(n-1)^2(n+2), n \geq 3$	$M(1-n, 1-n, 1-n)$	$\mathcal{A}: \mathcal{A}^3 = \varkappa$	предл. 9.3

В качестве следствия теоремы 2.3 получаем уточнение и дополнение к теореме 1.9.

ТЕОРЕМА 2.4. Число орбит действия группы кос как на матрицах Грама, так и на полуортогональных базисах фиксированной полуортогональной формы на $\mathbb{Z}$ -модуле ранга 3 конечно.

§ 3. Форма высоты 0

Рассмотрим форму Маркова $\chi^{(0)}$, матрица Грама которой в некотором полуортонормированном базисе $\varepsilon = (e_1, e_2, e_3)$ имеет вид $G = M(3, 3, 3)$. Матрицы K дуализирующего оператора этой формы в базисе ε и K_1 в жордановом

базисе $\iota = (v_1, v_2, v_3)$ имеют следующий вид:

$$K = \begin{pmatrix} 10 & 15 & 6 \\ -6 & -8 & -3 \\ 3 & 3 & 1 \end{pmatrix}, \quad K_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Матрица перехода от базиса ε к жорданову есть

$$C = \begin{pmatrix} 9 & 3 & -1 \\ -9 & 0 & 0 \\ 9 & -3 & 2 \end{pmatrix}.$$

В частности, вектор $u = \frac{1}{9}v_1$ является собственным вектором дуализирующего оператора.

Пусть $\mathcal{A}$ – изометрия формы $\chi^{(0)}$. Ввиду замечания 2.1 можно утверждать, что $\mathcal{A}$ коммутирует с дуализирующим оператором $\varkappa$. Следовательно, вектор u является собственным и для изометрии $\mathcal{A}$. Обозначим через ν собственное число этого вектора. Поскольку вектор u дополняется до базиса $\mathbb{Z}$ -модуля векторами e_2, e_3 , то $\nu \in \mathbb{Z}$. Более того, по этой же причине можно утверждать, что $\nu = \pm 1$. Поскольку $-\text{Id}$ является изометрией, то без ограничения общности можно предполагать, что $\nu = 1$.

Из коммутирования операторов $\mathcal{A}$ и $\varkappa$ и равенства $\nu = 1$ следует вид матрицы A_1 изометрии $\mathcal{A}$ в базисе ι :

$$A_1 = \begin{pmatrix} 1 & x_2 & x_3 \\ 0 & 1 & x_2 \\ 0 & 0 & 1 \end{pmatrix}.$$

Матрица Грама формы Маркова в базисе ι имеет вид

$$G_1 = \begin{pmatrix} 0 & 0 & 9 \\ 0 & -9 & 9 \\ 9 & 0 & -1 \end{pmatrix}.$$

Поэтому условие $A_1^t G_1 A_1 = G_1$ приводит к соотношению

$$2x_3 - x_2^2 + x_2 = 0 \iff x_3 = \frac{1}{2}x_2(x_2 - 1).$$

Итак, если $\mathcal{A}$ – изометрия формы Маркова, то ее матрицей в базисе ι является

$$A_1(a) = \begin{pmatrix} 1 & a & \frac{1}{2}a(a-1) \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}, \quad a \in \mathbb{Q}.$$

Заметим, что все такие матрицы образуют группу: $A(a)A(b) = A(a+b)$ и $A^3(1/3) = K_1$.

Поскольку изометрия $\mathcal{A}$ – изоморфизм $\mathbb{Z}$ -модуля, все элементы ее матрицы F в базисе ε должны быть целыми, т. е.

$$CA_1(a)C^{-1} = F(a) \in \text{GL}_3(\mathbb{Z}).$$

Вычислим матрицу

$$F(a) = \begin{pmatrix} 1 + \frac{9}{2}a(a+1) & 3a(3a+2) & \frac{3}{2}a(3a+1) \\ -\frac{3}{2}a(3a+1) & 1 - 9a^2 & \frac{3}{2}a(1-a) \\ \frac{3}{2}a(3a-1) & 3a(3a-2) & 1 + \frac{9}{2}a(a-1) \end{pmatrix}.$$

Так как $9a^2 \in \mathbb{Z}$, имеем $a \in \frac{1}{3}\mathbb{Z}$.

Таким образом, приходим к следующему предложению³.

ПРЕДЛОЖЕНИЕ 3.1. *Группа собственных изометрий формы Маркова, т. е. полуортогональной формы высоты 0, порождена изометрией⁴ $\mathcal{A}(1/3)$, матрица которой в базисе ε имеет вид*

$$F(1/3) = \begin{pmatrix} 3 & 3 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}.$$

При этом $\mathcal{A}^3(1/3) = \varkappa$, где $\varkappa$ – дуализирующий оператор формы.

§ 4. Форма высоты 4

Полуортогональная форма $\chi^{(4)}$ высоты 4 на $\mathbb{Z}$ -модуле V ранга 3 в одном из базисов $\varepsilon = (e_1, e_2, e_3)$ имеет матрицу Грама

$$G_a = \begin{pmatrix} 1 & -a & 2 \\ 0 & 1 & -a \\ 0 & 0 & 1 \end{pmatrix} \quad (4.1)$$

(см. теорему 1.10). Исследуем группу изометрий этой формы.

Зафиксируем форму высоты 4 с матрицей Грама $M(-a, 2, -a)$ в базисе ε , где $a \geq 0$, $a \neq 2$. Матрица дуализирующего оператора $\varkappa$ этой формы в базисе ε есть

$$K = \begin{pmatrix} a^2 - 3 & 3a - a^3 & a^2 - 2 \\ a & 1 - a^2 & a \\ 2 & -a & 1 \end{pmatrix}.$$

Обозначим через C матрицу перехода к жорданову базису ι оператора $\varkappa$:

$$C = \begin{pmatrix} a & 4 - a^2 & a^2 - 4 \\ 2 & 0 & a \\ a & a^2 - 4 & 2 \end{pmatrix}.$$

Тогда

$$K_1 = C^{-1}KC = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}.$$

Если A_1 – матрица собственной изометрии формы $\chi^{(4)}$ в базисе ι , то $A_1 K_1 = K_1 A_1$ (см. замечание 2.1). Следовательно,

$$A_1 = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & \beta \\ 0 & 0 & \mu \end{pmatrix}, \quad \lambda\mu^2 = 1.$$

Матрица формы в базисе ι имеет вид

$$G_1 = \begin{pmatrix} 4 & 0 & 0 \\ 0 & 0 & 2a^2 - 8 \\ 0 & 8 - 2a^2 & 4 - a^2 \end{pmatrix}.$$

³Ранее это предложение другими методами доказано А. Н. Рудаковым.

⁴Здесь $\mathcal{A}(\mu)$ – изометрия, матрица Грама которой в базисе ι равна $A_1(\mu)$.

Тот факт, что изометрия сохраняет форму, дает нам соотношение

$$A_1^t G_1 A_1 = G_1 = \begin{pmatrix} 4\lambda^2 & 0 & 0 \\ 0 & 0 & \mu^2(2a^2 - 8) \\ 0 & \mu^2(8 - 2a^2) & \mu^2(4 - a^2) \end{pmatrix},$$

откуда $\lambda^2 = \mu^2 = 1$. Учитывая изометрию $-\text{Id}$, можно считать, что $\lambda = 1$.

Таким образом, группа собственных изометрий над полем рациональных чисел порождается инволюцией $\mathcal{I}$ с матрицей

$$I_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}$$

и преобразованиями $\mathcal{A}^\pm(\beta)$ с матрицами

$$A_1^+(\beta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & \beta \\ 0 & 0 & 1 \end{pmatrix}, \quad A_1^-(\beta) = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & \beta \\ 0 & 0 & -1 \end{pmatrix}, \quad \beta \in \mathbb{Q},$$

в базисе ι .

Матрицы $F^\pm(\beta)$ изометрий $\mathcal{A}^\pm(\beta)$ и матрица I инволюции в базисе ε имеют вид

$$F^+(\beta) = \begin{pmatrix} 1 + \frac{1}{2}\beta(a^2 - 4) & \frac{1}{2}(4 - a^2)a\beta & \frac{1}{2}\beta(a^2 - 4) \\ 0 & 1 & 0 \\ \frac{1}{2}\beta(4 - a^2) & \frac{1}{2}\beta a(a^2 - 4) & 1 + \frac{1}{2}\beta(4 - a^2) \end{pmatrix} \in \text{GL}_3(\mathbb{Z}),$$

$$F^-(\beta) = \begin{pmatrix} \frac{a^2}{2} - 1 + \frac{\beta}{2}(a^2 - 4) & a - \frac{a^3}{2} - \frac{\beta a}{2}(a^2 - 4) & \frac{a^2}{2} + \frac{\beta}{2}(a^2 - 4) \\ a & 1 - a^2 & a \\ \frac{a^2}{2} + \frac{\beta}{2}(4 - a^2) & \frac{a}{2}(-a^2 + 2 + \beta(a^2 - 4)) & \frac{1}{2}(a^2 - 2 - \beta(a^2 - 4)) \end{pmatrix},$$

$$I = \begin{pmatrix} \frac{a^2}{2} - 1 & a - \frac{a^3}{2} & \frac{a^2}{2} \\ a & 1 - a^2 & a \\ \frac{a^2}{2} & \frac{a}{2}(2 - a^2) & \frac{a^2 - 2}{2} \end{pmatrix} \in \text{GL}_3(\mathbb{Z}).$$

Следовательно, инволюция входит в группу изометрий над $\mathbb{Z}$ тогда и только тогда, когда a – четное число.

Пусть $a = 2b$. В этом случае $F^+(\beta) \in \text{GL}_3(\mathbb{Z})$ тогда и только тогда, когда

$$\frac{1}{2}\beta(a^2 - 4) \in \mathbb{Z} \iff \beta \in \frac{1}{2b^2 - 2}\mathbb{Z}.$$

Поэтому можно утверждать, что группа собственных изометрий формы $\chi_{2b}^{(4)}$, $b \neq 1$, порождена инволюцией $\mathcal{I}$ и преобразованием $\mathcal{A}^+(1/(2b^2 - 2))$. При этом

$$\varkappa = \mathcal{I}\mathcal{A}^+\left(\frac{1}{2b^2 - 2}\right)^{2-2b^2}.$$

Пусть $a = 2b + 1$. В этой ситуации преобразование $\mathcal{I}$ в группу изометрий формы $\chi_{2b+1}^{(4)}$ не входит. Преобразование $\mathcal{A}^+(\beta)$ является изометрией формы над $\mathbb{Z}$ тогда и только тогда, когда

$$\frac{\beta}{2}(a^2 - 4) \in \mathbb{Z} \iff \beta \in \frac{2}{4b^2 + 4b - 3}\mathbb{Z}.$$

Преобразование $\mathcal{A}^-(\beta)$ является изометрией формы над $\mathbb{Z}$ тогда и только тогда, когда

$$\frac{1}{2} + \frac{\beta}{2}(4b^2 + 4b - 3) \in \mathbb{Z} \iff \beta = \frac{2n - 1}{4b^2 + 4b - 3}, \quad n \in \mathbb{Z}.$$

Поскольку $(\mathcal{A}^-(1/(4b^2 + 4b - 3)))^2 = \mathcal{A}^+(2/(4b^2 + 4b - 3))$, приходим к следующему утверждению.

ПРЕДЛОЖЕНИЕ 4.1. *Группа собственных изометрий полуортогональной формы $\chi_{2b}^{(4)}$ порождена инволюцией $\mathcal{I}$ и преобразованием $\mathcal{A}^+(1/(2b^2 - 2))$, матрицы которых в базисе ε имеют вид*

$$I = \begin{pmatrix} 2b^2 - 1 & 2b - 4b^3 & 2b^2 \\ 2b & 1 - 4b^2 & 2b \\ 2b^2 & 2b - 4b^3 & 2b^2 - 1 \end{pmatrix}, \quad F^+ = \begin{pmatrix} 2 & -2b & 1 \\ 0 & 1 & 0 \\ -1 & 2b & 0 \end{pmatrix}.$$

При этом

$$\varkappa = \mathcal{I}\mathcal{A}^+\left(\frac{1}{2b^2 - 2}\right)^{2-2b^2}.$$

Группа собственных изометрий полуортогональной формы $\chi_{2b+1}^{(4)}$ порождена преобразованием $\mathcal{A}^-(1/(4b^2 + 4b - 3))$ с матрицей в базисе ε , имеющей вид

$$F^- = \begin{pmatrix} 2b^2 + 2b - 1 & 1 - 6b^2 - 4b^3 & 2b^2 + 2b \\ 2b + 1 & -4b^2 - 4b & 2b + 1 \\ 2b^2 + 2b + 1 & -4b^3 - 6b^2 - 2b & 2b^2 + 2b \end{pmatrix}.$$

При этом $\varkappa = (\mathcal{A}^-(1/(4b^2 + 4b - 3)))^{3-4b^2-4b}$.

ПРЕДЛОЖЕНИЕ 4.2. *Изометрия $\mathcal{A}^+(1/(2b^2 - 2))$ с матрицей F^+ формы $\chi_{2b}^{(4)}$ принадлежит группе кос. Изометрия $\mathcal{A}^-(1/(4b^2 + 4b - 3))$ с матрицей F^- точно принадлежит группе кос при $b = 0$. В этом случае она получается как $\mathcal{L}_1\mathcal{L}_2$. В остальных случаях проверить включение $\mathcal{A}^-(1/(4b^2 + 4b - 3)) \in B_2$ сложно.*

ДОКАЗАТЕЛЬСТВО. 1) $a = 2b$. Напомним, что матрица Грама в базисе $\varepsilon = (e_1, e_2, e_3)$ имеет вид

$$G = \begin{pmatrix} 1 & -2b & 2 \\ 0 & 1 & -2b \\ 0 & 0 & 1 \end{pmatrix}.$$

Рассмотрим цепочку перестроек

$$(e_1, e_2, e_3) \xrightarrow{\mathcal{L}_1} (-2be_1 - e_2, e_1, e_3) \xrightarrow{\mathcal{L}_2} (-2be_1 - e_2, 2e_1 - e_3, e_1) \xrightarrow{\mathcal{R}_1} (2e_1 - e_3, e'_2, e_1),$$

где

$$\begin{aligned}
 e'_2 &= \chi_{2b}^{(4)}(-2be_1 - e_2, 2e_1 - e_3)(2e_1 - e_3) - (-2be_1 - e_2) \\
 &= [\chi_{2b}^{(4)}(-2be_1, 2e_1) + \chi_{2b}^{(4)}(-2be_1, -e_3) + \chi_{2b}^{(4)}(-e_2, -e_3)](2e_1 - e_3) \\
 &\quad - (-2be_1 - e_2) \\
 &= [-4b + 4b - 2b](2e_1 - e_3) + 2be_1 + e_2 = -4be_1 + 2be_3 + 2be_1 + e_2 \\
 &= -2be_1 + e_2 + 2be_3.
 \end{aligned}$$

Ясно, что $\mathcal{R}_1\mathcal{L}_2\mathcal{L}_1 = \mathcal{A}^+(1/(2b^2 - 2))$.

2) $a = 1$. В этом случае

$$G = \begin{pmatrix} 1 & -1 & 2 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}, \quad F^- = \begin{pmatrix} -1 & 13 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Требуемые перестройки устроены следующим образом:

$$(e_1, e_2, e_3) \xrightarrow{\mathcal{L}_2} (e_1, -e_3 - e_2, e_2) \xrightarrow{\mathcal{L}_1} (-e_1 + e_3 + e_2, e_1, e_2),$$

что завершает доказательство.

Рассмотрим теперь форму высоты 4 с матрицей Грама $M(2, 2, 2)$. Ее дуализирующий оператор диагонализирuem и в собственном базисе ι имеет матрицу

$$K_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & -1 \end{pmatrix}.$$

Матрица перехода от базиса ε к ι имеет вид

$$C = \begin{pmatrix} 1 & -1 & -1 \\ -1 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix}.$$

Матрицей Грама формы $\chi_2^{(4)}$ в базисе ι является матрица

$$G_1 := \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -1 & 0 \end{pmatrix}.$$

Изометрия $\mathcal{A}$ формы $\chi_2^{(4)}$ должна коммутировать с дуализирующим оператором. Поэтому матрица изометрии в базисе ι имеет вид

$$A_1 = \begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}, \quad \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \pm 1.$$

Однако условие $A_1^t G_1 A_1 = G_1$ дает равенство

$$\det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1.$$

Вычислив матрицу изометрии $\mathcal{A}$ в базисе ε

$$A = \begin{pmatrix} \pm 1 - a - c + b + d & \pm 1 - 2a - 2c + b + d & \pm 1 - a - c \\ a \mp 1 - b & 2a \mp 1 - b & a \mp 1 \\ \pm 1 + c - d & \pm 1 + 2c - d & \pm 1 + c \end{pmatrix},$$

из условия $A \in \mathrm{GL}_3(\mathbb{Z})$ получим, что

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Из формул (1.2), (1.3) следует, что перестройки $\mathcal{R}_1$ и $\mathcal{R}_2$ являются изометриями формы $\chi_2^{(4)}$. Их матрицы в базисе ε имеют вид

$$R_1 = \begin{pmatrix} 0 & -1 & 0 \\ 1 & 2 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad R_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 1 & 2 \end{pmatrix}.$$

В базисе ι матрица преобразования $\mathcal{R}_2$ останется прежней, а матрицей преобразования $\mathcal{R}_1$ будет следующая:

$$R'_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}.$$

Несложно проверить, что матрицы R'_1 и R_2 порождают группу $\mathrm{SL}_2(\mathbb{Z})$. Иными словами, изометрия с матрицей

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & a & b \\ 0 & c & d \end{pmatrix}, \quad \text{где} \quad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

в базисе ι принадлежит группе, порожденной перестройками $\mathcal{R}_1$ и $\mathcal{R}_2$.

ПРЕДЛОЖЕНИЕ 4.3. *Группа собственных изометрий полуортогональной формы $\chi_2^{(4)}$ порождается перестройками $\mathcal{R}_1$ и $\mathcal{R}_2$ из формул (1.2), (1.3).*

СЛЕДСТВИЕ 4.4. *Матрицы G_a (см. (4.1)) и G_b задают одно и ту же квадратичную форму высоты 4 тогда и только тогда, когда $b = \pm a$.*

ДОКАЗАТЕЛЬСТВО следует из того факта, что если $b \neq \pm a$, то группы изометрий форм $\chi_a^{(4)}$ и $\chi_b^{(4)}$ изоморфны друг другу (если a и b отличны от 2), но дуализирующий оператор выражается через образующие этих групп разными способами.

§ 5. Изометрии полуортогональной формы на векторном пространстве размерности 3

Далее будем предполагать, что $m \neq 0$ и $m \neq 4$. Дуализирующий оператор формы в этом случае диагонализуется (замечание 2.2).

ТЕОРЕМА 5.1. *Пусть $V_{\mathbb{Q}}$ – трехмерное векторное пространство над полем рациональных чисел, $\chi^{(m)}$ – квадратичная форма высоты m на $V_{\mathbb{Q}}$ с дуализирующим оператором $\varkappa$, матрица Грама которой в некотором базисе имеет вид*

$$G = M(a, b, c) = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}, \quad a^2 + b^2 + c^2 - abc = m, \quad a, b, c \in \mathbb{Z}.$$

Если $m \notin \{0, 4\}$, то любая изометрия формы $\chi^{(m)}$ имеет вид $\pm \mathcal{A}(\mu)$, где

$$\mu = u + v\sqrt{m^2 - 4m} \in \mathbb{Q}[\sqrt{m^2 - 4m}] \setminus \{0\},$$

причем $u^2 - v^2(m^2 - 4m) = 1$ и $\mathcal{A}(\mu_1)\mathcal{A}(\mu_2) = \mathcal{A}(\mu_1\mu_2)$.

ДОКАЗАТЕЛЬСТВО. Пусть $\varepsilon = (e_1, e_2, e_3)$ – полуортонормированный базис пространства $V_{\mathbb{Q}}$, в котором матрица Грама формы $\chi^{(m)}$ равна $M(a, b, c)$; $\varepsilon' = (e'_1, e'_2, e'_3)$ – собственный базис дуализирующего оператора.

Поскольку дуализирующий оператор сохраняет форму, матрица Грама формы $\chi^{(m)}$ в базисе ε' должна иметь вид

$$\begin{pmatrix} \alpha & 0 & 0 \\ 0 & 0 & \beta \\ 0 & \gamma & 0 \end{pmatrix}, \quad \alpha, \beta, \gamma \in \mathbb{Q}[\sqrt{d}], \quad d = m^2 - 4m. \quad (5.1)$$

Так как изометрия $\mathcal{A}$ коммутирует с $\varkappa$, ее матрица A в базисе ε' будет иметь диагональный вид с элементами из поля $\mathbb{Q}[\sqrt{d}]$. Тот факт, что $\mathcal{A}$ – изометрия, приведет нас к следующему виду ее матрицы в базисе ε' :

$$\pm A(\mu) = \pm \text{Diag}(1, \mu, \mu^{-1}) = \pm \begin{pmatrix} 1 & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \mu^{-1} \end{pmatrix}, \quad \mu \in \mathbb{Q}[\sqrt{d}]. \quad (5.2)$$

Изометрию с матрицей $A(\mu)$ в базисе ε' будем обозначать через $\mathcal{A}(\mu)$. Отсюда, в частности, следует, что $\mathcal{A}(\mu_1)\mathcal{A}(\mu_2) = \mathcal{A}(\mu_1\mu_2)$.

Для доказательства теоремы необходимо проверить, что все элементы матрицы изометрии $\mathcal{A}(\mu)$ в базисе ε в действительности принадлежат полю $\mathbb{Q}$.

Прежде всего заметим, что след (равный $1 + \mu + \mu^{-1}$) преобразования $\mathcal{A}(\mu)$ должен быть рациональным числом. Если $\mu = u + v\sqrt{d}$, то

$$\mu^{-1} = \frac{u}{u^2 - v^2d} - \frac{v\sqrt{d}}{u^2 - v^2d}$$

и из рациональности следа вытекает, что

$$u^2 - v^2d = 1. \quad (5.3)$$

В частности, $\mu^{-1} = \bar{\mu} = u - v\sqrt{d}$.

Учитывая обозначение $d = m^2 - 4m$, перепишем собственные числа оператора $\varkappa$:

$$1, \quad \lambda = 1 - \frac{m}{2} + \frac{1}{2}\sqrt{d}, \quad \lambda^{-1} = 1 - \frac{m}{2} - \frac{1}{2}\sqrt{d}. \quad (5.4)$$

Собственные векторы, соответствующие этим собственным числам, в базисе ε обладают координатами⁵:

$$e'_1 = \begin{pmatrix} c \\ -b \\ a \end{pmatrix}, \quad e'_2 = \begin{pmatrix} ac(2-m) + bm + b'\sqrt{d} \\ cm - 2ab - c\sqrt{d} \\ 2(a^2 - m) \end{pmatrix},$$

$$e'_3 = \begin{pmatrix} ac(2-m) + bm - b'\sqrt{d} \\ cm - 2ab + c\sqrt{d} \\ 2(a^2 - m) \end{pmatrix},$$

где $b' = ac - b$, и матрица перехода от базиса ε к ε' имеет вид

$$U = \begin{pmatrix} c & ac(2-m) + bm + b'\sqrt{d} & ac(2-m) + bm - b'\sqrt{d} \\ -b & cm - 2ab - c\sqrt{d} & cm - 2ab + c\sqrt{d} \\ a & 2(a^2 - m) & 2(a^2 - m) \end{pmatrix}. \quad (5.5)$$

⁵Все вычисления матриц проведены в программе “Maple” с учетом соотношений: $a^2 + b^2 + c^2 - abc = m$, $d = m^2 - 4m$, $b' = ac - b$, $bb' = a^2 + c^2 - m$.

Обозначим через $F(\mu) = UA(\mu)U^{-1}$ матрицу изометрии $\mathcal{A}(\mu)$ в базисе ε . Элементы матрицы $F(\mu) = F(u + v\sqrt{d})$ будут иметь вид

$$\begin{aligned}
 mF_{11}(\mu) &= -vm^2 + (u + vc^2)m - c^2(u - 1), \\
 mF_{12}(\mu) &= mv(c^2a - cb - 2a) + (c^2a - cb)(1 - u) = mv(cb' - 2a) - cb'(u - 1), \\
 mF_{13}(\mu) &= mv(ac - 2b) - ac(u - 1) = mv(b' - b) - (b' + b)(u - 1), \\
 mF_{21}(\mu) &= mv(2a - cb) + bc(u - 1), \\
 mF_{22}(\mu) &= m + mv(a^2 - c^2) + (a^2 + c^2)(u - 1), \\
 mF_{23}(\mu) &= mv(ab - 2c) + ab(u - 1), \\
 mF_{31}(\mu) &= mv(2b - ac) - ac(u - 1) = mv(b - b') - (b + b')(u - 1), \\
 mF_{32}(\mu) &= mv(2c - a^2c + ab) - (a^2c - ab)(u - 1) = mv(2c - ab') - ab'(u - 1), \\
 mF_{33}(\mu) &= vm^2 + (u - va^2)m - a^2(u - 1).
 \end{aligned} \tag{5.6}$$

Итак, $\mathcal{A}(\mu)$ действительно является изометрией формы $\chi^{(m)}$ на векторном пространстве $V_{\mathbb{Q}}$.

§ 6. Инволюция в группе изометрий

Рассмотрим полуортогональную форму $\chi^{(m)}$ на $\mathbb{Z}$ -модуле ранга 3 и ее группу изометрий из теоремы 5.1. Среди преобразований $\mathcal{A}(\mu)$ есть одна нетривиальная инволюция, а именно $\mathcal{I} = \mathcal{A}(-1)$. Оказывается, в общем случае она не будет изометрией формы над $\mathbb{Z}$.

ПРЕДЛОЖЕНИЕ 6.1. *Преобразование $\mathcal{I}$ является изометрией полуортогональной формы $\chi^{(m)}$ высоты $m \notin \{0, 4\}$ на $\mathbb{Z}$ -модуле ранга 3 только в случае форм со следующими матрицами Грама:*

$$\begin{aligned}
 m = 2, & \quad M(1, 1, 1); & m = -2, & \quad M(3, 4, 3); \\
 m = \nu^2, & \quad M(\nu, 0, 0); & m = -16, & \quad M(4, 4, 4); \\
 m = 2\nu^2, & \quad M(\nu, \nu, 0); & m = -32, & \quad M(4, 8, 4); \\
 & & m = -50, & \quad M(5, 5, 5).
 \end{aligned}$$

ДОКАЗАТЕЛЬСТВО. Матрица $F(-1)$ преобразования $\mathcal{I}$ в базисе (e_1, e_2, e_3) получается подстановкой в матрицу $F(\mu)$ значений $u = -1$, $v = 0$. Элементарные вычисления показывают, что

$$F(-1) = \frac{1}{m} \begin{pmatrix} 2c^2 - m & 2b'c & 2ac \\ -2bc & m - 2(a^2 + c^2) & -2ab \\ 2ac & 2ab' & 2a^2 - m \end{pmatrix}, \quad b' = ac - b. \tag{6.1}$$

Учитывая матрицу (6.1) преобразования $\mathcal{I}$, получаем, что $\mathcal{I}$ является изометрией $\mathbb{Z}$ -модуля тогда и только тогда, когда

$$\frac{2a^2}{m}, \frac{2c^2}{m}, \frac{2bc}{m}, \frac{2ab}{m}, \frac{2ac}{m} \in \mathbb{Z}. \tag{6.2}$$

Поскольку тройка (a, b, c) удовлетворяет уравнению

$$a^2 + b^2 + c^2 - abc = m, \tag{6.3}$$

то $2b^2/m$ также должно быть целым числом.

Обозначим через $\nu > 0$ наибольший общий делитель чисел a, b, c . Тогда $a = \nu\alpha, b = \nu\beta, c = \nu\gamma$ и $2\nu^2$ – наибольший общий делитель чисел $2a^2, 2b^2, 2c^2$. Поэтому $m \mid 2\nu^2$. С другой стороны,

$$m = \nu^2(\alpha^2 + \beta^2 + \gamma^2 - \nu\alpha\beta\gamma),$$

т. е. $\nu^2 \mid m$. Следовательно, $m = \eta\nu^2$, где $\eta \in \{\pm 1, \pm 2\}$, и

$$\alpha^2 + \beta^2 + \gamma^2 - \nu\alpha\beta\gamma = \eta. \quad (6.4)$$

Чтобы найти все формы, одной из изометрий над $\mathbb{Z}$ которых служит $\mathcal{I}$, нам достаточно найти решения диофантова уравнения (6.4), по решениям восстановить высоты m форм и их матрицы Грама $M(a, b, c)$.

Напомним, что на множестве решений уравнения (6.3) действует группа кос перестройками (1.5). Аналогично, если (α, β, γ) – решение уравнения (6.4), то $(\alpha', \beta, \gamma), (\alpha, \beta', \gamma), (\alpha, \beta, \gamma')$, где $\alpha' = \nu\beta\gamma - \alpha, \beta' = \nu\alpha\gamma - \beta, \gamma' = \nu\alpha\beta - \gamma$, также будут решениями. Более того, перестройки решений уравнений (6.3) и (6.4) согласованы. Действительно, если $\nu\alpha' = a' = bc - a$, то $\nu\alpha' = \nu^2\gamma\beta - \nu\alpha$ и $\alpha' = \nu\gamma\beta - \alpha$. В связи с этим для поиска нужных форм нам достаточно найти решения уравнения (6.4) с точностью до перестроек.

Пусть $\eta > 0$ и (α, β, γ) – решение уравнения (6.4). Если у двух координат этого решения поменять знак, то полученная тройка останется решением. Поэтому можно считать, что либо все координаты неотрицательны, либо две координаты неотрицательны, а третья неположительна.

Рассмотрим первый случай. Ввиду действия симметрической группы на множестве решений можно предполагать, что $\alpha \geq \beta \geq \gamma \geq 0$.

ЛЕММА 6.2. Если (α, β, γ) – решение уравнения (6.4) при $\eta > 0, \alpha \geq \beta \geq \gamma \geq 0$ и $\nu\gamma \geq 3$, то (α', β, γ) – тоже решение, причем $\alpha' < \beta$, где $\alpha' = \nu\beta\gamma - \alpha$ – второй корень многочлена $f_\alpha(t) = t^2 - \nu\beta\gamma t + \beta^2 + \gamma^2 - \eta$.

ДОКАЗАТЕЛЬСТВО. Оценим значение $f_\alpha(\beta)$:

$$f_\alpha(\beta) = \beta^2(2 - \nu\gamma) + \gamma^2 - \eta \leq -\beta^2 + \gamma^2 - \eta \leq -\eta < 0.$$

Значит, α' (второй корень многочлена $f_\alpha(t)$) меньше β (см. замечание 1.8), что и требовалось доказать.

Таким образом, мы можем уменьшать старшую координату решения до тех пор, пока не нарушится неравенство $\nu\gamma \geq 3$. Неравенство может нарушиться в следующих случаях:

$$(i) \nu = 1, \gamma = 2; \quad (ii) \nu = 2, \gamma = 1; \quad (iii) \nu = 1, \gamma = 1; \quad (iv) \gamma = 0.$$

(i) Если $\nu = 1$ и $\gamma = 2$, то уравнение (6.4) приобретает вид

$$\alpha^2 + \beta^2 + 4 - 2\alpha\beta = \eta \iff (\alpha - \beta)^2 = \eta - 4 < 0$$

(так как $\eta = 1, 2$), т. е. не имеет решений.

(ii) Если $\nu = 2, \gamma = 1$, то уравнение

$$\alpha^2 + \beta^2 + 1 - 2\alpha\beta = (\alpha - \beta)^2 + 1 = \eta$$

имеет решение $\alpha = \beta$ при $\eta = 1$. Тогда $m = \nu^2 = 4$, а этот случай мы не рассматриваем.

(iii) Пусть $\nu = \gamma = 1$. Тогда

$$\alpha^2 + \beta^2 + 1 - \alpha\beta = (\alpha - \beta)^2 + \alpha\beta + 1 = \eta.$$

Поскольку мы предполагаем, что $\alpha \geq \beta \geq \gamma = 1$ и $\eta = 1, 2$, решение последнего уравнения возможно, лишь когда $\alpha = \beta = 1$ и $\eta = 2$. В этом случае $m = 2$, $a = b = c = 1$. Таким образом, форма высоты 2 с матрицей Грама $M(1, 1, 1)$ обладает изометрией $\mathcal{I}$ над $\mathbb{Z}$.

(iv) Пусть $\gamma = 0$. Тогда

$$\alpha^2 + \beta^2 = \eta.$$

При $\eta = 1$ получаем $\alpha = 1$, $\beta = 0$, ν – произвольное натуральное число. Значит, форма высоты $m = \nu^2$ с матрицей Грама $M(\nu, 0, 0)$ обладает искомой изометрией над $\mathbb{Z}$. При $\eta = 2$ имеет место решение $\alpha = \beta = 1$ уравнения, что дает высоту $m = 2\nu^2$ и матрицу Грама $M(\nu, \nu, 0)$.

Предположим, наконец, что $\alpha \geq \beta \geq 0 > \gamma$. Тогда должно выполняться соотношение

$$\alpha^2 + \beta^2 + \gamma^2 + \nu\alpha\beta|\gamma| = \eta \in \{1, 2\},$$

т.е. сумма четырех неотрицательных целых чисел равна 1 или 2. Если $\eta = 1$, то такое возможно, лишь когда $\gamma = -1$, $\alpha = \beta = 0$ и $\nu \in \mathbb{N}$, что дает форму высоты $m = \nu^2$ и матрицу Грама $M(0, 0, -\nu)$. Если $\eta = 2$, то в сделанных предположениях имеем решение $\alpha = 1$, $\beta = 0$, $\gamma = -1$ и $\nu \in \mathbb{N}$. Это приводит к форме высоты $2\nu^2$ с матрицей Грама $M(\nu, 0, -\nu)$ или $M(0, \nu, -\nu)$. Однако все эти формы нами уже были учтены в п. (iv). Случай $\eta > 0$ разобран полностью.

Рассмотрим ситуацию, когда $\eta < 0$, т.е. $\eta = -1, -2$. Если (α, β, γ) – решение уравнения (6.4), то отрицательными могут быть лишь две координаты, но тогда $(|\alpha|, |\beta|, |\gamma|)$ – также решение и можно предполагать, что $\alpha \geq \beta \geq \gamma > 0$.

ЛЕММА 6.3. *Если (α, β, γ) – решение уравнения (6.4) при $\eta < 0$, $\alpha \geq \beta \geq \gamma > 0$ и $(3 - \nu\gamma)\beta^2 < \eta$, то (α', β, γ) – тоже решение, причем $0 < \alpha' < \beta$, где α' – второй корень многочлена $f_\alpha(t) = t^2 - \nu\beta\gamma t + \beta^2 + \gamma^2 - \eta$.*

ДОКАЗАТЕЛЬСТВО. Оценим $f_\alpha(\beta)$:

$$f_\alpha(\beta) = 2\beta^2 - \nu\beta^2\gamma + \gamma^2 - \eta \leq 3\beta^2 - \nu\beta^2\gamma - \eta < 0 \iff (3 - \nu\gamma)\beta^2 < \eta.$$

Поскольку $f_\alpha(\beta) < 0$, второй корень α' многочлена $f_\alpha(t)$ меньше β (см. замечание 1.8).

Благодаря лемме 6.3 нам надо найти решения уравнения (6.4) при $\eta = -1, -2$ и $(3 - \nu\gamma)\beta^2 \geq \eta$. Последнее неравенство можно переписать в следующем виде: $(\nu\gamma - 3)\beta^2 \leq |\eta|$. Если $\nu\gamma > 5$, то

$$(\nu\gamma - 3)\beta^2 > 2\beta^2 \geq 2 \geq |\eta|$$

и неравенство, а значит, и уравнение (6.4) не имеют решений в целых числах. Если же $\nu\gamma \leq 5$, то это дает ограничение $\nu \leq 5$. Высоты возможных форм приведены в следующей таблице:

ν	5		4		3		2		1	
η	-2	-1	-2	-1	-2	-1	-2	-1	-2	-1
m	-50	-25	-32	-16	-18	-9	-8	-4	-2	-1

Опираясь на работу [7], убеждаемся в том, что форм с высотами -1 , -4 , -8 , -9 , -18 и -25 не существует. Для остальных значений высот из той же работы получаем следующие матрицы Грама:

$$\begin{aligned} t &= -2, & M(3, 4, 3); \\ t &= -16, & M(4, 4, 4) \text{ и } M(5, 3, 5); \\ t &= -32, & M(4, 8, 4) \text{ и } M(7, 6, 3); \\ t &= -50, & M(5, 5, 5) \text{ и } M(7, 5, 4). \end{aligned}$$

Проверить это можно с помощью несложных вычислений, используя теорему 1.10.

Осталось заметить, что формы с матрицами Грама $M(5, 3, 5)$, $M(7, 6, 3)$ и $M(7, 5, 4)$ не подходят, поскольку не удовлетворяют условиям (6.2).

Все эти рассуждения приводят нас к списку форм, обладающих изометрией $\mathcal{I}$ над $\mathbb{Z}$, который приведен в формулировке предложения 6.1.

§ 7. Изометрии форм с высотами 1 и 2

ПРЕДЛОЖЕНИЕ 7.1. Пусть $\chi^{(m)}$, $m \neq 0, 4$, – полуортогональная форма высоты m на $\mathbb{Z}$ -модуле ранга 3 и $\text{Isom}^+(\chi^{(m)})$ – группа ее собственных изометрий. Тогда:

- 1) $\text{Isom}^+(\chi^{(1)}) = \mathbb{Z}_6$ с образующей $\varkappa$;
- 2) $\text{Isom}^+(\chi^{(2)}) = \mathbb{Z}_4$ с образующей $\varkappa$;
- 3) $\text{Isom}^+(\chi^{(m)}) = \mathbb{Z}_2 \times \mathbb{Z}$ при $m > 4$ с образующими I ($I^2 = \text{id}$) и $\mathcal{A}(\mu_0)$ (бесконечного порядка); сомножитель $\mathbb{Z}_2$ в группе изометрий присутствует в случаях, предусмотренных предложением 6.1.

ДОКАЗАТЕЛЬСТВО. По теореме 5.1 любая изометрия формы $\chi^{(m)}$, $m \neq 0, 4$, над полем $\mathbb{Q}$ имеет вид $\mathcal{A}(\mu)$, матрица которой в базисе, собственном для $\varkappa$, равна $\text{Diag}(1, \mu, \mu^{-1})$, где $\mu \in \mathbb{Q}[\sqrt{m^2 - 4m}]$, причем если $\mu^{\pm 1} = u \pm v\sqrt{m^2 - 4m}$, то имеет место равенство

$$u^2 - v^2(m^2 - 4m) = 1. \quad (7.1)$$

Если $\mathcal{A}(\mu)$ – изометрия над $\mathbb{Z}$, то ее след, равный $2u + 1$, должен быть целым, т. е. $u = n/2$, где $n \in \mathbb{Z}$. Обозначим $m^2 - 4m = r^2 m_1$, где m_1 свободно от квадратов. Тогда $\mu = \frac{n}{2} + vr\sqrt{m_1}$ – элемент квадратичного поля $\mathbb{Q}[\sqrt{m_1}]$ с целым следом и единичной нормой $N(\mu) = \frac{n^2}{4} - v^2 r^2 m_1 = 1$ (см. (7.1)). Следовательно, μ – алгебраическое целое число, которое является единицей квадратичного поля $\mathbb{Q}[\sqrt{m_1}]$ [8].

По теореме Дирихле о единицах [8] в случае $m_1 < 0$ все такие μ являются корнями из 1, лежащими в $\mathbb{Q}[\sqrt{m_1}]$, а если $m_1 > 0$, то существует основная единица поля μ_1 такая, что $\mu = \pm \mu_1^s$, где $s \in \mathbb{Z}$.

Если $m = 1$, то $m^2 - 4m = -3$ и μ – единица поля $\mathbb{Q}[\sqrt{-3}]$. Решая уравнение (7.1) в этом случае, получаем, что μ – корень шестой степени из 1 с примитивным корнем μ_0 . Сравнивая его с собственными числами дуализирующего оператора (5.4), находим, что $\mathcal{A}(\mu_0) = \varkappa$.

Аналогичные рассуждения показывают, что $\text{Isom}^+(\chi^{(2)}) \simeq \mathbb{Z}_4$ с образующей $\varkappa$.

Пусть теперь $m \notin \{0, 1, 2, 4\}$ (полуортогональной формы высоты 3 не существует). Тогда $m^2 - 4m > 0$ и μ – единица поля $\mathbb{Q}[\sqrt{m_1}]$ с положительным m_1 . По теореме Дирихле $\mu = \mu_1^s$, $s \in \mathbb{Z}$, где $\mu_1 = u_1 + v_1\sqrt{m_1}$, $u_1, v_1 > 0$, – основная единица. Вообще, $\mathcal{A}(\pm\mu_1)$ являются изометриями над $\mathbb{Q}$, но могут не быть преобразованиями $\mathbb{Z}$ -модуля. С другой стороны, $\varkappa \in \text{Isom}^+(\chi^{(m)})$ и его собственное число $\lambda(2-m)/2 + (r/2)\sqrt{m_1}$ – единица поля $\mathbb{Q}[\sqrt{m_1}]$. Следовательно, $\lambda = \mu_1^k$ при $m < 0$ и $\lambda = -\mu_1^{-k}$ при $m > 4$, $k \in \mathbb{N}$.

Обозначим

$$s = \min_{k \in \mathbb{N}} \mathcal{A}(\mu_1^k) \in \text{Isom}^+(\chi^{(m)}), \quad l = \min_{k \in \mathbb{N}} \mathcal{A}(-\mu_1^k) \in \text{Isom}^+(\chi^{(m)})$$

(заметим, что может быть $\mathcal{A}(-\mu_1^k) \notin \text{Isom}^+(\chi^{(m)})$ для любого $k \in \mathbb{N}$, тогда l неопределено). Равенство $l = s$ возможно, только если $I \in \text{Isom}^+(\chi^{(m)})$, и тогда $\text{Isom}^+(\chi^{(m)}) = \langle I, \mathcal{A}(\mu_1^s) \rangle = \mathbb{Z}_2 \times \mathbb{Z}$.

Предположим, что $I \notin \text{Isom}^+(\chi^{(m)})$, и разберем случаи $m < 0$ и $m > 4$ отдельно.

Если $m < 0$, то собственное число λ дуализирующего оператора $\varkappa$ выражается через основную единицу как $\lambda = \mu_1^k$, $k \in \mathbb{N}$. Поэтому $\mathcal{A}(-\mu_1^n)$ может не лежать в группе собственных изометрий ни при каком n , но если лежит, то $s = 2l$.

Если $m > 4$, то $\lambda = -\mu_1^{-k}$, $k \in \mathbb{N}$, и $\mathcal{A}(-\mu_1^k) \in \text{Isom}^+(\chi^{(m)})$. Поэтому образующей группы изометрий в этом случае служит $\mathcal{A}(-\mu_1^l)$. Предложение доказано.

В качестве следствия наших рассуждений удобно сформулировать

ПРЕДЛОЖЕНИЕ 7.2. Пусть $\chi^{(m)}$ – полуортогональная форма высоты m на $\mathbb{Z}$ -модуле V ранга 3 ($m \notin \{0, 1, 2, 3, 4\}$). Представим $m^2 - 4m$ в виде $r^2 m_1$, где m_1 свободно от квадратов. Обозначим через $\mu_1 = u_1 + v_1\sqrt{m_1}$ основную единицу поля $\mathbb{Q}[\sqrt{m_1}]$. Группа собственных изометрий формы $\chi^{(m)}$ изоморфна $\mathbb{Z}_2 \times \mathbb{Z}$ (если инволюция $\mathcal{I}$ является изометрией) или $\mathbb{Z}$, где образующая подгруппы $\text{Isom}_\infty^+(\chi^{(m)}) \simeq \mathbb{Z}$ – это:

- 1) $\mathcal{A}(\mu_1^s)$ для некоторого натурального s при $m < 0$, и тогда $\mathcal{A}(-\mu_1^k) \in \text{Isom}^+(\chi^{(m)})$, только если $\mathcal{I} \in \text{Isom}^+(\chi^{(m)})$;
- 2) $\mathcal{A}(-\mu_1^s)$ при $m < 0$, $\mathcal{I} \notin \text{Isom}^+(\chi^{(m)})$, и тогда минимальное натуральное число k , при котором $\mathcal{A}(\mu_1^k) \in \text{Isom}^+(\chi^{(m)})$, равно $2s$;
- 3) $\mathcal{A}(-\mu_1^s)$ при $m > 4$.

СЛЕДСТВИЕ 7.3. Если $m > 4$ – высота формы, $\mathcal{A}(-\mu_0^s)$ – образующая группы $\text{Isom}_\infty^+(\chi^{(m)})$ и дуализирующий оператор равен $\mathcal{A}(-\mu_0^{-2s})$, то группа $\text{Isom}^+(\chi^{(m)})$ содержит инволюцию.

ДОКАЗАТЕЛЬСТВО. Поскольку $\mathcal{A}(-\mu_0^s), \mathcal{A}(-\mu_0^{-2s}) \in \text{Isom}^+(\chi^{(m)})$, то $\mathcal{I} = \mathcal{A}(-\mu_0^{-2s})\mathcal{A}^2(-\mu_0^s) \in \text{Isom}^+(\chi^{(m)})$.

§ 8. Общая полуортогональная форма

ОПРЕДЕЛЕНИЕ 8.1. Пусть s – наименьшее натуральное число, при котором преобразование $\mathcal{A}(\mu_0^s)$ или $\mathcal{A}(-\mu_0^s)$ является автоморфизмом $\mathbb{Z}$ -модуля, т. е. образующей подгруппы $\text{Isom}_\infty^+(\chi^{(m)})$. Введем для μ_0^s символ $\mu = \frac{n}{2} + v\sqrt{m^2 - 4m}$.

Здесь $v = \sqrt{\frac{n^2 - 4}{4m(m-4)}}$.

ПРЕДЛОЖЕНИЕ 8.2. Пусть $\chi^{(m)}$ – полуортогональная форма высоты $m \notin \{0, 1, 2, 4\}$ на $\mathbb{Z}$ -модуле ранга 3 с дуализирующим оператором $\varkappa$. Для образующей $\mathcal{A}$ подгруппы $\text{Isom}_{\infty}^{+}(\chi^{(m)})$ возможны следующие ситуации:

- 1) если $\mathcal{A} = \mathcal{A}(\pm\mu)$ и $\mathcal{A}^2(\pm\mu) = \varkappa$, то $m = 4 - n^2$, $n \in \mathbb{Z}_{\geq 3}$;
 - 2) если $\mathcal{A} = \mathcal{A}(-\mu)$ и $\mathcal{A}(-\mu^2) = \varkappa^{-1}$, то $m = n^2$, $n \in \mathbb{Z}_{\geq 3}$ и $\mathcal{I} \in \text{Isom} \chi^{(m)}$;
 - 3) если $\mathcal{A} = \mathcal{A}(\mu)$ и $\mathcal{A}^3(\mu) = \varkappa$, то $m = -(n-2)(n+1)^2$, $n \in \mathbb{Z}_{\geq 3}$;
 - 4) если $\mathcal{A} = \mathcal{A}(-\mu)$ и $\mathcal{A}^3(\mu) = \varkappa$, то $m = -(n-2)(n+1)^2$, $n \in \mathbb{Z}_{\geq 3}$ и $\mathcal{I} \in \text{Isom} \chi^{(m)}$;
 - 5) если $\mathcal{A} = \mathcal{A}(-\mu)$ и $\mathcal{A}^3(-\mu) = \varkappa^{-1}$, то $m = n^3 - 3n + 2$, $n \in \mathbb{Z}_{\geq 3}$.
- В остальных случаях образующей подгруппы $\text{Isom}_{\infty}^{+}(\chi^{(m)})$ является $\varkappa$.

ДОКАЗАТЕЛЬСТВО. Поскольку $\mathcal{A}(\mu)$ (или $\mathcal{A}(-\mu)$) – образующая подгруппы $\text{Isom}_{\infty}^{+}(\chi^{(m)})$, то найдется целое число t такое, что $\mathcal{A}^t(\mu) = \varkappa$ (или $\mathcal{A}(-\mu^t) = \varkappa^{-1}$). Поскольку $\varkappa = \mathcal{A}(\lambda)$, $\lambda = 1 - \frac{m}{2} + \frac{1}{2}\sqrt{m^2 - 4m}$, $\mu > 0$, то отсюда следует одно из равенств

$$\mu^t = \lambda \quad \text{при} \quad \lambda > 0; \quad -\mu^t = \lambda^{-1} \quad \text{при} \quad \lambda^{-1} < 0 \quad (8.1)$$

(см. теорему 5.1), откуда имеем

$$2 - m = \mu^t + \mu^{-t} \quad \text{при} \quad m < 0; \quad m - 2 = \mu^t + \mu^{-t} \quad \text{при} \quad m > 4. \quad (8.2)$$

Обозначим $f_t = \mu^t + \mu^{-t}$. Тогда $f_0 = 2$, $f_1 = n$ и

$$f_{t+1} = f_t f_1 - f_{t-1}. \quad (8.3)$$

В этих обозначениях соотношения (8.2) переписываются следующим образом:

$$m = 2 - f_t \quad \text{при} \quad m < 0; \quad m = f_t + 2 \quad \text{при} \quad m > 0. \quad (8.4)$$

Прямые вычисления показывают, что:

- (i) если $\lambda = \mu^2$, то $m = 2 - f_2 = 4 - n^2$, $n \geq 3$;
- (ii) если $\lambda^{-1} = -\mu^2$, то $m = f_2 + 2 = n^2$, $n \geq 3$;
- (iii) если $\lambda = \mu^3$, то $m = 2 - f_3 = 2 + 3n - n^3 = -(n-2)(n+1)^2$, $n \geq 3$;
- (iv) если $\lambda^{-1} = -\mu^3$, то $m = f_3 + 2 = n^3 - 3n + 2$, $n \geq 3$.

Далее для окончания доказательства предложения применим предложение 7.2, следствие 7.3 и следующие утверждения.

ЛЕММА 8.3. Если $\varkappa = \mathcal{A}^t(\mu)$, т.е. $\lambda = \mu^t$ при $t \geq 4$, то $\mathcal{A}(\pm\mu) \notin \text{GL}_3(\mathbb{Z})$.

ЛЕММА 8.4. Если $\varkappa^{-1} = \mathcal{A}(-\mu^t)$, т.е. $\lambda^{-1} = -\mu^t$ при $t \geq 4$, то $\mathcal{A}(-\mu) \notin \text{GL}_3(\mathbb{Z})$.

Несмотря на схожесть формулировок, доказательство каждой из этих лемм приходится проводить отдельно. Начнем со следующего наблюдения.

ЛЕММА 8.5. Пусть матрица Грама полуортогональной формы $\chi^{(m)}$ в базисе $\varepsilon = (e_1, e_2, e_3)$ равна $M(a, b, c)$ и $\mu = \frac{n}{2} + v\sqrt{m^2 - 4m}$. Тогда если $\mathcal{A}(\mu) \in \text{Isom}_{\infty}^{+}(\chi^{(m)})$, то

$$\frac{ab(n-2)}{m} \in \mathbb{Z}, \quad \frac{ac(n-2)}{m} \in \mathbb{Z}, \quad \frac{bc(n-2)}{m} \in \mathbb{Z};$$

если $\mathcal{A}(-\mu) \in \text{Isom}_{\infty}^{+}(\chi^{(m)})$, то

$$\frac{ab(n+2)}{m} \in \mathbb{Z}, \quad \frac{ac(n+2)}{m} \in \mathbb{Z}, \quad \frac{bc(n+2)}{m} \in \mathbb{Z}.$$

ДОКАЗАТЕЛЬСТВО. Элементы матрицы $F(\mu)$ изометрии $\mathcal{A}(\mu)$ в базисе ε выписаны в формуле (5.6). По предположению леммы $F(\mu) \in \mathrm{GL}_3(\mathbb{Z})$. Поэтому $F_{ij}(\mu) \in \mathbb{Z}$. Суммируя F_{13} и F_{31} , получаем

$$\frac{2ac(1-u)}{m} \in \mathbb{Z}. \quad (8.5)$$

Матрица Грама формы $\chi^{(m)}$ в базисе $R_2\varepsilon = (e_1, e_3, e'_2)$ будет равна $M(b, bc - a, c)$ (см. (1.2), (1.3)). Поэтому из формулы (8.5), примененной к последней матрице, следует, что

$$\frac{2bc(1-u)}{m} \in \mathbb{Z}.$$

Наконец, матрица Грама формы $\chi^{(m)}$ в базисе $L_1\varepsilon = (e'_2, e_1, e_3)$ совпадает с $M(a, ab - c, b)$. Значит,

$$\frac{2ab(1-u)}{m} \in \mathbb{Z}.$$

Осталось заметить, что $u = n/2$ для матрицы $F(\mu)$ и $u = -n/2$ для $F(-\mu)$. Лемма доказана.

ДОКАЗАТЕЛЬСТВО ЛЕММЫ 8.3. В этом случае высота формы m отрицательна. По теореме 1.10 существует базис $\varepsilon = (e_1, e_2, e_3)$ $\mathbb{Z}$ -модуля, в котором матрица Грама формы $\chi^{(m)}$ имеет вид $M(a, b, c)$, причем

$$|c|, |a| > 2, \quad (8.6)$$

$$|c|^2(|c| - 3) \leq |m|, \quad (8.7)$$

$$(|c| - 2)a^2 \leq |m| + |c|^2. \quad (8.8)$$

Если $\mathcal{A}(\mu) \in \mathrm{Isom}_\infty^+(\chi^{(m)})$, то по лемме 8.5 отношение $\frac{|ac|(n-2)}{|m|}$ должно быть целым числом, в частности

$$|ac| \geq \frac{|m|}{n-2}. \quad (8.9)$$

Если $\mathcal{A}(-\mu) \in \mathrm{GL}_3(\mathbb{Z})$, то целым числом должно быть отношение $\frac{|ac|(n+2)}{|m|}$. Следовательно,

$$|ac| \geq \frac{|m|}{n+2}. \quad (8.10)$$

Наша цель – показать, что при $t \geq 4$ соотношения (8.4), (8.7), (8.8) противоречат соотношению (8.9) или (8.10).

Обозначив $\gamma = |c| - 3$, перепишем неравенство (8.7) в виде

$$(\gamma + 3)^2\gamma \leq |m|.$$

Поскольку $\gamma^3 \leq (\gamma + 3)^2\gamma$, это дает оценку для $|c|$:

$$|c| \leq \sqrt[3]{|m|} + 3. \quad (8.11)$$

При исследовании неравенства (8.8) надо разобрать два случая: $|c| = 3$ и $|c| \geq 4$. Если $|c| = 3$, то неравенство (8.8) имеет вид $|a| \leq \sqrt{|m|} + 9$. Следовательно,

$$|ac| \leq 3\sqrt{|m|} + 9.$$

Учитывая (8.9), получаем

$$|m|^2 \leq 9(|m| + 9)(n - 2)^2, \quad (8.12)$$

а из (8.10) вытекает неравенство

$$|m|^2 \leq 9(|m| + 9)(n + 2)^2. \quad (8.13)$$

Покажем, что при $m = 2 - f_t < 0$, $t \geq 4$, неравенство (8.13) не имеет решений, тогда и неравенство (8.12) не будет их иметь.

Заметим, что при $n = 1, 2$ высота $m = 2 - f_t$ принадлежит множеству $\{0, 1, 2, 3, 4\}$, которое мы не рассматриваем в этом параграфе. Поэтому нас интересуют значения $n \geq 3$.

Если $m = 2 - f_4(n)$, то, поскольку $f_4(n) = n^2(n^2 - 4) + 2$, неравенство (8.13) переписывается следующим образом:

$$n^4(n - 2)^2 \leq 9(n^2(n^2 - 4) + 9),$$

и оно не имеет решений при $n \geq 5$.

Индукцией по t можно показать, что при $n \geq 3$ значения многочленов $f_t(n)$ возрастают: $f_{t+1}(n) > f_t(n)$. Поэтому неравенство (8.13) не имеет решений при $m = 2 - f_t(n)$, $n \geq 5$, $t \geq 4$.

Если $m = 2 - f_5(n)$, то $|m| = n^5 - 5n^3 + 5n - 2 = (n - 2)(n^2 + n - 1)^2$ и неравенство (8.13) приобретает вид

$$(n - 2)^2(n^2 + n - 1)^4 \leq 9((n - 2)(n^2 + n - 1)^2 + 9)(n + 2)^2.$$

Последнее неравенство не имеет решений при $n \geq 4$. Следовательно, неравенство (8.13) не имеет решений при $m = 2 - f_t(n)$, $n \geq 4$, $t \geq 5$.

Если $m = 2 - f_6(n)$, то $|m| = n^2(n^2 - 3)^2$. Достаточно проверить, что неравенство (8.13) ложно при $n = 3$. При таком значении n неравенство (8.13) сводится к следующему:

$$(9 \cdot 36)^2 \leq 9(9 \cdot 36 + 9)(3 + 2)^2,$$

что, очевидно, неверно.

Осталось разобрать случаи $|m| = f_4(n) - 2$, $n = 3, 4$, и $|m| = f_5(3) - 2$.

Если $n = 3$, то $m = 2 - f_4(3) = -45 \equiv -1 \pmod{4}$ и форма такой высоты не существует (замечание 1.7).

Если $n = 4$, то $m = 2 - f_4(4) = -192 \equiv 0 \pmod{3}$, но $-192 \not\equiv 0 \pmod{9}$, поэтому форма высоты $m = -192$ не существует.

Наконец, $m = 2 - f_5(3) = -121 \equiv -1 \pmod{4}$, т.е. форма такой высоты не существует.

Случай $|c| = 3$ разобран полностью.

Предположим, что $|c| \geq 4$. Тогда неравенство (8.8) с учетом (8.11) переписывается в виде

$$2|a|^2 \leq (|c| - 2)|a|^2 \leq |m| + |c|^2 \leq |m| + (\sqrt[3]{|m|} + 3)^2.$$

Значит,

$$\begin{aligned} |c| |a|^2 &\leq |m| + |c|^2 + 2|a|^2 \leq |m| + (\sqrt[3]{|m|} + 3)^2 + |m| + (\sqrt[3]{|m|} + 3)^2 \\ &= 2(|m| + (\sqrt[3]{|m|} + 3)^2). \end{aligned}$$

В результате имеем

$$\begin{aligned} |ac|^2 &\leq 2(|m| + (\sqrt[3]{|m|} + 3)^2)(\sqrt[3]{|m|} + 3) \\ &= 2(|m|^{4/3} + 4|m| + 9|m|^{2/3} + 27|m|^{1/3} + 27). \end{aligned} \quad (8.14)$$

Нам потребуется следующая оценка выражения из правой части неравенства (8.14), доказательство которой мы не приводим.

ЛЕММА 8.6. Если $|m| \geq 7^3$, то

$$|m|^{4/3} + 4|m| + 9|m|^{2/3} + 27|m|^{1/3} + 27 \leq 2|m|^{4/3}.$$

С учетом леммы 8.6 и оценки (8.14) неравенства (8.9), (8.10) переписываются в виде

$$\frac{|m|^2}{(n-2)^2} \leq 4|m|^{4/3}, \quad \frac{|m|^2}{(n+2)^2} \leq 4|m|^{4/3},$$

что равносильно

$$|m| \leq 8(n-2)^3, \quad (8.15)$$

$$|m| \leq 8(n+2)^3. \quad (8.16)$$

Покажем, что если $|m| = f_t - 2$, $t \geq 4$, то неравенства (8.15), (8.16) не имеют решений при $n \geq 3$.

Если $|m| = f_4 - 2 = (n^2 - 4)n^2$, то неравенство (8.16) противоположно следующему:

$$(n-2)n^2 > 8(n+2)^2,$$

которое выполнено при $n \geq 13$. Следовательно, неравенства (8.15) и (8.16) не имеют решений при $|m| = f_t(n) - 2$, $t \geq 4$, $n \geq 13$.

Если $|m| = f_5 - 2 = (n-2)(n^2 + n - 1)^2$, то неравенство (8.16) приобретает вид

$$(n-2)(n^2 + n - 1)^2 \leq 8(n+2)^3$$

и не имеет решений при $n \geq 6$.

Если $|m| = f_6 - 2 = n^2(n^2 - 3)^2$, то неравенство (8.16) приобретает вид

$$n^2(n^2 - 3)^2 \leq 8(n+2)^3$$

и не имеет решений при $n \geq 4$.

Пусть $|m| = f_8(3) - 2 = 2207$. Поскольку это число больше $8(3+2)^2 = 1000$, то неравенства (8.15) и (8.16) могут иметь решения только в следующих случаях:

- (i) $|m| = f_4(n) - 2$, $n \in [3, 12]$;
- (ii) $|m| = f_5(n) - 2$, $n \in [3, 5]$;
- (iii) $|m| = f_6(3) - 2$;
- (iv) $|m| = f_7(3) - 2$.

Мы уже показали, что форм высоты $m = 2 - f_4(n)$ при $n = 3, 4$ и $m = 2 - f_5(3)$ не существует. Поскольку $2 - f_4(n) = -n^2(n^2 - 4) \equiv -1 \pmod{4}$ при нечетных n , форм высоты $m = 2 - f_4(n)$ с нечетными n также не существует. Далее, $2 - f_4(8) = -2205$ и $2 - f_4(10) = -9600$. Оба этих числа делятся на 3, но не на 9. Значит, форм высоты $m = -2205$ и $m = -9600$ не бывает.

Форма высоты $m = 2 - f_5(5) = -2523$ не существует, так как это число делится на 3, а на 9 не делится. Кроме того, формы высоты $f_7(3) - 2 = -841$ не бывает, поскольку $-841 \equiv -1 \pmod{4}$.

Неразобранными остаются случаи $m = 2 - f_4(6) = -1152$, $m = 2 - f_4(12) = -20160$, $m = 2 - f_5(4) = -722$ и $m = 2 - f_6(3) = -320$.

Итак, если

$$|m| \geq 7^3, \quad t \geq 4, \quad m \notin \{-722, -1152, -20160\} \quad (8.17)$$

и $\lambda = \mu^t$, то $\mathcal{A}(\pm\mu) \notin \text{Isom}_{\infty}^+(\chi^{(m)})$.

Выясним, при каких условиях для $|m|$ собственное число дуализирующего оператора есть $\lambda = \mu^t$ при $t \geq 4$ и $|m| < 7^3 = 343$. Как уже отмечалось, из соотношения $\lambda = \mu^t$ следует, что $|m| = f_t - 2$.

Если $t = 4$, то $m = 2 - f_4(n) = -(n^2 - 4)n^2$, а мы уже выяснили, что форм высоты $m = 2 - f_4(n)$ при $n = 3, 4$ не существует. Кроме того, имеет место неравенство $|m| = f_4(n) - 2 > 7^3$ при $n \geq 5$,

Если $t = 5$, то $|m| = f_5(n) - 2 = n^5 - 5n^3 + 5n - 2$ и форма высоты $f_5(3) - 2$ не существует, а $f_5(n) - 2 > 7^3$ при $n \geq 4$.

Если $t = 6$, то $|m| = f_6(n) - 2 = n^6 - 6n^4 + 9n^2 - 4$ и $f_6(n) - 2 > 7^3$ при $n \geq 4$, однако $f_6(3) - 2 = 320$, и форма высоты $m = -320$ вполне может существовать.

Наконец, $|m| = f_t(n) - 2 > 7^3$ при $t \geq 7$ для всех $n \geq 3$.

Таким образом, осталось исследовать формы высот -320 , -722 , -1152 и -20160 .

ЛЕММА 8.7. *Не существует полуортогональных форм высот $m = -20160$ и $m = -1152$. Существуют только две формы высоты $m = -720$ с матрицами Грама $G_1 = M(5, 12, 27)$ и $G_2 = M(9, 9, 13)$. Существуют только три формы высоты $m = -320$ с матрицами Грама⁶ $G_3 = M(6, 7, 15)$, $G_4 = M(7, 7, 11)$ и $G_5 = M(8, 8, 8)$.*

ДОКАЗАТЕЛЬСТВО. К сожалению, короткого доказательства этой леммы получить не удалось. Поэтому приведем здесь лишь его алгоритм. Как доказано в работе [7], для любой полуортогональной формы высоты m можно найти базис, в котором матрица Грама формы будет иметь вид $M(a, b, c)$, причем элементы c и a удовлетворяют неравенствам (8.6)–(8.8). Понятно, что таких элементов может быть лишь конечное число. Для каждой такой пары элементов (a_0, c_0) необходимо решить уравнение $a_0^2 + b^2 + c_0^2 - a_0 b c_0 = m$ относительно b . Если корень b_0 – целое число, то $M(a_0, b_0, c_0)$ – матрица Грама искомой формы.

Продолжим доказательство леммы 8.3. Пусть $M(a, b, c)$ – матрица Грама формы высоты $m = -722$ и $\mathcal{A}(\mu)$ – ее изометрия. Тогда числа

$$\frac{2ab}{-722}, \quad \frac{2cb}{-722}, \quad \frac{2ca}{-722}$$

должны быть целыми (см. лемму 8.5), так как в рассматриваемом случае $n = 4$. Однако $722 = 2^2 \cdot 19$, и это условие не выполнено ни для G_1 , ни для G_2 . Если же $\mathcal{A}(-\mu) \in \text{Isom}_{\infty}^+(\chi^{(m)})$, то целыми должны быть числа

$$\frac{6ab}{-722}, \quad \frac{6cb}{-722}, \quad \frac{6ca}{-722}$$

(см. лемму 8.5), что также не выполняется.

⁶Тот факт, что матрицы Грама G_1 и G_2 , как и G_3 , G_4 , G_5 , задают разные формы, не доказан. Его можно воспринимать как гипотезу.

Пусть $M(a, b, c)$ – матрица Грама формы высоты $m = -320$ и $\mathcal{A}(\mu)$ – ее изометрия. Тогда числа

$$\frac{ab}{-320}, \quad \frac{cb}{-320}, \quad \frac{ca}{-320}$$

должны быть целыми, так как $n = 3$. Поскольку по лемме 8.7 матрица Грама формы высоты -320 равна одной из G_i , $i = 3, 4, 5$, выписанные числа не принадлежат $\mathbb{Z}$. Если же $\mathcal{A}(-\mu) \in \text{Isom}_{\infty}^+(\chi^{(m)})$, то целыми должны быть числа

$$\frac{5ab}{-320}, \quad \frac{5cb}{-320}, \quad \frac{5ca}{-320},$$

что выполнено лишь для матрицы $G_3 = M(8, 8, 8)$. Тем не менее, $\mathcal{A}(-\mu) \notin \text{Isom}_{\infty}^+(\chi^{(m)})$ и в этом случае. Вычислим некоторые элементы матрицы $F(\mu)$ (см. (5.6)) преобразования $\mathcal{A}(-\mu)$ в базисе ε . Для этого сначала вычислим μ полностью. Мы знаем, что $\mu = \frac{n}{2} + v\sqrt{m^2 - 4m} + v\sqrt{320^2 - 4 \cdot 320}$, где $v = \frac{1}{2}\sqrt{\frac{n^2 - 4}{m^2 - 4m}}$ (определение 8.1), откуда $v = \frac{1}{288}$. Подставив теперь $u = -\frac{3}{2}$, $v = -\frac{1}{288}$, $c = 8$ и $m = -320$ в формулу для $F_{11}(\mu)$ (см. (5.6)), найдем, что $F_{11}(-\mu) = -10/3 \notin \mathbb{Z}$. Лемма 8.3 доказана полностью.

ДОКАЗАТЕЛЬСТВО ЛЕММЫ 8.4. Если $\lambda^{-1} = -\mu^t$, то высота m положительна (напомним, что в настоящем параграфе мы ограничиваемся значениями $m \geq 5$).

Из предположения $\lambda^{-1} = -\mu^t$ получаем, что $\mu^t = \frac{m-2}{2} + \frac{1}{2}\sqrt{m^2 - 4m}$ и $m = \mu^t + \mu^{-t} = f_t + 2$ (определение f_t см. в (8.3)).

По теореме 1.10 существует базис $\varepsilon = (e_1, e_2, e_3)$ $\mathbb{Z}$ -модуля, в котором матрица Грама формы $\chi^{(m)}$ имеет вид $M(a, b, c)$, причем

$$|a| \geq |b| \geq |c| \geq 2, \quad abc < 0, \quad (8.18)$$

или

$$\min(|a|, |b|, |c|) \leq 1. \quad (8.19)$$

Кроме того, из леммы 8.5 следует, что если $\mathcal{A}(-\mu) \in \text{Isom}_{\infty}^+(\chi^{(m)})$, $\mu = \frac{n}{2} + v\sqrt{m^2 - 4m}$, то

$$\frac{ab(n+2)}{m}, \frac{ac(n+2)}{m}, \frac{bc(n+2)}{m} \in \mathbb{Z}. \quad (8.20)$$

Предположим, что выполнено условие (8.18). Тогда

$$m = a^2 + b^2 + c^2 - abc \geq |abc| \implies |bc| \leq m^{2/3}.$$

С другой стороны, из целочисленности дробей (8.20) получаем, что

$$\frac{m}{n+2} \leq |bc|.$$

Собирая эти неравенства вместе, находим, что должно быть выполнено неравенство

$$(n+2)^3 \geq m. \quad (8.21)$$

Пусть $|a| \geq |b| \geq |c| = 1$. В этом случае

$$m = a^2 + b^2 + 1 - ab = (a-b)^2 + 1 + ab > b^2 \implies \sqrt{m} > b,$$

но ввиду леммы 8.5 при $c = 1$ имеем $b \frac{n+2}{m} \in \mathbb{Z}$, т. е. $b \geq \frac{m}{n+2}$. Следовательно,

$$(n+2)^2 > m. \quad (8.22)$$

Если $|a| > |b| \geq |c| = 0$, то матрица Грама формы $\chi^{(m)}$ в некотором базисе ε равна $M(a, b, 0)$. Следовательно,

$$m = a^2 + b^2 \geq a^2.$$

С другой стороны, если $A(-\mu) \in \text{Isom}_{\infty}^+(\chi^{(m)})$, $\mu = \frac{n}{2} + v\sqrt{m^2 - 4m}$, то матрица $F(-\mu)$ (см. (5.6)) изометрии $A(-\mu)$ в базисе ε должна иметь целые коэффициенты. В частности,

$$F_{21}(-\mu) = -2av \in \mathbb{Z}. \quad (8.23)$$

Мы знаем, что $v = \frac{1}{2}\sqrt{\frac{n^2-4}{m^2-4m}}$ (см. определение 8.1). Значит, число $a\sqrt{\frac{n^2-4}{m^2-4m}}$ должно быть целым, откуда получаем

$$a^2(n^2 - 4) \geq m^2 - 4m,$$

что вместе с оценкой $m \geq a^2$ дает неравенство

$$n^2 \geq m. \quad (8.24)$$

Теперь покажем, что при достаточно больших t и n неравенства (8.21), (8.22) и (8.24) не выполнены, и рассмотрим оставшееся конечное число случаев.

Прежде всего заметим, что $m = f_t + 2 \in \{1, 2, 3, 4\}$ при $n = 1, 2$, а эти высоты мы здесь не рассматриваем, так что нас интересуют значения $n \geq 3$. Поскольку $f_{t+1}(n) \geq f_t(n)$ при $n \geq 3$, возьмем $m = f_4(n) + 2 = (n^2 - 2)^2$. Тогда (начиная с $n = 5$) имеет место неравенство

$$m > (n+2)^3, \quad (8.25)$$

что доказывает ложность неравенств (8.21), (8.22) и (8.24) при $t \geq 4$ и $n \geq 5$. Если $m = f_5(n) + 2 = n^5 - 5n^3 + 3n + 2$, то неравенство (8.25) выполняется при $n \geq 4$. Наконец, если $m = f_6(n) + 2 = n^2 - 6n^4 + 7n^2 + 2$, то (8.25) верно для всех $n \geq 3$.

Осталось разобрать случаи $m = f_4(3) + 2 = 49$, $m = f_4(4) + 2 = 196$ и $m = f_5(3) + 2 = 119$.

Поскольку $119 \equiv -1 \pmod{4}$, форма высоты $m = f_5(3) + 2$ не существует (см. замечание 1.7).

ЛЕММА 8.8. *Существуют две формы высоты 49 с матрицами Грама $M(8, 4, 1)$ и $M(7, 0, 0)$ и одна форма высоты 196 с матрицей Грама $M(14, 0, 0)$.*

ДОКАЗАТЕЛЬСТВО получим перебором случаев, которые ограничиваются теоремой 1.10.

Преобразование $A(-\mu)$ форм с матрицами Грама $M(7, 0, 0)$ и $M(14, 0, 0)$ не является изоморфизмом $\mathbb{Z}$ -модуля, поскольку элемент $F_{21}(-\mu)$ матриц этих форм в базисе ε в первом случае равен $1/3$, а во втором $1/4$. Действительно, в первом случае $n = 3$, $a = 7$ и $m = 49$, а во втором $n = 4$, $a = 14$ и $m = 196$.

Преобразование $A(-\mu)$ формы с матрицей Грама $M(8, 4, 1)$ не является изоморфизмом $\mathbb{Z}$ -модуля, поскольку отношение $ab(n \pm 2)/m$ в случае $n = 4$ — дробное число. Лемма 8.4 доказана.

В следующих двух параграфах мы точнее исследуем возможности 1)–5) из предложения 8.2 для образующей подгруппы $\text{Isom}_{\infty}^+(\chi^{(m)})$.

§ 9. Кубический корень из дуализирующего оператора

ПРЕДЛОЖЕНИЕ 9.1. Пусть $\chi^{(m)}$ – полуортогональная форма высоты $m < 0$ на $\mathbb{Z}$ -модуле ранга 3 с дуализирующим оператором $\varkappa$; преобразование $\mathcal{A}(\mu)$ – образующая подгруппы $\text{Isom}_{\infty}^{+}(\chi^{(m)})$. Тогда $\mathcal{A}^3(\mu) = \varkappa$, если и только если выполнены следующие условия:

- 1) $m = -(n-2)(n+1)^2$ для некоторого натурального $n \geq 3$;
- 2) матрица Грама формы $\chi^{(m)}$ в каком-то базисе имеет вид $M((n+1), (n+1), (n+1))$, в этом случае $\mathcal{A}(\mu) = \mathcal{L}_2 \mathcal{L}_1$, т. е. $\mathcal{A}(\mu)$ принадлежит группе кос (см. (1.2)).

ДОКАЗАТЕЛЬСТВО. Если $\sqrt[3]{\varkappa} \in \text{Isom}_{\infty}^{+}(\chi^{(m)})$, то $-m = (n-2)(n+1)^2$ в силу предложения 8.2. Рассмотрим матрицу Грама $M(a, b, c)$ формы $\chi^{(m)}$ в каком-нибудь базисе. По лемме 8.5 имеем

$$\frac{ab(n-2)}{m} \in \mathbb{Z}, \quad \frac{ac(n-2)}{m} \in \mathbb{Z}, \quad \frac{bc(n-2)}{m} \in \mathbb{Z}.$$

Следовательно,

$$\frac{ab}{(n+1)^2} \in \mathbb{Z}, \quad \frac{ac}{(n+1)^2} \in \mathbb{Z}, \quad \frac{bc}{(n+1)^2} \in \mathbb{Z}, \quad (9.1)$$

причем

$$a^2 + b^2 + c^2 - abc = -(n-2)(n+1)^2. \quad (9.2)$$

Пусть q – произвольный простой делитель числа $n+1$. Из (9.1) вытекает, что по крайней мере два числа из a, b, c делятся на q , но тогда равенство (9.2) показывает, что и третье из них кратно q .

Это рассуждение доказывает, что $a = \alpha(n+1)$, $b = \beta(n+1)$, $c = \gamma(n+1)$, причем

$$\alpha^2 + \beta^2 + \gamma^2 - (n+1)\alpha\beta\gamma = 2 - n. \quad (9.3)$$

Предположим теперь, что матрица Грама формы $\chi^{(m)}$ высоты $m = -(n-2) \times (n+1)^2$ в некотором базисе равна $M(\alpha(n+1), \beta(n+1), \gamma(n+1))$. Тогда, как мы уже заметили, числа α, β, γ удовлетворяют соотношению (9.3).

На множестве базисов и матрицах Грама формы $\chi^{(m)}$ действует группа кос (1.2). Наша цель – показать, что в орбите этого действия лежит матрица $M(n+1, n+1, n+1)$.

Заметим, что на множестве решений уравнения (9.3) также действует группа кос

$$\begin{array}{ccc} & & ((n+1)\beta\gamma - \alpha, \beta, \gamma) \\ & \nearrow A & \\ (\alpha, \beta, \gamma) & \xrightarrow{B} & (\alpha, (n+1)\alpha\gamma - \beta) \\ & \searrow C & \\ & & (\alpha, \beta, (n+1)\alpha\beta - \gamma) \end{array} \quad (9.4)$$

согласованно с действием (1.2), (1.3) на матрицах Грама. Поэтому нам достаточно показать, что в орбите действия (9.4) лежит решение $(1, 1, 1)$.

Без ограничения общности можно считать, что $\alpha \geq \beta \geq \gamma \geq 1$. Рассмотрим многочлен $f_\alpha(t) = t^2 + \beta^2 + \gamma^2 - (n+1)t\beta\gamma + n - 2$ и оценим его значение в точке β :

$$\begin{aligned} f_\alpha(\beta) &= 2\beta^2 - (n+1)\beta^2\gamma + \gamma^2 + n - 2 \\ &= \beta^2(2 - \gamma) + (\gamma^2 - \beta^2\gamma) + (n - 2 - (n-1)\beta^2\gamma) < 0 \end{aligned}$$

при $\gamma \geq 2$. Значит, перестройка A уменьшает значение α при $\gamma \geq 2$.

Пусть $\gamma = 1$. Тогда $f_\alpha(t) = 2\beta^2 - (n+1)\beta^2 + (n-1) = (n-1)(1 - \beta^2) < 0$ при $\beta > 1$. Поэтому перестройка A уменьшает значение α и при $\gamma = 1$, но $\beta > 1$. Если же $\gamma = \beta = 1$, то получается следующее уравнение для α :

$$\alpha^2 - (n+1)\alpha = -n,$$

которое имеет два корня: n и 1 .

Итак, мы доказали, что существует базис $\varepsilon = (e_1, e_2, e_3)$, в котором матрица Грама формы имеет вид $M((n+1), (n+1), (n+1))$. Прямыми вычислениями проверяется, что преобразование $\mathcal{A}$ с матрицей

$$A = \begin{pmatrix} n+1 & n+1 & 1 \\ -1 & 0 & 0 \\ 0 & -1 & 0 \end{pmatrix}$$

в базисе ε является изометрией формы и $\mathcal{A}^3 = \varkappa$ (матрицу оператора $\varkappa$ см. в (1.4)). Тот факт, что $\mathcal{A}(\mu) = \mathcal{L}_2\mathcal{L}_1$, проверяется прямым вычислением. Предложение доказано.

ПРЕДЛОЖЕНИЕ 9.2. Пусть $\chi^{(m)}$ – полуортогональная форма высоты $m < 0$ на $\mathbb{Z}$ -модуле ранга 3 с дуализирующим оператором $\varkappa$ и $\mathcal{A}(-\mu)$ – образующая подгруппы $\text{Isom}_\infty^+(\chi^{(m)})$. Тогда $\mathcal{A}^3(\mu) = \varkappa$, если и только если $m = -16$ и матрица Грама формы в каком-то базисе равна $M(4, 4, 4)$ или $m = -50$ и матрица Грама есть $M(5, 5, 5)$.

ДОКАЗАТЕЛЬСТВО. Согласно предложению 8.2 ситуация, описанная в формулировке предложения, возможна, лишь когда $\mathcal{I} \in \text{Isom}^+(\chi^{(m)})$. С другой стороны, равенство $\mathcal{A}^3(\mu) = \varkappa$ дает условие $m(n) = (2-n)(n+1)^2$ и вид матрицы Грама: $M(n+1, n+1, n+1)$. Осталось заметить, что по предложению 6.1 из $\mathcal{I} \in \text{Isom}^+(\chi^{(m)})$ вытекает, что $m = -2, -16, -32, -50$, но $m(3) = -16$, $m(4) = -50$ и $m(n) < -50$ при $n > 4$.

ПРЕДЛОЖЕНИЕ 9.3. Пусть $\chi^{(m)}$ – полуортогональная форма высоты $m > 4$ на $\mathbb{Z}$ -модуле ранга 3 с дуализирующим оператором $\varkappa$ и $\mathcal{A}(\mu)$ – образующая подгруппы $\text{Isom}_\infty^+(\chi^{(m)})$. Тогда $\mathcal{A}^3(-\mu) = \varkappa^{-1}$, если и только если $m = (n-1)^2(n+2)$ для некоторого натурального $n \geq 3$ и матрица Грама формы $\chi^{(m)}$ в каком-то базисе имеет вид $M(1-n, 1-n, 1-n)$.

ДОКАЗАТЕЛЬСТВО. Если $\mu = \frac{n}{2} + v\sqrt{m^2 - 4m}$, то по предложению 8.2 высота формы в этом случае представляется формулой $m = f_3 + 2 = n^3 - 3n + 2 = (n-1)^2(n+2)$, $n \geq 3$. Пусть $M(a, b, c)$ – матрица Грама формы χ . Тогда по лемме 8.5 имеем

$$\frac{ab(n+2)}{m}, \frac{ac(n+2)}{m}, \frac{bc(n+2)}{m} \in \mathbb{Z} \iff \frac{ab}{(n-1)^2}, \frac{ac}{(n-1)^2}, \frac{bc}{(n-1)^2} \in \mathbb{Z}.$$

Как и при доказательстве предложения 9.1, можно показать, что эти условия вместе с уравнением для коэффициентов матрицы Грама ($a^2 + b^2 + c^2 - abc = m$) доказывают, что $a = \alpha(n-1)$, $b = \beta(n-1)$, $c = \gamma(n-1)$, причем

$$\alpha^2 + \beta^2 + \gamma^2 - (n-1)\alpha\beta\gamma = n+2. \quad (9.5)$$

Далее потребуется следующая

ЛЕММА 9.4. *Существует базис, в котором матрица Грама формы $\chi^{(m)}$ из предложения 9.3 равна $M(1-n, 1-n, 1-n)$ или $M(\alpha(1-n), \beta(1-n), 0)$, где $\alpha^2 + \beta^2 = n+2$.*

ДОКАЗАТЕЛЬСТВО. Перестройки (1.2), (1.3) матрицы Грама согласованы с перестройками решений уравнения (9.5):

$$\begin{array}{ccc} & & ((n-1)\beta\gamma - \alpha, \beta, \gamma) \\ & \nearrow & \\ (\alpha, \beta, \gamma) & \longrightarrow & (\alpha, (n-1)\alpha\gamma - \beta, \gamma) \\ & \searrow & \\ & & (\alpha, \beta, (n-1)\alpha\beta - \gamma) \end{array}$$

Поэтому для поиска базиса, в котором матрица Грама формы будет иметь наиболее простой вид, достаточно исследовать действие группы кос на множестве решений уравнения (9.5).

Пусть (α, β, γ) – решение этого уравнения и $\alpha\beta\gamma < 0$. Тогда, очевидно, $|\alpha| = |\beta| = |\gamma| = 1$. Если $\alpha\beta\gamma = 0$, то, не ограничивая общности, можно считать, что $\gamma = 0$ и $\alpha^2 + \beta^2 = n+2$.

Покажем, что любое решение уравнения (9.5) переводится перестройками в одно из двух предыдущих. Можно считать, что $\alpha \geq \beta \geq \gamma > 0$. Рассмотрим многочлен $f_\alpha(t) = t^2 + \beta^2 + \gamma^2 - (n-1)t\beta\gamma - (n+2)$ и оценим его значение

$$f_\alpha(\beta) = \beta^2 \left(2 - \frac{n-1}{2}\gamma \right) + \gamma \left(\gamma - \frac{n-1}{2}\beta^2 \right) - (n+2).$$

Легко проверить, что $f_\alpha(\beta) < 0$ для всех $\gamma > 0$ и $n \geq 3$. Поэтому существует перестройка, уменьшающая вес $\alpha + \beta + \gamma$ решения. Следовательно, вместе с любым решением в одной орбите найдется решение, в котором $\gamma = 0$ или $\gamma < 0$. Лемма доказана.

Вернемся к доказательству предложения. Если матрица Грама формы в каком-то базисе ε равна $M(1-n, 1-n, 1-n)$, то матрица $F(-\mu)$ преобразования $\mathcal{A}(-\mu)$ в том же базисе имеет вид

$$F(-\mu) = \begin{pmatrix} 0 & -1 & 0 \\ 0 & 0 & -1 \\ 1 & 1-n & 1-n \end{pmatrix},$$

т.е. принадлежит $GL_3(\mathbb{Z})$. Коэффициенты матрицы вычисляются по формулам (5.6) с учетом следующих предположений: $m = (n-1)^2(n+2)$, $a = b = c = 1-n$, $u = -n/2$, а $v = -1/(2n^2 - 2)$. Последнее равенство получается из вида v (см. определение 8.1).

Предположим, что матрица Грама нашей формы в некотором базисе ε равна $M((n-1)\alpha, (n-1)\beta, 0)$, $\alpha^2 + \beta^2 = n+2$ (можно считать, что $\alpha \neq 0$), и покажем, что в этом случае $\mathcal{A}(-\mu) \notin \text{Isom}_{\infty}^+(\chi^{(m)})$. Для этого достаточно рассмотреть элемент $F_{21}(-\mu)$ (см. (5.6)) матрицы преобразования $\mathcal{A}(-\mu)$ в базисе ε . Поскольку $v = -1/(2n^2 - 2)$, по определению 8.1 имеем

$$F_{21}(-\mu) = 2av = -\frac{\alpha(n-1)}{n^2-1} = -\frac{\alpha}{n+1}.$$

Однако так как $\alpha^2 + \beta^2 = n+2$, то $\alpha \leq \sqrt{n+2}$ и дробь $\alpha/(n+1)$ не может быть целым числом при $n \geq 3$. Предложение доказано.

§ 10. Квадратный корень из дуализирующего оператора

ПРЕДЛОЖЕНИЕ 10.1. Пусть $\chi^{(m)}$ – полуортогональная форма высоты $m < 0$ на $\mathbb{Z}$ -модуле ранга 3, $\varkappa$ – ее дуализирующий оператор, и пусть $\mathcal{A}(\mu)$ – образующая подгруппы $\text{Isom}_{\infty}^+(\chi^{(m)})$. Тогда $\mathcal{A}^2(\mu) = \varkappa$, если и только если $m = 4w^2(2-w^2)$, $w \geq 2$, и матрица Грама формы в некотором базисе ε равна $M(2w^2, 2w, 2w)$. В этом случае $\mathcal{A}(\mu) = \mathcal{L}_1\mathcal{L}_2\mathcal{L}_2$.

ДОКАЗАТЕЛЬСТВО. По предложению 8.2 в этом случае

$$m = 4 - n^2, \quad \mu = \frac{n}{2} + v\sqrt{m^2 - 4m}.$$

Пусть $\mathcal{A}(\mu) \in \text{GL}_3(\mu)$ и $\mathcal{A}^2(\mu) = \varkappa$. Тогда при $\mu = \frac{n}{2} + \frac{p}{2}\sqrt{m_1}$ имеет место равенство $m = 4 - n^2$ (см. предложение 8.2). Далее потребуются следующие вспомогательные утверждения.

ЛЕММА 10.2. Имеем $n \equiv 0 \pmod{2}$.

ДОКАЗАТЕЛЬСТВО. Высота полуортогональной формы есть $m = 4 - n^2$. Если $n \equiv 1 \pmod{2}$, то $m \equiv -1 \pmod{4}$, а полуортогональных форм такой высоты не бывает (см. замечание 1.7).

Учитывая лемму 8.5, получаем

$$\frac{ab}{2+n}, \frac{ac}{2+n}, \frac{bc}{2+n} \in \mathbb{Z}. \quad (10.1)$$

ЛЕММА 10.3. Числа a, b, c четные, и если q – нечетный простой делитель числа $n+2$, то $a \equiv b \equiv c \equiv 0 \pmod{q}$ и $n+2 \equiv 0 \pmod{q^2}$.

ДОКАЗАТЕЛЬСТВО. Поскольку $ab/(n+2) \in \mathbb{Z}$ и n четно, то либо a , либо b четны. Не ограничивая общности, считаем, что $a \equiv 0 \pmod{2}$. Кроме того, $bc/(n+2) \in \mathbb{Z}$. Поэтому один из сомножителей числителя должен быть четным. Пусть, например, b четно.

По определению высоты имеет место соотношение

$$a^2 + b^2 + c^2 - abc = m = -(n-2)(n+2), \quad (10.2)$$

из которого вытекает четность c .

Аналогично проверяется, что $a \equiv b \equiv c \equiv 0 \pmod{q}$ и левая часть равенства (10.2) делится на q^2 . Значит, и $(n-2)(n+2)$ делится на q^2 . Осталось заметить, что $\text{НОД}(n-2, n+2) \in \{2, 4\}$ и $q \notin \{2, 4\}$.

СЛЕДСТВИЕ 10.4. Пусть $2 + n = 2^i k^2$, $i \geq 1$, $k \equiv 1 \pmod{2}$. Тогда

$$a = 2^{j_1} \alpha k, \quad b = 2^{j_2} \beta k, \quad c = 2^{j_3} \gamma k,$$

где $j_1 \geq j_2 \geq j_3 \geq 1$, $\alpha \equiv \beta \equiv \gamma \equiv 1 \pmod{2}$ и

$$2^{2j_1} \alpha^2 + 2^{2j_2} \beta^2 + 2^{2j_3} \gamma^2 - 2^{j_1+j_2+j_3} \alpha \beta \gamma k = -2^i (2^i k^2 - 4). \quad (10.3)$$

Дальше разберем три случая: $i = 1$, $i = 2$ и $i \geq 3$.

Если $i = 1$, то равенство (10.3) приобретает вид

$$2^{2j_1} \alpha^2 + 2^{2j_2} \beta^2 + 2^{2j_3} \gamma^2 - 2^{j_1+j_2+j_3} \alpha \beta \gamma k = -4(k^2 - 2). \quad (10.4)$$

При $j_3 \geq 2$ левая часть уравнения делится на 16, а правая на это число не делится. Следовательно, $j_3 = 1$.

Введем следующие обозначения: $x = 2^{j_1-1} \alpha$, $y = 2^{j_2-1} \beta$, $z = \gamma$, $w = k$. Сокращая равенство (10.4) на 4, получаем диофантово уравнение для x , y , z , w :

$$x^2 + y^2 + z^2 + w^2 - 2xyzw = 2. \quad (10.5)$$

При этом любое решение уравнения (10.5) с нечетными z и w дает решение $a = 2xw$, $b = 2yw$, $c = 2zw$, $n = 2w^2 - 2$ уравнения (10.2), удовлетворяющее условию (10.1).

В случае $i = 2$ соотношение (10.3) имеет вид

$$2^{2j_1} \alpha^2 + 2^{2j_2} \beta^2 + 2^{2j_3} \gamma^2 - 2^{j_1+j_2+j_3} \alpha \beta \gamma k = -2^4(k^2 - 1).$$

Если $j_3 = 1$, то после сокращения на 4 правая часть останется четной, а в левой появится по крайней мере одно нечетное слагаемое γ^2 . Поэтому $j_2 = 1$, $j_1 \geq 2$ и можно утверждать, что

$$2^{2(j_1-1)} \alpha^2 + \beta^2 + \gamma^2 - 2^{j_1} \alpha \beta \gamma k = -4(k^2 - 1).$$

Обозначив $x = 2^{j_1-1} \alpha$, $y = \beta$, $z = \gamma$, $w = 2k$, приходим к диофантову уравнению

$$x^2 + y^2 + z^2 + w^2 - xyzw = 4. \quad (10.6)$$

При этом любое решение уравнения (10.6) с нечетными y и z дает решение $a = xw$, $b = yw$, $c = zw$, $n = w^2 - 2$ уравнения (10.2), удовлетворяющее условию (10.1).

Если $j_3 \geq 2$, то соотношение (10.3) можно сократить на 2^4 :

$$2^{2(j_1-2)} \alpha^2 + 2^{2(j_2-2)} \beta^2 + 2^{2(j_3-2)} \gamma^2 - 2^{j_1+j_2+j_3-4} \alpha \beta \gamma k = -k^2 + 1.$$

Обозначив $x = 2^{j_1-2} \alpha$, $y = 2^{j_2-2} \beta$, $z = 2^{j_3-2} \gamma$, $w = k$, и получим уравнение

$$x^2 + y^2 + z^2 + w^2 - 4xyzw = 1. \quad (10.7)$$

При этом любое решение уравнения (10.7) с нечетным w дает решение $a = 4xw$, $b = 4yw$, $c = 4zw$, $n = 4w^2 - 2$ уравнения (10.2), удовлетворяющее условию (10.1).

Пусть, наконец, $i \geq 3$. Тогда из (10.1) вытекает, что $j_1 + j_2 \geq i$, $j_1 + j_3 \geq i$, $j_2 + j_3 \geq i$, и уравнение (10.3) переписывается следующим образом:

$$2^{2j_1} \alpha^2 + 2^{2j_2} \beta^2 + 2^{2j_3} \gamma^2 - 2^{j_1+j_2+j_3} \alpha \beta \gamma k = -2^{i+2}(2^{i-2} k^2 - 1). \quad (10.8)$$

Заметим, что $2j_3 \leq i + 2$, так как в противном случае, сократив соотношение (10.8) на 2^{i+2} , получим равенство с четной левой и нечетной правой частями.

Если $2j_3 = i + 2$ (т. е. i четно), то после сокращения (10.8) на 2^{2j_3} приходим к соотношению

$$2^{2(j_1-j_3)}\alpha^2 + 2^{2(j_2-j_3)}\beta^2 + \gamma^2 - 2^{j_1+j_2-j_3}\alpha\beta\gamma k = -(2^{i-2}k^2 - 1).$$

В обозначениях $x = 2^{j_1-j_3}\alpha$, $y = 2^{j_2-j_3}\beta$, $z = \gamma$, $w = 2^{(i-2)/2}k$ имеем уравнение

$$x^2 + y^2 + z^2 + w^2 - 4xyzw = 1. \quad (10.9)$$

При этом любое решение уравнения (10.9) с нечетным z дает решение $a = 4xw$, $b = 4yw$, $c = 4zw$, $n = 4w^2 - 2$ уравнения (10.2), удовлетворяющее условию (10.1).

Если $2j_3 < i + 2$, то $j_1 > j_2 = j_3$ и после сокращения (10.8) на 2^{2j_3} имеем

$$2^{2(j_1-j_3)}\alpha^2 + \beta^2 + \gamma^2 - 2^{j_1}\alpha\beta\gamma k = -2^{i+2-2j_3}(2^{i-2}k^2 - 1) = 2^{i+2-2j_3} - 2^{2(i-j_3)}k^2.$$

Пусть $x = 2^{j_1-j_3}\alpha$, $y = \beta$, $z = \gamma$, $w = 2^{i-j_3}k$. Тогда

$$x^2 + y^2 + z^2 + w^2 - 2^{2j_3-i}xyzw = 2^{i+2-2j_3}.$$

Заметим, что $2j_3 - i \geq 0$. Действительно, в противном случае $j_2 + j_3 = 2j_3 < i$, что невозможно. Поскольку мы рассматриваем случай, когда $2j_3 < i + 2$, получаем $0 \leq 2j_3 - i < 2$.

Если $i = 2j_3$, то имеем уравнение

$$x^2 + y^2 + z^2 + w^2 - xyzw = 4,$$

любое решение которого с нечетными y и z дает решение $a = xw$, $b = yw$, $c = zw$, $n = w^2 - 2$ уравнения (10.2), удовлетворяющее условию (10.1).

Если $i + 1 = 2j_3$, то имеем уравнение

$$x^2 + y^2 + z^2 + w^2 - 2xyzw = 2,$$

любое решение которого с нечетными y и z дает решение $a = 2xw$, $b = 2yw$, $c = 2zw$, $n = 2w^2 - 2$ уравнения (10.2), удовлетворяющее условию (10.1).

Подводя итог вычислениям, сформулируем лемму.

ЛЕММА 10.5. *Решение уравнения*

$$a^2 + b^2 + c^2 - abc = -(n - 2)(n + 2),$$

обладающее свойством

$$\frac{ab}{n+2}, \frac{ac}{n+2}, \frac{bc}{n+2} \in \mathbb{Z}, \quad (10.10)$$

однозначно восстанавливается по решениям следующих уравнений:

1) $x^2 + y^2 + z^2 + w^2 - xyzw = 4$, где y и z нечетны, $a = xw$, $b = yw$, $c = zw$, $n = w^2 - 2$;

2) $x^2 + y^2 + z^2 + w^2 - 4xyzw = 1$, где w или z нечетно, $a = 4xw$, $b = 4yw$, $c = 4zw$, $n = 4w^2 - 2$;

3) $x^2 + y^2 + z^2 + w^2 - 2xyzw = 2$, где y и z или z и w нечетны, $a = 2xw$, $b = 2yw$, $c = 2zw$, $n = 2w^2 - 2$.

ЛЕММА 10.6. Множество решений уравнения

$$x^2 + y^2 + z^2 + w^2 - xzyw = 4 \quad (10.11)$$

получается из $(2, 0, 0, 0)$ действием симметрической группы и сменой знака ненулевой координаты, т. е. не дает решения уравнения (10.2), удовлетворяющего свойству (10.10).

ДОКАЗАТЕЛЬСТВО. Заметим, что если (x, y, z, w) – решение уравнения (10.11), то количество отрицательных координат в нем должно быть четным. Кроме того, если у двух координат решения изменить знак, то оно останется решением. Следовательно, можно считать, что $x \geq y \geq z \geq w \geq 0$. Если $w = 0$, то легко видеть, что $x = 2, y = z = 0$.

Пусть $w \geq 1$. Покажем, что если $zw \geq 4$, то (x', y, z, w) , где $x' = yzw - x$, также будет решением, причем $x' < y$.

Тот факт, что (x', y, z, w) – решение, очевиден. Рассмотрим многочлен $f_x(t) = t^2 + y^2 + z^2 + w^2 - tyzw - 4$, корнями которого служат числа x и x' . Чтобы доказать неравенство $x' < y$, достаточно проверить, что $f_x(y) < 0$:

$$f_x(y) = 2y^2 + z^2 + w^2 - y^2zw - 4 = y^2 \left(2 - \frac{zw}{2} \right) + z \left(z - \frac{y^2w}{4} \right) + w \left(w - \frac{y^2z}{4} \right) - 4.$$

При $zw \geq 4$ первая скобка неположительна. Неположительность второй скобки равносильна неравенству $4z \leq y^2w$, которое выполнено, так как $y \geq z$ и $yw \geq zw \geq 4$. Аналогично проверяется, что последняя скобка не больше нуля.

Итак, можно считать, что существует решение, у которого $zw \leq 3$.

Пусть $zw = 3$, т. е. $z = 3, w = 1$. Тогда исходное уравнение записывается в виде

$$x^2 + y^2 - 3xy + 6 = 0,$$

что по модулю 3 имеет вид $x^2 + y^2 \equiv 0 \pmod{3}$. Следовательно, имеем $x \equiv y \equiv 0 \pmod{3}$, $x^2 + y^2 - 3xy \equiv 0 \pmod{9}$, что невозможно.

Пусть $zw = 2$, т. е. $z = 2, w = 1$. Тогда

$$x^2 + y^2 - 2xy = -1,$$

а это уравнение не имеет решений.

Пусть, наконец, $zw = 1$. Тогда

$$x^2 + y^2 - xy = 2 \iff (x - y)^2 + xy = 2,$$

но последнее уравнение не имеет решений в целых числах. Лемма доказана.

ЛЕММА 10.7. Множество решений уравнения

$$x^2 + y^2 + z^2 + w^2 - 4xyzw = 1$$

получается из $(1, 0, 0, 0)$ действием симметрической группы и сменой знака ненулевой координаты, т. е. не дает решения уравнения (10.2), удовлетворяющего свойству (10.10).

ДОКАЗАТЕЛЬСТВО. Как и в лемме 10.6, можно считать, что $x \geq y \geq z \geq w \geq 0$. Покажем, что $x' = 4yzw - x < y$ в новом решении (x', y, z, w) , для чего оценим значение многочлена

$$f_x(y) = 2y^2 + z^2 + w^2 - 4y^2zw - 1 = 2y^2(1 - zw) + z(z - y^2w) + w(w - y^2z) - 1.$$

Видно, что оно отрицательно при $zw \geq 1$.

Следовательно, вместе с любым решением $x \geq y \geq z \geq w \geq 0$ должно существовать решение, у которого $w = 0$, откуда $x = 1, y = z = 0$.

ЛЕММА 10.8. На множестве решений уравнения

$$x^2 + y^2 + z^2 + w^2 - 2xyzw = 2 \quad (10.12)$$

с неотрицательными координатами действует симметрическая группа и группа кос B_3

$$\begin{array}{ccccc} & & (x, y', z, w) & & \\ & & \uparrow & & \\ (x', y, z, w) & \longleftarrow & (x, y, z, w) & \longrightarrow & (x, y, z', w) \\ & & \downarrow & & \\ & & (x, y, z, w') & & \end{array}$$

где $x' = 2yzw - x$, $y' = 2xzw - y$, $z' = 2xyw - z$, $w' = 2xyz - w$. Представители орбит исчерпываются списком $(x, x, 1, 1)$, $x \in \mathbb{Z}_{\geq 0}$, причем старшая координата решения (x, y, z, w) с неотрицательными координатами может быть уменьшена, если $\min\{xy, xz, xw, yz, yw, zw\} > 1$.

ДОКАЗАТЕЛЬСТВО. Без ограничения общности можно считать, что $x \geq y \geq z \geq w \geq 1$. Заметим, что $x' < y$ при $zw \geq 2$. Это следует из неравенства

$$f_x(y) = 2y^2 + z^2 + w^2 - 2y^2zw - 2 = y^2(2 - zw) + z\left(z - \frac{y^2w}{2}\right) + w\left(w - \frac{y^2z}{2}\right) - 2 < 0.$$

Значит, в одной орбите с решением (x, y, z, w) содержится четверка $(x, y, 1, 1)$. Подставив ее в (10.12), получим, что $x = y$.

СЛЕДСТВИЕ 10.9. Если (a, b, c) – решение уравнения (10.2), удовлетворяющее условию (10.1), то

$$a = 2xw, \quad b = 2yw, \quad c = 2zw, \quad n = 2w^2 - 2,$$

где набор (x, y, z, w) получается перестройками и перестановками координат из $(x, x, 1, 1)$.

ЛЕММА 10.10. Пусть $\mu = \frac{n}{2} + v\sqrt{m^2 - 4m}$, $\mathcal{A}^2(\mu) = \kappa$ и $\mathcal{A}(\mu) \in \text{Isom}_{\infty}^+(\chi^{(m)})$. Тогда $v = \frac{1}{2n}$, $m = -(n^2 - 4) = -2w^2(2w^2 - 4)$ и числа

$$\begin{aligned} & \frac{z^2 - 1}{w^2 - 1}, \quad \frac{2xz - x - yzw}{w^2 - 1}, \quad \frac{xzw - y}{w^2 - 1}, \\ & \frac{x - yzw}{w^2 - 1}, \quad \frac{x^2 - z^2}{w^2 - 1}, \quad \frac{xyw - z}{w^2 - 1}, \\ & \frac{y - xzw}{w^2 - 1}, \quad \frac{2x^2z - xyw - z}{w^2 - 1}, \quad \frac{x^2 - 1}{w^2 - 1} \end{aligned} \quad (10.13)$$

должны быть целыми.

ДОКАЗАТЕЛЬСТВО. Поскольку $\mathcal{A}^2(\mu) = \kappa$, то $\mu^2 = \frac{2-m}{2} + \frac{1}{2}\sqrt{m^2 - 4m}$. Возводя μ в квадрат, находим, что $m = -(n^2 - 4)$ и $v = \frac{1}{2n}$. По лемме 8.5 числа

$$\frac{ab(n-2)}{m}, \quad \frac{ac(n-2)}{m}, \quad \frac{bc(n-2)}{m}$$

должны быть целыми, откуда с учетом следствия 10.9 получаем

$$a = 2xw, \quad b = 2yw, \quad c = 2zw, \quad n = 2w^2 - 2,$$

т. е. $m = -2w^2(2w^2 - 4)$. Подставим эти данные в коэффициенты матрицы изометрии $\mathcal{A}(\mu)$ в базисе (e_1, e_2, e_3) (см. (5.6)). Поскольку коэффициенты должны быть целыми, получаем

$$\begin{aligned} F_{11} &= \frac{2w^2(2w^2 - 4) + 4z^2w^2}{2(2w^2 - 2)} + w^2 - 1 + \frac{4z^2w^2(w^2 - 2)}{2w^2(2w^2 - 4)} \\ &= \frac{w^2(z^2 - 2 + w^2)}{w^2 - 1} + w^2 - 1 + z^2 \in \mathbb{Z}. \end{aligned} \quad (10.14)$$

Учитывая, что w^2 и $w^2 - 1$ взаимно просты, находим, что

$$\frac{z^2 - 1}{w^2 - 1} \in \mathbb{Z}.$$

Рассмотрим элемент

$$\begin{aligned} F_{12} &= \frac{8xzw^3 - 4yzw^2 - 4xw}{4(w^2 - 1)} + \frac{(8xzw^3 - 2yzw^2)(2 - w^2)}{-4w^2(w^2 - 2)} \\ &= \frac{w(2xzw^2 - yzw - x)}{(w^2 - 1)} + 2xzw - yz \in \mathbb{Z}. \end{aligned} \quad (10.15)$$

Поскольку $\text{НОД}(w, w^2 - 1) = 1$, то $\frac{2xzw^2 - yzw - x}{w^2 - 1} \in \mathbb{Z}$. Проводя деление в последней дроби с остатком, получим $\frac{2xz - x - yzw}{w^2 - 1} \in \mathbb{Z}$. Далее,

$$F_{13} = \frac{4xzw^2 - 4yw}{4(w^2 - 1)} - \frac{4xzw^2(w^2 - 1)}{-4w^2(w^2 - 2)} = \frac{w(xzw - y)}{w^2 - 1} + xz \in \mathbb{Z}. \quad (10.16)$$

Значит, $\frac{xzw - y}{w^2 - 1} \in \mathbb{Z}$. Рассмотрим следующий элемент:

$$F_{21} = \frac{4xw - 4yzw^2}{4(w^2 - 1)} + \frac{4yzw^2(w^2 - 2)}{-4w^2(w^2 - 2)} = \frac{w(x - yzw)}{w^2 - 1} - yz \in \mathbb{Z}. \quad (10.17)$$

Следовательно, $\frac{x - yzw}{w^2 - 1} \in \mathbb{Z}$. Далее,

$$\begin{aligned} F_{22} &= 1 + \frac{4x^2w^2 - 4z^2w^2}{4(w^2 - 1)} + \frac{(4x^2w^2 + 4z^2w^2)(w^2 - 2)}{-4w^2(w^2 - 2)} \\ &= 1 + \frac{w^2(x^2 - z^2)}{w^2 - 1} - x^2 - z^2 \in \mathbb{Z}. \end{aligned} \quad (10.18)$$

Поэтому $\frac{x^2 - z^2}{w^2 - 1} \in \mathbb{Z}$. Рассмотрим элемент

$$F_{23} = \frac{4xyw^2 - 4zw}{4(w^2 - 1)} + \frac{4xyw^2(w^2 - 2)}{-4w^2(w^2 - 2)} = \frac{w(xyw - z)}{w^2 - 1} - xy \in \mathbb{Z}. \quad (10.19)$$

Отсюда имеем $\frac{xyw - z}{w^2 - 1} \in \mathbb{Z}$. Теперь рассмотрим

$$F_{31} = \frac{4yw - 4xzw^2}{4(w^2 - 1)} - \frac{4xzw^2(w^2 - 2)}{-4w^2(w^2 - 2)} = -\frac{w(y - xzw)}{w^2 - 1} - xz \in \mathbb{Z}, \quad (10.20)$$

откуда получаем $\frac{y-xzw}{w^2-1} \in \mathbb{Z}$. Далее,

$$\begin{aligned} F_{32} &= \frac{4zw - 8x^2zw^3 + 4xyw^2}{4(w^2-1)} - \frac{(8x^2zw^3 - 4xyw^2)(w^2-2)}{-4w^2(w^2-2)} \\ &= \frac{-w(2x^2zw^2 - xyw - z)}{w^2-1} + 2x^2zw - yx \in \mathbb{Z}. \end{aligned} \quad (10.21)$$

В результате имеем $\frac{2x^2z-xyw-z}{w^2-1} \in \mathbb{Z}$. И наконец, рассмотрим

$$\begin{aligned} F_{33} &= \frac{-4w^2(w^2-2) - 4x^2w^2}{4(w^2-1)} + w^2 - 1 - \frac{4x^2w^2(w^2-2)}{-4w^2(w^2-2)} \\ &= -\frac{w^2(w^2-2+x^2)}{w^2-1} + w^2 - 1 + x^2. \end{aligned} \quad (10.22)$$

Значит, $\frac{x^2-1}{w^2-1} \in \mathbb{Z}$.

ЛЕММА 10.11. Числа (10.13) являются целыми тогда и только тогда, когда целыми будут числа

$$\frac{z^2-1}{w^2-1}, \quad \frac{xzw-y}{w^2-1}, \quad \frac{x-yzw}{w^2-1}, \quad \frac{xyw-z}{w^2-1}, \quad \frac{x^2-1}{w^2-1}.$$

Таким образом, доказана следующая

ЛЕММА 10.12. Пусть $\chi^{(m)}$ – полуортогональная форма высоты $m < 0$ на $\mathbb{Z}$ -модуле ранга 3 и $\varkappa$ – ее дуализирующий оператор. Тогда $\sqrt[3]{\varkappa} \in \text{GL}_3(\mathbb{Z})$ (т. е. является изометрией формы), если и только если матрица Грама формы в некотором базисе равна $M(2xw, 2yw, 2zw)$ (в частности, $m = 4w^2(2-w^2)$), где $x^2 + y^2 + z^2 + w^2 - 2xyzw = 2$, причем числа

$$\frac{x^2-1}{w^2-1}, \quad \frac{z^2-1}{w^2-1}, \quad \frac{xzw-y}{w^2-1}, \quad \frac{xyw-z}{w^2-1}, \quad \frac{yzw-x}{w^2-1}$$

являются целыми.

Продолжим доказательство предложения 10.1. По лемме 10.12 матрица Грама формы в некотором базисе (e_1, e_2, e_3) имеет вид $M(2xw, 2yw, 2zw)$, где

$$x^2 + y^2 + z^2 + w^2 - 2xyzw = 2. \quad (10.23)$$

Будем перестраивать базис (e_1, e_2, e_3) . Тогда матрица Грама формы будет меняться по формулам (1.2), (1.3) и одновременно будут перестраиваться первые три компоненты решения (x, y, z, w) уравнения (10.23). Очевидно, что если $(\bar{x}, \bar{y}, \bar{z}, w)$ получено такими перестройками из решения (x, y, z, w) , то числа $\frac{\bar{x}^2-1}{w^2-1}$ и $\frac{\bar{z}^2-1}{w^2-1}$ также должны быть целыми. Покажем, что в орбите таких перестроек обязательно лежит решение $(w, 1, 1, w)$ (с точностью до перестановки первых трех координат).

Поскольку $\frac{x^2-1}{w^2-1} \in \mathbb{Z}$, то $x = 1$ или $x \geq w > 1$. Заметим, что если величина

$$\zeta = \min\{xy, xz, xw, yz, yw, zw\}$$

равна 1, то $\{x, y, z\} = \{w, 1, 1\}$. Пусть $\zeta > 1$. Тогда согласно лемме 10.8 старшая координата уменьшается в результате перестроек. Следовательно, наряду с решением (x, y, z, w) при $x, z \geq w$ должно найтись решение $(\bar{x}, \bar{y}, \bar{z}, w)$

при $\bar{x}, \bar{y}, \bar{z} \leq w$, и тогда $\min\{\bar{x}\bar{y}, \bar{x}\bar{z}, \bar{y}\bar{z}\} = 1$. Итак, матрица Грама формы $\chi^{(m)}$ в некотором базисе ε имеет вид $M(2w^2, 2w, 2w)$. Подставляя в формулы (10.14)–(10.22) значения $x = w, y = z = 1$, получим матрицу A изометрии $\mathcal{A}(\mu)$ в базисе ε :

$$A = F(\mu) = \begin{pmatrix} 2w^2 & 4w^2 - 1 & 2w \\ -1 & 0 & 0 \\ 0 & -2w & -1 \end{pmatrix}.$$

Прямым вычислением можно проверить, что $\mathcal{A}(\mu) = \mathcal{L}_1 \mathcal{L}_2 \mathcal{L}_2$. Предложение доказано.

ПРЕДЛОЖЕНИЕ 10.13. Пусть $\chi^{(m)}$ – полуортогональная форма высоты $m < 0$ на $\mathbb{Z}$ -модуле ранга 3, $\varkappa$ – ее дуализирующий оператор и $\mathcal{A}(-\mu)$ – образующая подгруппы $\text{Isom}_{\infty}^+(\chi^{(m)})$. Тогда $\mathcal{A}^2(-\mu) = \varkappa$, если и только если $m = -32$ и матрица Грама формы в некотором базисе равна $M(4, 8, 4)$.

ДОКАЗАТЕЛЬСТВО. По предложению 8.2 высота формы в этом случае равна $4 - n^2$, а $\mu = \frac{n}{2} + \frac{1}{2n}\sqrt{m^2 - 4m}$. По лемме 10.2 заключаем, что n четно.

По лемме 8.5 получаем, что

$$\frac{ab}{2-n}, \frac{ac}{2-n}, \frac{bc}{2-n} \in \mathbb{Z}. \quad (10.24)$$

Далее потребуются следующие вспомогательные утверждения, доказательства которых аналогичны доказательствам лемм 10.3, 10.5.

ЛЕММА 10.14. Числа a, b, c четные, и если q – нечетный простой делитель числа $n - 2$, то $a \equiv b \equiv c \equiv 0 \pmod{q}$ и $n - 2 \equiv 0 \pmod{q^2}$.

СЛЕДСТВИЕ 10.15. Пусть $n - 2 = 2^i k^2$, $i \geq 1, k \equiv 1 \pmod{2}$. Тогда

$$a = 2^{j_1} \alpha k, \quad b = 2^{j_2} \beta k, \quad c = 2^{j_3} \gamma k,$$

где $j_1 \geq j_2 \geq j_3 \geq 1, \alpha \equiv \beta \equiv \gamma \equiv 1 \pmod{2}$ и

$$2^{2j_1} \alpha^2 + 2^{2j_2} \beta^2 + 2^{2j_3} \gamma^2 - 2^{j_1+j_2+j_3} \alpha \beta \gamma k = -2^i (2^i k^2 + 4).$$

ЛЕММА 10.16. Решение уравнения

$$a^2 + b^2 + c^2 - abc = -(n-2)(n+2), \quad (10.25)$$

обладающего свойством

$$\frac{ab}{n-2}, \frac{ac}{n-2}, \frac{bc}{n-2} \in \mathbb{Z},$$

однозначно восстанавливается по решениям следующих уравнений:

1) $x^2 + y^2 + z^2 + w^2 - xyzw = -4$, где y и z нечетны, $a = xw, b = yw, c = zw, n = w^2 - 2$;

2) $x^2 + y^2 + z^2 + w^2 - 4xyzw = -1$, где w или z нечетно, $a = 4xw, b = 4yw, c = 4zw, n = 4w^2 - 2$;

3) $x^2 + y^2 + z^2 + w^2 - 2xyzw = -2$, где y и z или z и w нечетны, $a = 2xw, b = 2yw, c = 2zw, n = 2w^2 - 2$.

ЛЕММА 10.17. На множестве решений уравнения

$$x^2 + y^2 + z^2 + w^2 - xyzw = -4$$

с положительными координатами группа кос B_3 и симметрическая группа действуют транзитивно. Представителем орбиты является $(4, 2, 2, 2)$.

ДОКАЗАТЕЛЬСТВО. Заметим, что если (x, y, z, w) – решение уравнения, то количество отрицательных координат в нем должно быть четным. Кроме того, если у двух координат решения изменить знак, то оно останется решением. Следовательно, можно считать, что $x \geq y \geq z \geq w \geq 1$.

Покажем, что если $zw \geq 5$ или $zw = 4$, но $y \geq 3$, то (x', y, z, w) при $x' = yzw - x$ также будет решением, причем $x' < y$.

Тот факт, что (x', y, z, w) – решение, очевиден. Рассмотрим многочлен $f_x(t) = t^2 + y^2 + z^2 + w^2 - tyzw + 4$, корнями которого являются числа x и x' . Чтобы доказать неравенство $x' < y$, достаточно проверить, что $f_x(y) < 0$:

$$f_x(y) = 2y^2 + z^2 + w^2 - y^2zw + 4 = y^2\left(2 - \frac{zw}{2}\right) + z\left(z - \frac{y^2w}{4}\right) + w\left(w - \frac{y^2z}{4}\right) + 4.$$

При $zw \geq 5$ имеем $2 - \frac{zw}{2} \leq -\frac{1}{2}$. Кроме того, при $zw \geq 5$ выполнено $y \geq 3$. Следовательно, $y^2\left(2 - \frac{zw}{2}\right) \leq -\frac{9}{2} < -4$. Далее, $4z < y^2w$, так как $y \geq z$ и $yw > 4$. Аналогично, $w - \frac{y^2z}{4} < 0$.

Пусть $zw = 4$, т.е. $z = 4, w = 1$ или $z = w = 2$. В первом случае $y \geq 4$ и мы имеем оценки $z\left(z - \frac{y^2w}{4}\right) = 4\left(4 - \frac{y^2}{4}\right) \leq 0$ и $w\left(w - \frac{y^2z}{4}\right) = 1 - y^2 < -4$. Во втором случае $y \geq 2$ и $z\left(z - \frac{y^2w}{4}\right) = w\left(w - \frac{y^2z}{4}\right) = 2\left(2 - \frac{y^2}{2}\right) \leq 0$, но если $y \geq 3$, то $z\left(z - \frac{y^2w}{4}\right) = w\left(w - \frac{y^2z}{4}\right) < -4$.

Если $y = z = w = 2$, то $x^2 - 8x + 16 = 0$, откуда $x = 4$. Итак, $(4, 2, 2, 2)$ – решение.

Пусть $zw = 3$, т.е. $z = 3, w = 1$. Тогда исходное уравнение записывается в виде

$$x^2 + y^2 - 3xy + 14 = 0.$$

Поскольку $-y^2 + 14 < 0$ при $y \geq 4$, большую координату решения (x, y) можно уменьшить при $y \geq 4$. Если $y = 3$, то уравнение $x^2 - 9x + 23 = 0$ не имеет вещественных корней. Если $y = 2$, то уравнение $x^2 - 6x + 18 = 0$ также не имеет решений. Наконец, при $y = 1$ получаем соотношение $x^2 - 3x + 15 = 0$, которое также неразрешимо.

Пусть $zw = 2$. Тогда уравнение для x и y запишется в виде

$$x^2 + y^2 - 2xy + 9 = 0 \iff (x - y)^2 + 9 = 0$$

и оно не имеет решений.

Если $zw = 1$, то опять приходим к уравнению $x^2 + y^2 - xy + 6 = 0$, не имеющему решений в натуральных числах.

ЛЕММА 10.18. На множестве решений уравнения

$$x^2 + y^2 + z^2 + w^2 - 4xyzw = -1$$

с положительными координатами группа кос B_3 и симметрическая группа действуют транзитивно. Представителем орбиты является $(2, 1, 1, 1)$.

ДОКАЗАТЕЛЬСТВО следует из того факта, что при $x \geq y \geq z \geq w$ старшую координату можно уменьшить, если $zw > 1$ или $zw = 1$, но $y \geq 2$. Для проверки этого высказывания достаточно оценить знак значения многочлена $f_x(y)$:

$$f_x(y) = 2y^2 + z^2 + w^2 - 4y^2zw + 1 = 2y^2(1 - zw) + z(z - y^2w) + w(w - y^2z) + 1 < 0.$$

Если $y = z = w = 1$, то для x получается соотношение $x^2 - 4x + 4 = 0$, откуда следует, что $x = 2$.

ЛЕММА 10.19. *Диофантово уравнение $x^2 + y^2 + z^2 + w^2 - 2xyzw = -2$ не имеет решений.*

ДОКАЗАТЕЛЬСТВО. Можно считать, что $x \geq y \geq z \geq w \geq 1$ в решении (x, y, z, w) . Старшая координата решения может быть уменьшена при $zw \geq 2$, поскольку

$$f_x(y) = 2y^2 + z^2 + w^2 - 2y^2zw + 2 = y^2(2 - zw) + z\left(z - \frac{y^2w}{2}\right) + w\left(w - \frac{y^2z}{2}\right) + 2 < 0.$$

Заметим, что $y(2 - zw) \leq -2$ при $zw > 2$; $\left(z - \frac{y^2w}{2}\right) \leq 0$, поскольку $y \geq z$ и $yw \geq 2$; $w\left(w - \frac{y^2z}{2}\right) < 0$, так как $y \geq w$ и $yz \geq 2$.

Если $zw = 2$, то это влечет за собой $y \geq z = 2$, $w = 1$ и легко проверяется, что $f_x(y) < 0$.

Таким образом, если диофантово уравнение имеет решение, то должно существовать решение, в котором $zw = 1$:

$$4 + y^2 + x^2 - xy = 0 \iff (x - y)^2 + yx = -4,$$

а последнее уравнение не имеет решений в натуральных числах.

В качестве следствия вычислений получаем следующую лемму.

ЛЕММА 10.20. *Если $\mathcal{A}(-\mu) \in \text{Isom}_{\infty}^+(\chi^{(m)})$ и $\mathcal{A}^2(-\mu) = \kappa$, то матрица Грама формы в некотором базисе равна $M(4xw, 4yw, 4zw)$, а высота формы есть $t = -16w^2(w^2 + 1)$, где (x, y, z, w) – решение уравнения*

$$x^2 + y^2 + z^2 + w^2 - 4xyzw = -1.$$

При этом числа

$$\frac{2x^2 + 1}{2w^2 + 1}, \quad \frac{2z^2 + 1}{2w^2 + 1}, \quad \frac{4xyw - 2z}{2w^2 + 1}, \quad \frac{4xzw - 2y}{2w^2 + 1}, \quad \frac{4yzw - 2x}{2w^2 + 1}$$

должны быть целыми.

ДОКАЗАТЕЛЬСТВО. Известно уже, что высота формы должна быть равна $4 - n^2$ с четным n . Если $M(a, b, c)$ – матрица Грама нашей формы в некотором базисе (e_1, e_2, e_3) , то числа a, b, c и n должны удовлетворять уравнению (10.25) и условию (10.24).

Тогда согласно лемме 10.16 числа a, b и c однозначно восстанавливаются из решений одного из трех диофантовых уравнений. Однако одно из них не имеет решений, а решения второго имеют только четные координаты (по лемме 10.16 какие-то компоненты решений должны быть нечетными). Таким образом, a, b и c восстанавливаются по решениям оставшегося уравнения $x^2 + y^2 + z^2 + w^2 - 4xyzw = -1$ по следующей схеме: $a = 4xw$, $b = 4yw$, $c = 4zw$, $n = 4w^2 + 2$.

Элементы матрицы $F(-\mu)$ изометрии $\mathcal{A}(-\mu)$ в базисе (e_1, e_2, e_3) вычисляются по формулам (5.6). Поскольку в нашем случае $-\mu = -\frac{n}{2} - \frac{1}{2n}\sqrt{m^2 - 4m}$, целочисленность элементов матрицы $F(-\mu)$ дает следующие условия. Рассмотрим первый элемент матрицы

$$\begin{aligned} F_{11}(-\mu) &= -\frac{16z^2w^2 + 16w^2(w^2 + 1)}{4(2w^2 + 1)} - 1 - 2w^2 - \frac{16z^2w^2(2w^2 + 2)}{16w^2(w^2 + 1)} \\ &= -\frac{4w^2(z^2 + w^2 + 1)}{2w^2 + 1} - 1 - 2w^2 - 2z^2. \end{aligned}$$

Значит, $\frac{4w^2(z^2 + w^2 + 1)}{2w^2 + 1} \in \mathbb{Z}$. Проводя деление в последней дроби с остатком, получим

$$\frac{2z^2 + 1}{2w^2 + 1} \in \mathbb{Z}. \quad (10.26)$$

Далее,

$$\begin{aligned} F_{12}(-\mu) &= -\frac{64z^2xw^3 - 16yzw^2 - 8xw}{4(2w^2 + 1)} + \frac{(64z^2xw^3 - 16yzw^2)(2w^2 + 2)}{-16w^2(w^2 + 1)} \\ &= -\frac{16z^2xw^2 - 4yzw - 2z}{2w^2 + 1} - (8z^2wx - 2yz). \end{aligned}$$

Следовательно, $\frac{16z^2xw^3 - 4yzw^2 - 2xw}{2w^2 + 1} \in \mathbb{Z}$. Однако так как $\text{НОД}(w, 2w^2 + 1) = 1$, имеем

$$\frac{16z^2xw^2 - 4yzw - 2x}{2w^2 + 1} \in \mathbb{Z}.$$

Проводя здесь деление с остатком, получаем

$$\frac{4yzw + 8z^2x + 2x}{2w^2 + 1} \in \mathbb{Z}. \quad (10.27)$$

Рассмотрим элемент

$$F_{13}(-\mu) = -\frac{16xzw^2 - 8yw}{4(2w^2 + 1)} - \frac{16xzw^2(2w^2 + 2)}{16w^2(w^2 + 1)} = -\frac{4xzw^2 - 2yw}{2w^2 + 1} - 2xz.$$

Учитывая взаимную простоту w и $2w^2 + 1$, получаем

$$\frac{4xzw - 2y}{2w^2 + 1} \in \mathbb{Z}. \quad (10.28)$$

Теперь рассмотрим

$$F_{21}(-\mu) = \frac{16yzw^2 - 8xw}{4(2w^2 + 1)} + \frac{16yzw^2(2w^2 + 2)}{16w^2(w^2 + 1)} = \frac{4yzw^2 - 2xw}{2w^2 + 1} + 2yz,$$

откуда имеем

$$\frac{4yzw - 2x}{2w^2 + 1} \in \mathbb{Z}. \quad (10.29)$$

Далее,

$$\begin{aligned} F_{22}(-\mu) &= 1 - \frac{16(x^2 - z^2)}{4(2w^2 + 1)} + \frac{16w^2(x^2 + z^2)(2w^2 + 2)}{16w^2(w^2 + 1)} \\ &= 1 - \frac{4w^2(x^2 - z^2)}{2w^2 + 1} + 2(x^2 + z^2). \end{aligned}$$

Следовательно, имеем

$$\frac{4(x^2 - z^2)}{2w^2 + 1} \in \mathbb{Z}. \quad (10.30)$$

Рассмотрим элемент

$$F_{23}(-\mu) = -\frac{16xyw^2 - 8zw}{4(2w^2 + 1)} + \frac{16xyw^2(2w^2 + 2)}{16w^2(w^2 + 1)} = -\frac{4xyw^2 - 2zw}{2w^2 + 1} + 2xy,$$

т. е. получаем

$$\frac{4xyw - 2z}{2w^2 + 1} \in \mathbb{Z}. \quad (10.31)$$

Далее, рассмотрим

$$F_{31}(-\mu) = \frac{16xzw^2 - 8yw}{4(2w^2 + 1)} - \frac{16xzw^2(2w^2 + 2)}{16w^2(w^2 + 1)} = \frac{4xzw^2 - 2yw}{2w^2 + 1} - 2xz.$$

Отсюда имеем

$$\frac{4xzw - 2y}{2w^2 + 1} \in \mathbb{Z}. \quad (10.32)$$

Теперь рассмотрим элемент

$$\begin{aligned} F_{32}(-\mu) &= -\frac{8zw - 64x^2zw^3 + 16xyw^2}{4(2w^2 + 1)} - \frac{(64x^2zw^3 - 16xyw^2)(2w^2 + 2)}{16w^2(w^2 + 1)} \\ &= -\frac{w(2z - 16x^2zw^2 + 4xyw)}{2w^2 + 1} - 8x^2zw + 2xy. \end{aligned}$$

После несложных преобразований находим, что

$$\frac{4xzw + 2z + 8x^2z}{2w^2 + 1} \in \mathbb{Z}. \quad (10.33)$$

И наконец, рассмотрим

$$\begin{aligned} F_{33}(-\mu) &= \frac{16w^2(w^2 + 1) + 16x^2w^2}{4(2w^2 + 1)} - 2(w^2 + 1) + 1 - \frac{16x^2w^2(2w^2 + 2)}{16w^2(w^2 + 1)} \\ &= \frac{4(w^4 + w^2 + x^2w^2)}{2w^2 + 1} - 2w^2 - 1 - 2x^2. \end{aligned}$$

Значит, имеем

$$\frac{2w^2 - 2x^2}{2w^2 + 1} \in \mathbb{Z}. \quad (10.34)$$

Осталось заметить, что условия (10.26)–(10.34) равносильны целочисленности дробей, перечисленных в формулировке леммы. Лемма доказана.

Продолжим доказательство предложения 10.13. Предположим, что форма $\chi^{(m)}$ высоты $m < 0$ с матрицей Грама $M(a, b, c)$ в базисе ε обладает изометрией $\mathcal{A}(-\mu)$ и $\mathcal{A}^2(-\mu) = \varkappa$. Тогда $a = 4xw$, $b = 4yw$, $c = 4zw$, $m = -16w^2(w^2 + 1)$ по лемме 10.20, где (x, y, z, w) – решение уравнения $x^2 + y^2 + z^2 + w^2 - 4xyzw = -1$. При этом числа

$$\frac{2x^2 + 1}{2w^2 + 1}, \quad \frac{2z^2 + 1}{2w^2 + 1}, \quad \frac{4xyw - 2z}{2w^2 + 1}, \quad \frac{4xzw - 2y}{2w^2 + 1}, \quad \frac{4yzw - 2x}{2w^2 + 1}$$

принадлежат $\mathbb{Z}$. В частности, $\frac{2x^2 + 1}{2w^2 + 1} \in \mathbb{Z}$, а значит, $x \geq w$.

Заметим, что, перестраивая базис ε с помощью элементов группы кос, мы меняем матрицу Грама формы по формулам (1.2), (1.3), однако форма при этом остается неизменной и (по предположению) обладает изометрией $\mathcal{A}(-\mu)$.

При замене базиса с помощью перестроек решения диофантова уравнения $x^2 + y^2 + z^2 + w^2 - 4xyzw = -1$ синхронно подвергаются перестройкам. Действительно, если $a' = bc - a$, то

$$a' = 16yzw^2 - 4xw = 4w(4yzw - x) = 4wx'.$$

Согласованность остальных перестроек проверяется аналогично.

Таким образом, если $(\bar{x}, \bar{y}, \bar{z}, w)$ получено перестройками из (x, y, z, w) , то число $\frac{2\bar{x}^2+1}{2w^2+1}$ также должно быть целым. Однако если $w > 1$, то существует серия перестроек, ведущая к решению $(\bar{x}, \bar{y}, \bar{z}, w)$, в котором $\bar{x} < w$ (см. лемму 10.18). Таким образом, существование изометрии $\mathcal{A}(-\mu)$ влечет, что высота формы равна -32 , а матрица Грама в некотором базисе равна $M(4, 8, 4)$. Предположение доказано.

ПРЕДЛОЖЕНИЕ 10.21. Пусть $\chi^{(m)}$ – полуортогональная форма высоты $m > 4$ с дуализирующим оператором $\varkappa$, $\mathcal{A}(-\mu)$ – образующая подгруппы $\text{Isom}_\infty^+(\chi^{(m)})$ и $\mathcal{A}(-\mu^2) = \varkappa^{-1}$. Тогда $m = n^2$, матрица Грама формы в некотором базисе ε равна $M(n, 0, 0)$ и $\mathcal{I} \in \text{Isom}^+(\chi^{(m)})$. Формально $\mathcal{A}(-\mu) \notin B_2$.

ДОКАЗАТЕЛЬСТВО. По предложению 8.2 в этом случае высота формы есть $m = n^2$, $\mu = \frac{n}{2} + v\sqrt{m^2 - 4m}$ и $\mathcal{I} \in \text{Isom}^+(\chi^{(m)})$. Значит, по предложению 6.1 матрица формы $\chi^{(m)}$ в некотором базисе ε равна $M(n, 0, 0)$. Необходимо проверить, что коэффициенты матрицы $F(-\mu)$ преобразования $\mathcal{A}(-\mu)$ в базисе ε (см. формулу (5.6)) являются целыми числами. Напомним, что в нашей ситуации $u = -\frac{n}{2}$, $v = -\frac{1}{2n}$, $m = n^2$, $a = n$, $b = c = 0$. Поэтому

$$F(-\mu) = \begin{pmatrix} 0 & 1 & 0 \\ -1 & -n & 0 \\ 0 & 0 & 1 \end{pmatrix} \in \text{SL}_3(\mathbb{Z}).$$

Рассмотрим изометрию $\mathcal{A}'$ с матрицей

$$F' = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & -n \\ 1 & 0 & 0 \end{pmatrix}.$$

Легко проверить, что $\mathcal{A}' = \mathcal{R}_2 \mathcal{R}_1^2$, откуда следует, что $\mathcal{A}(-\mu) \notin B_2$. Предложение доказано.

Список литературы

1. А.Л. Городенцев, “Перестройки исключительных расслоений на $\mathbf{P}^n$ ”, *Изв. АН СССР. Сер. матем.*, **52**:1 (1988), 3–15; англ. пер.: A. L. Gorodentsev, “Transformations of exceptional bundles on $\mathbf{P}^n$ ”, *Math. USSR-Izv.*, **32**:1 (1989), 1–13.
2. С.А. Кулешов, “О многообразии модулей стабильных расслоений на квадрике”, *Матем. заметки*, **62**:6 (1997), 843–864; англ. пер.: S. A. Kuleshov, “On moduli spaces for stable bundles on quadrics”, *Math. Notes*, **62**:6 (1997), 707–725.

3. С. А. Кулешов, Д. О. Орлов, “Исключительные пучки на поверхностях дель Пеццо”, *Изв. РАН. Сер. матем.*, **58**:3 (1994), 53–87; англ. пер.: S. A. Kuleshov, D. O. Orlov, “Exceptional sheaves on del Pezzo surfaces”, *Russian Acad. Sci. Izv. Math.*, **44**:3 (1995), 479–513.
4. А. Н. Рудаков, “Числа Маркова и исключительные расслоения на $\mathbf{P}^2$ ”, *Изв. АН СССР. Сер. матем.*, **52**:1 (1988), 100–112; англ. пер.: A. N. Rudakov, “The Markov numbers and exceptional bundles on $\mathbf{P}^2$ ”, *Math. USSR-Izv.*, **32**:1 (1989), 99–112.
5. J. M. Drezet, J. Le Potier, “Fibrés stables et fibrés exceptionnels sur $\mathbb{P}^2$ ”, *Ann. Sci. École Norm. Sup. (4)*, **18**:2 (1985), 193–243.
6. Д. Ю. Ногин, “Спирали периода четыре и уравнения типа Маркова”, *Изв. АН СССР. Сер. матем.*, **54**:4 (1990), 862–878; англ. пер.: D. Yu. Nogin, “Spirals of period four and equations of Markov type”, *Math. USSR-Izv.*, **37**:1 (1991), 209–226.
7. С. А. Кулешов, А. Н. Рудаков, *Целозначные билинейные формы*, Тр. VI Колмогоровских чтений, ЯГПУ, Ярославль, 2008.
8. З. И. Бореви́ч, И. Р. Шафаревич, *Теория чисел*, 3-е изд., Наука, М., 1985; англ. пер. 1-го изд.: A. I. Borevich, I. R. Shafarevich, *Number theory*, Academic Press, New York–London, 1966.

С. А. КУЛЕШОВ (S. A. KULESHOV)
E-mail: kuleshov@mail.miem.edu.ru

Поступило в редакцию
30.11.2011
10.04.2012