Math-Net.Ru

Общероссийский математический портал

В. Г. Журавлев, Деформации квадратичных диофантовых систем, *Изв. РАН. Сер. матем.*, 2001, том 65, выпуск 6, 15–56

DOI: <https://doi.org/10.4213/im364>

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: 107.22.136.117

26 апреля 2023 г., 10:11:05

УДК 511

В. Г. Журавлев

Деформации квадратичных диофантовых систем

Для матричных квадратичных уравнений введены специализации, сохраняющие инвариантными тип уравнения и формулу веса для представлений квадратичной формы родом положительно определенных форм. Даны приложения к формам кубических решеток и решеток Госсета.

Библиография: 9 наименований.

Введение

0.1. Сечения тернарных форм. Для единичной матрицы $Q = 1_3$ размерности 3 и матрицы $A = \begin{pmatrix} a' & b \\ b & a'' \end{pmatrix}$ рассмотрим уравнение

$$Q[X] = {}^t X Q X = A, \quad (0.1)$$

где $X = (x, y)$ и переменные в ${}^t x = (x_1, x_2, x_3)$, ${}^t y = (y_1, y_2, y_3)$ принимают значения из кольца целых чисел $\mathbb{Z}$. Для разрешимости уравнения (0.1) необходимо, чтобы матрица A была положительно полуопределенной. Ограничимся строго определенной матрицей A , когда диагональные элементы a' , a'' и определитель $|A| = a'a'' - b^2$ больше нуля. В координатах x_i, y_i уравнение (0.1) принимает вид квадратичной системы уравнений

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= a', & y_1^2 + y_2^2 + y_3^2 &= a'', \\ x_1 y_1 + x_2 y_2 + x_3 y_3 &= b. \end{aligned} \quad (0.2)$$

Эта система имеет конечное число решений $n(A, 1_3)$. Обозначим a уровень матрицы A – наименьшее положительное целое число такое, что матрица aA^{-1} имеет целые коэффициенты. Если определитель $|A|$ матрицы A совпадает с ее степенью a и a – четное бесквадратное число, то для $n(A, 1_3)$ выполняется формула [1, с. 102]

$$n(A, 1_3) = 24 \prod_{\substack{p|a \\ p \neq 2}} (1 + \varepsilon_p), \quad (0.3)$$

где p пробегает нечетные простые делители степени a , $\varepsilon_p = \varepsilon_1(A) \left(\frac{-1}{p}\right)$, $\left(\frac{*}{p}\right)$ – символ Лежандра и знак $\varepsilon_1(A) = \left(\frac{A_1}{p}\right)$ определяется из жорданова разложения в прямую сумму над кольцом целых p -адических чисел $\mathbb{Z}_p$ [5, с. 132]:

$$A \sim {}_{\mathbb{Z}_p} A_1 \oplus p^\alpha A_{p^\alpha}. \quad (0.4)$$

Работа выполнена при финансовой поддержке РФФИ (грант № 99-01-00070).

Рассмотрим диагональную матрицу $A = \begin{pmatrix} a' & 0 \\ 0 & a'' \end{pmatrix}$ с бесквадратными взаимно простыми элементами a' , a'' , причем a'' четное. В этом случае система

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= a', & y_1^2 + y_2^2 + y_3^2 &= a'', \\ x_1 y_1 + x_2 y_2 + x_3 y_3 &= 0 \end{aligned} \quad (0.5)$$

согласно формуле (0.3) имеет число решений

$$n(A, 1_3) = 24 \prod_{p'|a'} \left(1 + \left(\frac{-a''}{p'}\right)\right) \prod_{\substack{p''|a'' \\ p'' \neq 2}} \left(1 + \left(\frac{-a'}{p''}\right)\right). \quad (0.6)$$

Пусть сначала $a' = 1$. Группа целых автоморфизмов $O_{\mathbb{Z}}(1_3)$ квадратичной формы с единичной матрицей $Q = 1_3$ имеет порядок $o(1_3) = 48$. Уравнение $x_1^2 + x_2^2 + x_3^2 = 1$ имеет шесть решений, образующих одну орбиту с представителем ${}^t x = (0, 0, 1)$. Подставляя ${}^t x$ в систему (0.5), приходим к задаче о представлении целых чисел суммой двух квадратов:

$$y_1^2 + y_2^2 = a''. \quad (0.7)$$

Все шесть решений порождают уравнение такого же типа. Поэтому число решений $n(a'', 1_2)$ уравнения (0.7) и число решений системы (0.5) связаны равенством

$$n(A, 1_3) = 6n(a'', 1_2). \quad (0.8)$$

Из (0.6) и (0.8) вытекает известная формула для суммы двух квадратов:

$$n(a'', 1_2) = 4 \sum_{\substack{p''|a'' \\ p'' \neq 2}} \left(1 + \left(\frac{-1}{p''}\right)\right) = 4 \prod_{\substack{\delta|a'' \\ \delta \text{ нечет}}} \chi_{-1}(\delta), \quad (0.9)$$

где $\chi_{-1}(\delta) = \left(\frac{-1}{\delta}\right) = (-1)^{(\delta-1)/2}$ – характер Дирихле по модулю 4.

Выберем $a' = 3$, а $a'' = 2a_1$ четным бесквадратным, не делящимся на 3. Восемь решений уравнения $x_1^2 + x_2^2 + x_3^2 = 3$ образуют одну орбиту и получаются из ${}^t x = (1, 1, 1)$ всевозможными переменами знаков. Подставляем ${}^t x$ в систему (0.5) и приходим к задаче

$$2y_1^2 + 2y_1 y_2 + 2y_2^2 = a'' \quad (0.10)$$

о представлении числа a'' бинарной положительно определенной квадратичной формой с матрицей $K' = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, имеющей определитель $|K'| = 3$. Теперь для числа решений $n(a'', K')$ уравнения (0.10) выполняется соотношение $n(A, 1_3) = 8n(a'', K')$, и (0.6) приводит к другой известной формуле:

$$n(a'', K') = 6 \prod_{\substack{p''|a'' \\ p'' \neq 2}} \left(1 + \left(\frac{-3}{p''}\right)\right) = 6 \sum_{\delta|a_1} \chi_{-3}(\delta); \quad (0.11)$$

здесь $\chi_{-3}(\delta) = \left(\frac{\delta}{3}\right)$ – характер Дирихле по модулю 3.

Диагональные специализации $A = \begin{pmatrix} a' & 0 \\ 0 & a'' \end{pmatrix}$ матричного уравнения (0.1) приводят к однородным квадратичным формам (0.7), (0.10). Выбор матрицы $A = \begin{pmatrix} 3 & b \\ b & a'' \end{pmatrix}$ с $b \neq 0$ приводит к неоднородному квадратичному уравнению

$$y_1^2 + y_1 y_2 + y_2^2 + b y_1 + b y_2 + e = 0. \quad (0.12)$$

Если $b^2 - 3e > 0$ – нечетное бесквадратное число, не делящееся на 3, то уравнение (0.12) согласно формуле (0.3) имеет число решений, равное

$$n(b, e; K'_{\text{неодн}}) = 3 \sum_{\delta | b^2 - 3e} \chi_{-3}(\delta).$$

Теперь разрешимость и число решений уравнения (0.12) определяются мультипликативным разложением выражения $b^2 - 3e$.

Итак, специализации A квадратичной системы уравнений (0.2) приводят к квадратичным уравнениям для форм K' меньшего числа переменных. При этом правая часть формулы (0.3) переформулируется в терминах инвариантов дополнительных квадратичных форм K' , отождествляемых с их матрицами. Для неоднородных квадратичных бинарных форм (0.12) естественным объемлющим пространством является трехмерное, они получаются сечением кубической решетки $\mathbb{Z}^3$. Общая формула (0.3) для тернарной формы $Q = 1_3$ содержит в себе бесконечное множество частных формул представлений чисел бинарными квадратичными формами K' . Это в точности формы подрешеток $L_{K'} \subset \mathbb{Z}^3$, ортогональных векторам x , имеющим норму $Q[x] = a'$. Так как решетка $\mathbb{Z}^3$ унимодулярная, то дополнительные формы имеют определитель $|K'| = a'$. Отсюда можно сделать вывод: $|K'| \not\equiv 7 \pmod{8}$, поскольку числа $a' \equiv 7 \pmod{8}$ не представимы суммой трех квадратов.

Под знаком сумм (0.9), (0.11) стоят характеры квадратичных полей $\mathbb{Q}(\sqrt{-1})$, $\mathbb{Q}(\sqrt{-3})$. Различные квадратичные поля и их характеры, квадратичные формы, однородные и неоднородные, объединены одной решеткой $\mathbb{Z}^3$.

0.2. Формы высших размерностей. Уравнение (0.1) является частным случаем матричного уравнения

$$Q[X] = {}^t X Q X = A, \quad X \in \text{Mat}_{n,m}(\mathbb{Z}), \quad (0.13)$$

где $Q = 1_n$ – единичная матрица n -го порядка, A – симметричная матрица m -го порядка, $m < n$, и X пробегает множество целых $(n \times m)$ -матриц.

В настоящей статье рассматриваются специализации A , переводящие уравнения (0.13) в уравнения того же типа (ср. (0.7), (0.10)):

$$K'[Y] = A'', \quad (0.14)$$

и сохраняющие *формулу веса* [1]

$$\frac{n(A, Q)}{o(Q)} = \text{std}(n - m) \alpha_2(A, Q) \prod_{\substack{p | |A| \\ p \neq 2}} \alpha_p(A, Q). \quad (0.15)$$

Здесь $n(A, Q)/o(Q)$ – вес представлений формы A формой Q , $n(A, Q)$ – число решений уравнения (0.13), $o(Q)$ обозначает порядок группы целых автоморфизмов формы Q . Функция $\text{std}(n - m)$ зависит только от разности размерностей $n - m$, и все множители в правой части (0.15) явно вычисляются (ср. (0.3)). Специализация $A = \begin{pmatrix} A' & 0 \\ 0 & A'' \end{pmatrix}$ с фиксированным блоком A' переводит, с точностью до некоторого множителя, равного числу склеивающих A' с K' векторов, формулу (0.15) в формулу веса

$$\frac{n(A'', K')}{o(K')} = \text{std}(n - m) \alpha_2(A'', K') \prod_{\substack{p \mid |K'| \cdot |A''| \\ p \neq 2}} \alpha_p(A'', K') \quad (0.16)$$

представлений формы A'' квадратичной формой K' решетки $L_{K'}$, ортогональной некоторому представлению X' : $Q[X'] = A'$ (избегая усложнений, считаем род $[K']$ одноклассным).

Приведенную конструкцию поясним примером из § 8, выбирая единичную матрицу $Q = 1_6$ и тернарную форму A , имеющую бесквадратный определитель. Тогда вес представлений выражается формулой

$$\frac{n(A, 1_6)}{o(1_6)} = \frac{1}{6} \alpha_2(A, Q) \prod_{\substack{p \mid |A| \\ p \neq 2}} (p + \varepsilon_1(A)), \quad (0.17)$$

где $\varepsilon_1(A)$ – знак единичной составляющей A_1 жорданова разложения A (0.4) над кольцом $\mathbb{Z}_p$. Специализацией выберем форму $A = \begin{pmatrix} A' & 0 \\ 0 & A'' \end{pmatrix}$ с одномерным блоком $A' = 14$. Решения $x = (x_1, \dots, x_6)$ уравнения $x_1^2 + \dots + x_6^2 = 14$ распадаются на три орбиты с представителями (123000), (112220), (111113). Ортогональные дополнения к ним – формы с матрицами Грама K'_1, K'_2 и

$$K' = \begin{pmatrix} 2 & 1 & 1 & 1 & 0 \\ 1 & 2 & 1 & 1 & 0 \\ 1 & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 4 \end{pmatrix}.$$

Первые две нечетные формы образуют род $[K'_{\text{нечет}}]$, а последняя, четная, форма – род $[K'_{\text{чет}}]$. В п. 0.1 рассмотрены одноорбитные решения x . Случай существования нескольких орбит – более сложный и требует разделения родов. Формула веса (0.17) позволяет это сделать, и после выделения рода $[K'_{\text{чет}}]$ она преобразуется к виду

$$n(A'', K') = 5 \left(7 + \left(\frac{|A''|}{7} \right) \right) \prod_{p \mid |A''|} \left(p + \varepsilon_1(A'') \left(\frac{14}{p} \right) \right). \quad (0.18)$$

Здесь $n(A'', K')$ – число решений $Y \in \text{Mat}_{5,2}(\mathbb{Z})$ матричного уравнения $K'[Y] = A''$ (0.14), $\varepsilon_1(A'') = \left(\frac{|A''|}{p} \right)$ – знак блока A''_1 из жорданова разложения $A'' \sim_{\mathbb{Z}_p} A''_1 \oplus p^\alpha A''_{p^\alpha}$.

Другая специализация

$$A = \begin{pmatrix} A' & B \\ {}^tB & A'' \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & b \\ 0 & b & c \end{pmatrix}, \quad b \neq 0,$$

приводит нас к неоднородной квадратичной форме. Теперь множество решений $X' \in \text{Mat}_{6,2}(\mathbb{Z})$ матричного уравнения $Q[X'] = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ имеет одну орбиту,

$${}^tX' = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}$$

— ее представитель. Предположим, что $b^2 - 3e > 0$ — нечетное бесквадратное число, не делящееся на 3. Тогда (0.17) преобразуется в формулу

$$n(b, e; K'_{\text{неодн}}) = \left(2 - \left(\frac{-1}{b^2 - 3e} \right) \right) \prod_{p|b^2 - 3e} \left(p + \left(\frac{3}{p} \right) \right). \quad (0.19)$$

Здесь $n(b, e; K'_{\text{неодн}})$ — число целых решений $y = (y_1, \dots, y_4) \in \mathbb{Z}^4$ неоднородного уравнения (ср. (0.11))

$$y_1^2 + y_2^2 + y_3^2 + 3y_4^2 + 2by_4 + e = 0.$$

Формула веса (0.17) не является жесткой структурой. Формулы (0.18), (0.19) представляют ее различные вариации. Изолированные квадратичные уравнения и системы оказываются сечениями одной базисной системы (0.13).

0.3. История вопроса. Дж.Конвей и Н.Слоэн [7] применили метод дополнения для конструирования квадратичных форм из известных форм меньшей размерности, являющийся обращением метода склейки Витта–Кнезера. Выдающимся результатом применения метода склейки является список Нимейера всех четных унимодулярных форм размерности 24. Локальный вариант метода склейки применен в работах [2]–[4] к нахождению числа решений матричных уравнений (0.13) для форм Q и A с не взаимно простыми определителями $|Q|$ и $|A|$.

Цель статьи состоит в следующем:

- 1) получить с помощью специализаций $A = \begin{pmatrix} A' & * \\ * & A'' \end{pmatrix}$ сечения матричных уравнений $Q[X] = A$ для квадратичных форм Q кубических решеток $\mathbb{Z}^n$ и решетки Госсета E_8 — четной восьмимерной унимодулярной решетки;
- 2) показать, как эти специализации приводят нас к формулам числа целых представлений $n(A'', K')$ форм A'' соответствующими сечениями K' .

0.4. Содержание. В ч. I рассматриваются минимальные локальные вложения форм A в Q над $\mathbb{Z}_p$. Если определители $|A|$ и $|Q|$ взаимно простые, вложения для нечетных p задаются изоморфизмами между дискриминантными формами A^{-1} и $K^{-1} \bmod \mathbb{Z}_p$ и ортогональные дополнения K определяются однозначно формами A и Q (§ 2). При наличии общих делителей $|A|$ и $|Q|$ имеет место ветвление вложений. Само ветвление и его арифметические приложения изложены в [2]–[4].

Трудности представляют вложения форм над четным кольцом $\mathbb{Z}_2$, ветвящиеся даже в условиях взаимной простоты определителей (§ 3, 4). В следующих двух параграфах определяются ортогональные дополнения K и инверсные к ним формы G , входящие в формулу веса, для квадратичных форм Q кубических решеток $\mathbb{Z}^n$ размерностей $n \leq 8$ и решетки Госсета E_8 . Найдены одноклассные формы K для вложений одномерных и двумерных форм A , имеющих небольшие определители.

В ч. II рассматриваются преобразования квадратичных систем и формул веса представлений. В § 7, 8 приводятся примеры конкретных диофантовых систем и обсуждается связь неоднородных квадратичных уравнений с проблемой близнецов. С помощью теории склейки, по-видимому, можно доказать, что ортогональные дополнения $K' \perp X'$ представлений $X': Q_i[X'] = A'$ для всех форм Q_i рода $[Q]$ образуют полный род $[K']$.

Полнота рода доказывается в § 9 для одноклассных форм A и для суммы квадратов Q . Применяемый метод дает, как следствие, доказательство линейной независимости тета-рядов $\theta^{k-1}(Z, K'_i)$ рода $k-1$ и веса $k/2$, другим методом полученную в [8]. В ходе доказательства возникла идея о существовании орбитальной масс-формулы (см. (10.16)) для взвешенной суммы числа орбит $\{X'\}$ представлений $Q[X'] = A'$ с ортогональными дополнениями $K' \perp X'$ из рода $[K']$. Простое доказательство этой формулы получается использованием одной конструкции из [1]. Попутно вычисляется коэффициент пропорциональности $c(A', Q; G')$, появляющийся в масс-формуле и в процессе деформации веса представлений форм (лемма 10.1). Как уже отмечалось, $c(A', Q; G')$ равно числу склеивающих A' и K' векторов. Формула (11.2)

$$o(K') = c(A', Q; G') \text{stab}(X'),$$

где $\text{stab}(X')$ – порядок стабилизатора представления X' в группе автоморфизмов $O_{\mathbb{Z}}(Q)$, указывает дополнительно на алгебраическое значение векторов склейки (ср. [7, с. 28]): они отвечают за подъем автоморфизмов из стабилизатора $\text{Stab}(X')$ в полную группу автоморфизмов $O_{\mathbb{Z}}(K')$. В заключительном § 12 в связи с одноклассными формами Ватсона [9] обсуждается способ восстановления рода $[K']$ по одному его представителю.

0.5. Обозначения:

$\mathbb{Z}, \mathbb{Z}_p$ – целые рациональные и p -адические числа;

$\left(\frac{\cdot}{p}\right)$ – символ Лежандра;

$|Q|$ – определитель квадратичной формы Q ;

$h(Q)$ – число классов $\{Q\}$ рода $[Q]$;

$\sim, \sim_p$ – эквивалентность форм над $\mathbb{Z}$ и $\mathbb{Z}_p$;

$A' \oplus A'', A' \overset{[\cdot]}{\oplus} A''$ – прямая сумма и склейка форм A' и A'' ;

$A = A_1 \oplus A_{\geq p}$ – жорданово разложение формы A над $\mathbb{Z}_p$;

$J(A) = A_1 \oplus J(A_{\geq p}), J(A_{\geq p}) = \begin{pmatrix} A_{\geq p} & 1 \\ 1 & 0 \end{pmatrix}$ – минимальные вложения A ;

$Q' = Q \ominus A$, если $A \oplus Q' \sim_p Q$;

Q_I, Q_{II} – нечетная и четная формы;

$K' \perp X', \{X'\} \rightarrow \{K'\}$ – ортогональное дополнение к $X': Q[X'] = A'$;

$\mathbb{Z}^n$ – кубическая n -мерная решетка;
 A_n, D_n – решетка с нулевой суммой и шахматная решетка;
 E_6, E_7, E_8 – решетки Госсета.

Часть I. Локальные минимальные вложения. Одноклассные формы

§ 1. Примитивные вложения решеток

1.1. Пусть R – кольцо целых рациональных чисел $\mathbb{Z}$ или p -адических чисел $\mathbb{Z}_p$, Q и A – целые симметрические невырожденные матрицы размеров $n > m \geq 1$ с определителями $|Q| = \det Q$ и $|A| = \det A$. Отождествим матрицы Q, A с определяемыми ими квадратичными формами. Форма A *примитивно представима формой* Q , если существует целая $(n \times m)$ -матрица b с условием

$$Q[b] = {}^t b Q b = A,$$

при этом b *примитивна*, т.е. наибольший общий делитель ее миноров порядка m равен единице кольца R . Свойство примитивности равносильно существованию расширенной матрицы $B = (b \mid e)$ из унимодулярной группы $\mathrm{SL}_n^\pm(R)$, и, следовательно, форма Q *эквивалентна относительно $\mathrm{SL}_n^\pm(R)$ целой форме*

$$Q_B = Q[B] = \begin{pmatrix} A & C \\ {}^t C & Q' \end{pmatrix}.$$

Преобразование, вообще говоря, рациональное, $M_C = \begin{pmatrix} 1 & -A^{-1}C \\ 0 & 1 \end{pmatrix}$ разлагает Q_B в прямую сумму форм A и $G' = Q' - A^{-1}[C]$:

$$Q_B[M_C] = \begin{pmatrix} A & 0 \\ 0 & G' \end{pmatrix} = A \oplus G'. \quad (1.1)$$

Умножим равенство (1.1) на *ступень* a формы A и получим разложение

$$aQ_B[M_C] = \begin{pmatrix} aA & 0 \\ 0 & G \end{pmatrix}, \quad (1.2)$$

где $G = aQ' - E[C]$ – целая симметрическая невырожденная матрица порядка $k = n - m > 0$ и матрица $E = aA^{-1}$ также целая. Блок Q' целый, поэтому C содержится во множестве c_G^A решений матричного уравнения

$$E[C] \equiv -G \pmod{a}, \quad C \in M_{m,k}(R). \quad (1.3)$$

Обратно, для произвольного решения C форма

$$Q_G^A(C) = \frac{1}{a} \begin{pmatrix} aA & 0 \\ 0 & G \end{pmatrix} [M_C^{-1}] = \begin{pmatrix} A & C \\ {}^t C & \frac{1}{a}(E[C] + G) \end{pmatrix} \quad (1.4)$$

будет целой, эквивалентной исходной форме Q . Из разложения (1.2) вытекает независимость определителя

$$|G| = a^{n-m} |Q| / |A| \quad (1.5)$$

формы G от выбора примитивного представления b .

1.2. Пусть

$$Q = Q_G^A(C) = \begin{pmatrix} A & C \\ {}^tC & Q' \end{pmatrix} \quad (1.6)$$

с целым блоком $Q' = \frac{1}{a}(E[C] + G)$. Два решения C и C' , $C \equiv C' \pmod{A}$, дают эквивалентные формы $Q \sim Q'$. Примитивному представлению формы A отвечает примитивное вложение решетки

$$M_A = \left\{ x = \begin{pmatrix} x' \\ 0 \end{pmatrix} : x' \in M_{m,1}(R) \right\} \xrightarrow{\text{em}} M_Q = M_{n,1}(R)$$

с сохранением значений квадратичных форм $Q[x] = A[x']$. *Примитивность* вложения означает, что R -модуль M_Q/M_A свободный. Обозначим $M_K = M_A^\perp$ ортогональную к M_A подрешетку из M_Q . То, что $y \in M_K$, согласно (1.6) равносильно условию, что y имеет вид

$$y = \begin{pmatrix} y' \\ y'' \end{pmatrix}, \quad \text{где } y' = -A^{-1}Cy''. \quad (1.7)$$

Определим подрешетку L из $M = M_{k,1}(R)$, состоящую из решений матричного сравнения

$$A^{-1}C \cdot X \equiv 0 \pmod{1}. \quad (1.8)$$

Так как имеют место включения $aM \subset L \subset M$, то $\dim L = \dim M$. Выберем некоторый базис подрешетки L в качестве столбцов матрицы B . Тогда $L = BM$ и в силу (1.7) и (1.8) $M_K = \begin{pmatrix} -A^{-1}C \\ 1 \end{pmatrix} BM$, матрица $B_1 = A^{-1}CB$ целая и $CB = AB_1$. Используя выбранный базис, (1.4) и (1.6), находим для решетки M_K ее матрицу Грама

$$K = \frac{1}{a}G[B]. \quad (1.9)$$

Определитель $|K|$ – целое число, и по формуле (1.5)

$$|K| = |Q| \cdot |B|^2 / |A|. \quad (1.10)$$

Согласно (1.6) ${}^tCA^{-1}C \equiv -\frac{1}{a}G \pmod{1}$. Из сравнений

$$\frac{1}{a}GB \equiv -{}^tCA^{-1}CB \equiv -{}^tCB_1 \equiv 0 \pmod{1}$$

видно, что матрица $U = \frac{1}{a}GB$ целая, а ее определитель по формуле (1.5) равен $|U| = |Q| \cdot |B| / |A|$. Из последнего равенства выразим матрицу B . Подставляя ее в формулу (1.9), получим

$$K = aG^{-1}[U], \quad |K| = |A| \cdot |U|^2 / |Q|. \quad (1.11)$$

1.3. Пусть $R = \mathbb{Z}_p$ – локальное кольцо. В [1] доказано, что определитель $|U|$ целой матрицы U делит в кольце $\mathbb{Z}_p$ определитель $|Q|$, если p не делит $|Q|$. Таким образом, в этом случае из равенства (1.11) вытекает эквивалентность над $\mathbb{Z}_p$:

$$K \sim_p aG^{-1}, \quad \text{если } p \nmid |Q|. \quad (1.12)$$

Предположим, что определители $|A|$ и $|Q|$ взаимно простые. Если p не делит $|Q|$, то по (1.11)

$$|K| \sim_p |A|/|Q| \sim_p |A| \cdot |Q|.$$

Сокращение $a \sim_p a'$ означает, что $a = \varepsilon^2 a'$ для некоторой единицы ε из $\mathbb{Z}_p^\times$. Если же p делит $|Q|$, то $p \nmid |A|$ и в силу определения (1.8) подрешетка L совпадает со всей решеткой M . Матрицу B можно выбрать единичной, и по (1.10) снова получим $|K| \sim_p |A| \cdot |Q|$. Отсюда вытекает равенство

$$|K| = |A| \cdot |Q|, \quad (1.13)$$

если $|A|$ и $|Q|$ не имеют общих делителей.

§ 2. Вложения над нечетным локальным кольцом

2.1. В этом параграфе p будет нечетным простым числом, не делящим $|Q|$. По теории приведения над $\mathbb{Z}_p$ [5, с.131] будем полагать

$$A = A_1 \oplus A_{\geq p},$$

где блок A_1 имеет максимальную размерность с условием $|A_1| \not\equiv 0 \pmod{p}$. Обозначим $a = p^\alpha$ степень формы A над $\mathbb{Z}_p$. При этих предположениях целая форма G из сравнения (1.3) должна удовлетворять ограничению [1, (6.14)]

$$G \sim_p \begin{pmatrix} -aA_{\geq p}^{-1} & 0 \\ 0 & 0 \end{pmatrix} \pmod{a}.$$

Поэтому будем считать

$$G = G_{<a} \oplus aG_a \quad \text{с блоком } G_{<a} = -aA_{\geq p}^{-1}. \quad (2.1)$$

2.2. Множество $C_G^A = c_G^A / \text{mod } A$ содержит единственную *орбиту* $\{C\}$ из классов $CS / \text{mod } A$, где S пробегает группу целых автоморфизмов $O_{\mathbb{Z}_p}(G)$. В терминах примитивных представлений $Q[X] = A$ все решения X образуют одну $O_{\mathbb{Z}_p}(Q)$ -орбиту $\{X\}$ над кольцом $\mathbb{Z}_p$. Согласно (1.3) орбита $\{C\}$ содержит представителя $C = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$, и тогда по (1.6) форма Q распадается в следующую прямую сумму:

$$Q = Q_G^A(C) = \begin{pmatrix} A_1 & 0 & 0 & 0 \\ 0 & A_{\geq p} & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & G_a \end{pmatrix} = A_1 \oplus J(A_{\geq p}) \oplus G_a, \quad (2.2)$$

где $J(A_{\geq p}) = \begin{pmatrix} A_{\geq p} & 1 \\ 1 & 0 \end{pmatrix}$ – минимальное вложение формы $A_{\geq p} \equiv 0 \pmod{p}$.

2.3. Будем говорить, что квадратичные формы X и Y удовлетворяют неравенству $Y \leq X$, если $X \sim_p Y \oplus Z$ для некоторой формы Z . Разность $X \ominus Y$ обозначает любую из форм Z , определяемую формами X и Y однозначно (с точностью до эквивалентности над $\mathbb{Z}_p$) для нечетного p и, в общем случае, неоднозначно для $p = 2$. Таким образом, условие $Y \leq X$ равносильно существованию разности форм $X \ominus Y$.

2.4. Обозначим $J(A)$ прямую сумму форм $A_1 \oplus J(A_{\geq p})$. Из разложения (2.2) вытекает

ПРЕДЛОЖЕНИЕ 2.1 [4]. *Если p нечетное и p не делит определитель $|Q|$, то форма A примитивно представима над $\mathbb{Z}_p$ формой Q только в том случае, когда выполнено неравенство $J(A) \leq Q$.*

Кроме того, разложения (2.1) и (2.2) показывают, что, с точностью до эквивалентности $\sim_p$, форма G однозначно определяется формами A и Q . Для нее имеет место разложение

$$G = -aA_{\geq p}^{-1} \oplus a(Q \ominus J(A)). \quad (2.3)$$

Аналогичное разложение можно записать и для формы $K = A^\perp$ (см. п. 1.2), ортогональной к A . Поскольку $(Q \ominus J(A))^{-1} \sim_p Q \ominus J(A)$, то из (1.11) и (2.3) заключаем:

$$K = (Q \ominus J(A)) \oplus (-A_{\geq p}). \quad (2.4)$$

§ 3. Вложение над кольцом $\mathbb{Z}_2$: одномерный случай

Представления A формой Q над четным кольцом $\mathbb{Z}_2$ начинают ветвиться и сильно зависят от характеристик форм A и Q . Выясним условия существования примитивных представлений для форм A с жордановыми составляющими A_q , $q \geq 2$, небольших размерностей.

3.1. Пусть $p = 2$ не делит $|Q|$ и $a = 2^\alpha$ будет степенью формы $A = A_1 \oplus A_{\geq p}$. В сравнении (1.3) $C \bmod A$ можем выбрать в виде $\begin{pmatrix} 0 \\ C \end{pmatrix}$, и тогда в силу равенства (1.6)

$$Q = A_1 \oplus \begin{pmatrix} A_{\geq p} & C \\ {}^t C & Q' \end{pmatrix} \quad (3.1)$$

с блоком $Q' = (E[C] + G)/a$, $E = aA_{\geq p}^{-1}$. В частности, если $A = A_1$, то из разложения (3.1) и равенства (1.11) сразу выводим

$$G = G_1 = Q \ominus A_1, \quad K = Q \ominus A_1. \quad (3.2)$$

Пользуясь формулой (3.1), достаточно рассмотреть форму $A = A_{\geq p}$, т.е. $A \equiv 0 \pmod{2}$. Согласно [1, (7.3)], с точностью до эквивалентности над $\text{GL}(\mathbb{Z}_2)$, имеет место матричное сравнение

$$G \equiv^* \begin{pmatrix} -E & 0 \\ 0 & 0 \end{pmatrix} \pmod{a}, \quad (3.3)$$

где знаком $\equiv^*$ для нечетных форм $Q = Q_I$ обозначено обычное сравнение, а для четных форм $Q = Q_{II}$ – сравнение с дополнительным условием, что диагонали сравнимы по $\bmod 2a$.

3.2. Рассмотрим первый нетривиальный одномерный случай $A = 2A_2$, $\dim A_2 = 1$, со ступенью $a = 2$, $E = A_2^{-1} \equiv 1 \pmod{2}$ и $E \equiv A_2 \pmod{8}$. Сравнения (3.3) налагают на форму G следующие ограничения: $G = G_1 \oplus 2G_2$, $\dim G_1 = 1$ и G_1 нечетное. В сравнении (1.3) в качестве $C \pmod{2}$ возьмем $C = (1 \ 0)$. В силу (3.1) имеем разложение

$$Q = J(2A_2) \oplus G_2 \quad (3.4)$$

с минимальным для формы $A = 2A_2$ вложением $J(2A_2) = \begin{pmatrix} 2A_2 & 1 \\ 1 & Q' \end{pmatrix}$, $Q' = (A_2 + G_1)/2$. Прямым вычислением находим все инварианты формы $J = J(2A_2)$ (подробности см. в [6, с. 478]):

$$\dim J = 2, \quad |J| \equiv A_2 G_1 \pmod{8}, \quad (3.5)$$

и $J = J_I$ или $J = J_{II}$, если соответственно $A_2 + G_1 \not\equiv 0$ или $A_2 + G_1 \equiv 0 \pmod{4}$,

$$t(J_I) \equiv (A_2 + G_1)(1 + A_2 G_1)/2 \pmod{8}, \quad t(J_{II}) = 0.$$

ТАБЛИЦА 3.1

$J(2A_2)$	$1_{I,1}^{+1}$	$1_{I,5}^{-1}$	$1_{I,3}^{-1}$	$1_{I,7}^{+1}$
$2_{I,1}^{+1}$	$1_{I,2}^{+2}$	$1_{I,2}^{-2}$	1_{II}^{-2}	1_{II}^{+2}
$2_{I,5}^{-1}$	$1_{I,2}^{-2}$	$1_{I,2}^{+2}$	1_{II}^{+2}	1_{II}^{-2}
$2_{I,3}^{-1}$	1_{II}^{-2}	1_{II}^{+2}	$1_{I,6}^{+2}$	$1_{I,6}^{-2}$
$2_{I,7}^{+1}$	1_{II}^{+2}	1_{II}^{-2}	$1_{I,6}^{-2}$	$1_{I,6}^{+2}$

Удобно записать инварианты в виде табл. 3.1, где в первой строке указаны 2-символы блоков G_1 , в первом столбце – форм $A = 2A_2$, а на пересечении строк и столбцов симметрично относительно главной диагонали расположены 2-символы двумерных форм $J(2A_2)$ из разложения (3.4).

Возвращаясь к более общему случаю $A = A_1 \oplus 2A_2$, $\dim A_2 = 1$, обозначим $J(A) = A_1 \oplus J(2A_2)$. Из (3.1), (3.4) и (1.11) выводим разложения

$$G = G_1 \oplus 2(Q \ominus J(A)), \quad K = (Q \ominus J(A)) \oplus 2G_1, \quad (3.6)$$

где одномерный блок G_1 может быть любым нечетным числом, а $J(A)$ вычисляется по A_1 и табл. 3.1.

3.3. Перейдем к следующему случаю форм $A = 4A_4$, $\dim A_4 = 1$, когда $a = 4$ и $E \equiv A_4 \pmod{8}$. Из (3.3) вытекают условия на G :

$$G = G_1 \oplus 4G_4, \quad \dim G_1 = 1, \quad G_1 \equiv -A_4 \pmod{4}.$$

В сравнении (1.3) C рассматривается по mod 4; снова выбираем $C = (1 \ 0)$. Тогда из (3.1) получаем разложение

$$Q = J(4A_4) \oplus G_4, \quad (3.7)$$

где с точностью до эквивалентности $J(4A_4) = \begin{pmatrix} 4A_4 & 1 \\ 1 & Q' \end{pmatrix}$ и $Q' = (A_4 + G_1)/4$. Теперь форма $J = J(4A_4)$ имеет *инварианты*:

$$\dim J = 2, \quad |J| \equiv A_4 G_1 \pmod{8}, \quad (3.8)$$

и $J = J_I$ или $J = J_{II}$ соответственно для $A_4 + G_1 \not\equiv 0$ или $A_4 + G_1 \equiv 0 \pmod{8}$,

$$t(J_I) \equiv A_4 + G_1 \pmod{8}, \quad t(J_{II}) = 0.$$

В табл. 3.2 в первом столбце указаны 2-символы форм $A = 4A_4$, а на пересечении строк и столбцов – форм $J(4A_4)$ из разложения (3.7).

ТАБЛИЦА 3.2

$J(4A_4)$	$1_{I,1}^{+1}$	$1_{I,5}^{-1}$	$1_{I,3}^{-1}$	$1_{I,7}^{+1}$
$4_{I,5}^{+1}$			$1_{I,4}^{-2}$	1_{II}^{+2}
$4_{I,5}^{-1}$			1_{II}^{+2}	$1_{I,4}^{-2}$
$4_{I,3}^{-1}$	$1_{I,4}^{-2}$	1_{II}^{+2}		
$4_{I,7}^{+1}$	1_{II}^{+2}	$1_{I,4}^{-2}$		

Для случая общих форм вида $A = A_1 \oplus 4A_4$, $\dim A_4 = 1$, определим $J(A) = A_1 \oplus J(4A_4)$. Из (3.1), (3.7) следует

$$G = G_1 \oplus 4(Q \ominus J(A)), \quad K = (Q \ominus J(A)) \oplus 4G_1, \quad (3.9)$$

где одномерный блок G_1 удовлетворяет сравнению

$$G_1 \equiv -A_4 \pmod{4}.$$

3.4. Формы $A = qA_q$, $\dim A_q = 1$, со степенью $q = 2^\alpha$, $\alpha \geq 3$, как мы увидим, имеют особое поведение. Так как по (3.3) $G = G_1 \oplus qG_q$, $\dim G_1 = 1$, $G_1 \equiv -A_q \pmod{q}$, то можем сразу считать $G_1 = -A_q$. В сравнении (1.3) выбираем $C = (C_1, 0)$, число $C_1 \pmod{q}$ удовлетворяет условию $C_1^2 \equiv 1 \pmod{q}$. Сравнения $x^2 \equiv 1 \pmod{2^\beta}$ для $\beta = 2$ и $\beta \geq 3$ имеют два решения $x \equiv \pm 1$ и четыре решения $x \equiv \pm 1, \pm(1 + 2^{\beta-1})$ соответственно. Это следует из сравнений $x - 1 \equiv 0 \pmod{2^{\beta-1}}$ или $x + 1 \equiv 0 \pmod{2^{\beta-1}}$. Решения $C_1 = 1$ и $C_1 = 1 + q/2$ дадут разложения

$$Q = J(qA_q) \oplus G_q \quad (3.10)$$

с блоками

$$J(qA_q) = \begin{pmatrix} qA_q & 1 \\ 1 & 0 \end{pmatrix}_{\Pi} \quad \text{и} \quad \begin{pmatrix} qA_q & 1 + q/2 \\ 1 + q/2 & Aq(1 + q/4) \end{pmatrix}_{\Pi},$$

имеющими одинаковые определители $|J(qA_q)| \equiv -1$ и странности $t \equiv 0 \pmod{8}$.

ТАБЛИЦА 3.3

$J(qA_q)$	$1_{I,1}^{+1}$	$1_{I,5}^{-1}$	$1_{I,3}^{-1}$	$1_{I,7}^{+1}$
$q_{I,1}^{+1}$				$1_{\Pi}^{+2}, 1_{I,0}^{+2}$
$q_{I,5}^{-1}$			$1_{\Pi}^{+2}, 1_{I,0}^{+2}$	
$q_{I,3}^{-1}$		$1_{\Pi}^{+2}, 1_{I,0}^{+2}$		
$q_{I,7}^{+1}$	$1_{\Pi}^{+2}, 1_{I,0}^{+2}$			

В табл. 3.3 в первой строке и первом столбце расположены 2-символы форм $G_1 = -A_q$ и $A = qA_q$, $q = 2^\alpha$, $\alpha \geq 3$. На пересечении строк и столбцов указаны соответствующие формы $J(qA_q)$ из (3.10).

Общие формы $A = A_1 \oplus qA_q$, $\dim A_q = 1$, согласно (3.1) и (3.10) приводят к разложениям

$$G = -A_q \oplus q(Q \ominus J(A)), \quad K = (Q \ominus J(A)) \oplus q(-A_q), \quad (3.11)$$

где снова использовано сокращение $J(A) = A_1 \oplus J(qA_q)$.

§ 4. Вложения над кольцом $\mathbb{Z}_2$: двумерный случай

4.1. Переходим к формам $A = 2A_2$ с нечетным блоком A_2 размерности $\dim A_2 = 2$. Из локальной классификации следует, что A_2 – одна из следующих шести диагональных двумерных форм:

$$\begin{aligned} 0^+ &= \begin{pmatrix} 1 & \\ & 7 \end{pmatrix}, & 4^- &= \begin{pmatrix} 1 & \\ & 3 \end{pmatrix}, & 2^+ &= \begin{pmatrix} 1 & \\ & 1 \end{pmatrix}, \\ 6^- &= \begin{pmatrix} 1 & \\ & 5 \end{pmatrix}, & 6^+ &= \begin{pmatrix} 3 & \\ & 3 \end{pmatrix}, & 2^- &= \begin{pmatrix} 3 & \\ & 7 \end{pmatrix}. \end{aligned} \quad (4.1)$$

В дальнейшем станет ясным приведенный порядок расположения форм. Знаки $+$ и $-$ обозначают знак определителя, номер формы указывает ее странность t .

Из сравнения (3.3) выводим $G = G_1 \oplus 2G_2$ с блоком $G_1 \equiv -A_2 \pmod{2}$, и поэтому G_1 – одна из приведенных форм (4.1). Если положить $A_2 = \begin{pmatrix} a_2 & \\ & a'_2 \end{pmatrix}$ и $G_1 = \begin{pmatrix} g_1 & \\ & g'_1 \end{pmatrix}$, то в формуле (3.1) полагаем $E = A_2$ и $C = (C_1 \ 0)$, где (2×2) -матрица C_1 есть решение матричного сравнения $A_2[C_1] \equiv G_1 \pmod{2}$. Группа $\text{SL}_2(\mathbb{Z}/2\mathbb{Z})$ содержит шесть элементов. Их перебор показывает, что сравнению удовлетворяют только матрицы $C_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Формула (3.1) для таких C_1 приводит к разложению

$$Q = J(2A_2) \oplus G_2, \quad (4.2)$$

где, с точностью до эквивалентности, первые блоки можно представить соответственно в виде

$$J(2A_2) = \begin{pmatrix} 2a_2 & 1 \\ 1 & (a_2 + g_1)/2 \end{pmatrix} \oplus \begin{pmatrix} 2a'_2 & 1 \\ 1 & (a'_2 + g'_2)/2 \end{pmatrix}$$

или

$$J(2A_2) = \begin{pmatrix} 2a_2 & 1 \\ 1 & (a_2 + g'_1)/2 \end{pmatrix} \oplus \begin{pmatrix} 2a'_2 & 1 \\ 1 & (a'_2 + g_2)/2 \end{pmatrix}.$$

Следовательно, $J(2A_2)$ задают *минимальные разложимые вложения* двумерных форм $A = 2A_2$. Странности составляющих для $J(2A_2)$ суммируются, и по (3.5) в обоих случаях $|J(2A_2)| \equiv |A_2| \cdot |G_1| \pmod{8}$. Приведенные соображения сводят вычисление инвариантов форм $J(2A_2)$ к их двумерным аналогам из (3.4). На основании формул (3.5) вычислена табл. 4.1. В первой строке и первом столбце стоят 2-символы двумерных форм G_1 и $A = 2A_2$ в том же порядке, что и в (4.1).

ТАБЛИЦА 4.1

$J(2A_2)$	$1_{I,0}^{+2}$	$1_{I,4}^{-2}$	$1_{I,2}^{+2}$	$1_{I,6}^{-2}$	$1_{I,6}^{+2}$	$1_{I,2}^{-2}$
$2_{I,0}^{+2}$	$1_{II}^{+4}, 1_{I,0}^{+4}$	$1_{II}^{-4}, 1_{I,0}^{-4}$	$1_{I,2}^{+4}$	$1_{I,2}^{-4}$	$1_{I,6}^{+4}$	$1_{I,6}^{-4}$
$2_{I,4}^{-2}$	$1_{II}^{-4}, 1_{I,0}^{-4}$	$1_{II}^{+4}, 1_{I,0}^{+4}$	$1_{I,2}^{-4}$	$1_{I,2}^{+4}$	$1_{I,6}^{-4}$	$1_{I,6}^{+4}$
$2_{I,2}^{+2}$	$1_{I,2}^{+4}$	$1_{I,2}^{-4}$	$1_{I,4}^{+4}$	$1_{I,4}^{-4}$	1_{II}^{+4}	1_{II}^{-4}
$2_{I,6}^{-2}$	$1_{I,2}^{-4}$	$1_{I,2}^{+4}$	$1_{I,4}^{-4}$	$1_{I,4}^{+4}$	1_{II}^{-4}	1_{II}^{+4}
$2_{I,6}^{+2}$	$1_{I,6}^{+4}$	$1_{I,6}^{-4}$	1_{II}^{+4}	1_{II}^{-4}	$1_{I,4}^{+4}$	$1_{I,4}^{-4}$
$2_{I,2}^{-2}$	$1_{I,6}^{-4}$	$1_{I,6}^{+4}$	1_{II}^{-4}	1_{II}^{+4}	$1_{I,4}^{-4}$	$1_{I,4}^{+4}$

Упорядочение (4.1) делает прозрачными симметрии табл. 4.1. Для общих форм $A = A_1 \oplus 2A_2$, $\dim A_2 = 2$, формулы (3.1) и (4.2) приводят к разложениям

$$G = G_1 \oplus 2(Q \ominus J(A)), \quad K = (Q \ominus J(A)) \oplus 2G_1, \quad (4.3)$$

где G_1 – любая из форм (4.1) с 2-символами из первой строки табл. 4.1.

4.2. Для форм $A = 2A_2$ с четным блоком A_2 размерности $\dim A_2 = 2$ приходится рассматривать автоморфизмы *двойственных* им форм G_1 . Поскольку $E = A_2^{-1} \equiv A_2 \pmod{2}$, $G = G_1 \oplus 2G_2$ и по (3.3) $G_1 \equiv -E \pmod{2}$, то формы A_2 и G_1 $\mathbb{Z}_2$ -эквивалентны одной из неразложимых форм

$$0_{II}^{+} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad 0_{II}^{-} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}.$$

Выбирая в формуле (3.1) $C = (C_1 \ 0)$, где C_1 рассматривается по $\pmod{2}$, видим, что сравнение

$$E[C_1] \equiv -G_1 \pmod{2} \quad (4.4)$$

равносильно сравнению $0_{\Pi}^{-}[C_1] \equiv 0_{\Pi}^{-} \pmod{2}$. Его решения образуют группу $\mathrm{SL}_2(\mathbb{Z}/2\mathbb{Z}) = O_{\mathbb{Z}}(0_{\Pi}^{-})/\mathrm{mod} 2$, где $O_{\mathbb{Z}}(0_{\Pi}^{-}) = \mathrm{Aut} A_2 \simeq \mathfrak{D}_6$ – группа автоморфизмов *гексагональной решетки*, изоморфная *диэдральной группе* симметрий правильного 6-угольника. Матрицы $h = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $\sigma = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$ – образующие группы $O_{\mathbb{Z}}(0_{\Pi}^{-}) = \langle h, \sigma \rangle$ с *порождающими соотношениями* (генетическим кодом) $h^2 = \sigma^6 = (h\sigma)^2 = 1$.

Класс $\mathbb{Z}_2$ -эквивалентности формы Q (3.1) для C_1 (4.4) зависит [2] от класса смежности $C_1 \cdot O_{\mathbb{Z}}(G_1)/\mathrm{mod} 2$. Для вычисления фактормножества потребуется еще группа автоморфизмов гиперболической решетки $O_{\mathbb{Z}}(0_{\Pi}^{+}) = \langle -1, h \rangle$ с порождающими соотношениями $(-1)^2 = h^2 = (-1 \cdot h)^2 = 1$, где -1 обозначает матрицу $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. Эту группу еще называют *четверной* или *группой Клейна*. Из матричного представления следует, что $O_{\mathbb{Z}}(0_{\Pi}^{+})$ – подгруппа из $O_{\mathbb{Z}}(0_{\Pi}^{-})$, не являющаяся нормальным делителем, и $O_{\mathbb{Z}}(0_{\Pi}^{-})/O_{\mathbb{Z}}(0_{\Pi}^{+}) = \{1, \sigma, \sigma^2\}$ – ее классы смежности. Таким образом, для нахождения инвариантов формы Q (3.1) в сравнении (4.4) можем ограничиться решениями $C_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ и $C_1 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ для $G_1 = 0_{\Pi}^{-}$ и $G_1 = 0_{\Pi}^{+}$ соответственно.

В случае $A_2 = 0_{\Pi}^{-}$, $G_1 = 0_{\Pi}^{+}$ последние три матрицы C_1 согласно формуле (3.1) дают по mod 8 соответственно блоки $Q' = \begin{pmatrix} -1 & -1 \\ -1 & -1 \end{pmatrix}$, $\begin{pmatrix} -1 & -2 \\ -2 & 3 \end{pmatrix}$, $\begin{pmatrix} 3 & -2 \\ -2 & -1 \end{pmatrix}$ и формы $J(2A_2)$ размерности 4:

$$\begin{pmatrix} 4 & 2 & 1 & 0 \\ 2 & 4 & 0 & 1 \\ 1 & 0 & -1 & -1 \\ 0 & 1 & -1 & -1 \end{pmatrix}, \quad \begin{pmatrix} 4 & 2 & 0 & 1 \\ 2 & 4 & 1 & 1 \\ 0 & 1 & -1 & -2 \\ 1 & 1 & -2 & 3 \end{pmatrix}, \quad \begin{pmatrix} 4 & 2 & 1 & 1 \\ 2 & 4 & 1 & 0 \\ 1 & 1 & 3 & -2 \\ 1 & 0 & -2 & -1 \end{pmatrix},$$

с одинаковыми 2-символами $1_{I,4}^{-4}$. Последовательно переставляя строки и столбцы 1, 2 и 3, 4, убеждаемся в эквивалентности двух последних форм $J(2A_2)$. Поэтому первые две формы $J(2A_2)$ задают все различные *минимальные неразложимые вложения* формы $A_2 = 0_{\Pi}^{-}$. В оставшихся случаях получаются следующие формы $J(2A_2)$ и их 2-символы:

$$J(2A_2) = \begin{pmatrix} 0 & 2 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}_{\Pi}, \quad 1_{\Pi}^{+4} \quad \text{и} \quad J(2A_2) = \begin{pmatrix} 0 & 2 & 0 & 1 \\ 2 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \quad 1_{I,0}^{+4}$$

для $A_2 = 0_{\Pi}^{+}$, $G_1 = 0_{\Pi}^{+}$;

$$J(2A_2) = \begin{pmatrix} 0 & 2 & 1 & 0 \\ 2 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}, \quad 1_{I,4}^{-4}$$

для $A_2 = 0_{\Pi}^+$, $G_1 = 0_{\Pi}^-$;

$$J(2A_2) = \begin{pmatrix} 4 & 2 & 1 & 0 \\ 2 & 4 & 0 & 1 \\ 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \end{pmatrix}, \quad 1_{\Pi}^{+4}$$

для $A_2 = 0_{\Pi}^-$, $G_1 = 0_{\Pi}^-$.

Если форма $A = A_1 \oplus 2A_2$ имеет четный двумерный блок A_2 , то для G и K остаются справедливыми формулы (4.3), в которых $G_1 = 0_{\Pi}^{\pm}$ – формы из первой строки, $J(A) = A_1 \oplus J(2A_2)$ и для $2A_2$ из первого столбца 2-символы минимальных неразложимых вложений $J(2A_2)$ даются в табл. 4.2.

ТАБЛИЦА 4.2

$J(2A_2)$	1_{Π}^{+2}	1_{Π}^{-2}
2_{Π}^{+2}	$1_{\Pi}^{+4}, 1_{I,0}^{+4}$	$1_{I,4}^{-4}$
2_{Π}^{-2}	$1_{I,4}^{-4}$	1_{Π}^{+4}

§ 5. Кубические решетки

5.1. Кубическая n -мерная решетка $\mathbb{Z}^n$ состоит из векторов $x = (x_1, \dots, x_n)$ с целыми координатами $x_i \in \mathbb{Z}$. Единичные векторы образуют $\mathbb{Z}$ -базис решетки $\mathbb{Z}^n$. Поэтому относительно обычного скалярного произведения она имеет *единичную матрицу Грама* $Q = 1_n$, определитель $d = 1$ и локальные символы

$$p_Q = 1^{+n} \quad \text{для } p \neq 2 \quad \text{и} \quad 2_Q = 1_{I,n}^{+n}. \quad (5.1)$$

Число ее автоморфизмов $o(1_n) = 2^n \cdot n!$ и число классов h в роде $[Q]$ равно 1 для размерностей $n \leq 8$. Выбор решеток $\mathbb{Z}^n$, $n \leq 8$, обусловлен их простым строением.

5.2. При вложении над нечетным кольцом $\mathbb{Z}_p$ форм A в $Q = 1_n$ формы G и K однозначно определяются формулами (2.3) и (2.4) в терминах жорданова разложения $A = A_1 \oplus A_{\geq p}$. По этим формулам легко вычисляются p -символы G и K , если форма A конкретная. Для одноблочных форм A p -символы можно выписать явно. Так, при $A = A_1$, $a = 1$ согласно (2.3), (2.4) получим

$$G = K = 1_n \ominus A_1, \quad p_G = p_K = 1^{\varepsilon_1(n-m)}, \quad (5.2)$$

где $p_A = 1^{\varepsilon_1 m}$ и символ $1^{\varepsilon_1 0}$ существует только при $\varepsilon_1 = +1$. А в случае одноблочных форм $A = qA_q$ масштаба $q = p^\alpha$ с $\alpha \geq 1$ и знаком $\varepsilon_q = \left(\frac{|A_q|}{p}\right)$ по формуле (2.3) получим

$$G = -A_q \oplus q(1_n \ominus J(qA_q)), \quad p_G = 1^{(-1)^m \varepsilon_q m} q^{(-1)^m (n-2m)} \quad (5.3)$$

и сокращение (-1) обозначает значение символа Лежандра $\left(\frac{-1}{p}\right)$. По (2.4) символ p_K получается перестановкой показателей в p_G .

5.3. Формам Q и Q' из одного класса эквивалентности $\{Q\}$ над $\mathbb{Z}_2$ отвечают эквивалентные 2-символы $2_Q \sim 2_{Q'}$, преобразующиеся друг в друга элементарными преобразованиями: *слиянием странностей* и *проходом знаков* [6, с. 480]. Если условиться ставить общий знак в определенном месте входящих в 2-символы поездов, то восстанавливается биекция

$$Q \sim 2Q' \Leftrightarrow 2_Q^{\text{can}} = 2_{Q'}^{\text{can}}.$$

Вычисление форм G и K (5.2) в случае $p = 2$ сводится к следующим формулам вычитания 2-символов:

$$\begin{aligned} 1_{I,t}^{\varepsilon n} \ominus 1_{I,t_1}^{\varepsilon_1 m} &= 1_{I,t-t_1}^{\varepsilon \varepsilon_1(n-m)}, \quad 1_{II}^{\varepsilon \varepsilon_1(n-m)}, \quad \text{если } t \equiv t_1 \pmod{8}, \\ 1_{I,t}^{\varepsilon n} \ominus 1_{II}^{\varepsilon_1 m} &= 1_{I,t}^{\varepsilon \varepsilon_1(n-m)}, \quad 1_{II}^{\varepsilon n} \ominus 1_{II}^{\varepsilon_1 m} = 1_{II}^{\varepsilon \varepsilon_1(n-m)}. \end{aligned} \quad (5.4)$$

Операция $\ominus$ определена только при условии существования соответствующего 2-символа справа (см. [1, с. 70]). В табл. 5.1 по формулам (5.2), (5.4) вычислены 2-символы форм $G = K$ для вложений над $\mathbb{Z}_2$ одномерных форм $A = A_1$ в $Q = 1_n$. Пропуски означают невозможность соответствующего вложения над $\mathbb{Z}_2$.

ТАБЛИЦА 5.1

G/K	$n = 1$	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$1_{I,1}^{+1}$	1_{II}^{+0}	$1_{I,1}^{+1}$	$1_{I,2}^{+2}$	$1_{I,3}^{+3}$	$1_{I,4}^{+4}$	$1_{I,5}^{+5}$	$1_{I,6}^{+6}$	$1_{I,7}^{+7}$
$1_{I,5}^{-1}$		$1_{I,5}^{-1}$	$1_{I,6}^{-2}$	$1_{I,7}^{-3}$	$1_{II}^{-4}, 1_{I,0}^{-4}$	$1_{I,1}^{-5}$	$1_{I,2}^{-6}$	$1_{I,3}^{-7}$
$1_{I,3}^{-1}$			1_{II}^{-2}	$1_{I,1}^{-3}$	$1_{I,2}^{-4}$	$1_{I,3}^{-5}$	$1_{I,4}^{-6}$	$1_{I,5}^{-7}$
$1_{I,7}^{+1}$				$1_{I,5}^{+3}$	$1_{I,6}^{+4}$	$1_{I,7}^{+5}$	$1_{II}^{+6}, 1_{I,0}^{+6}$	$1_{I,1}^{+7}$

5.4. Для исследования вложений форм $A = qA_q$ степени $a = q = 2^\alpha$, $\alpha \geq 1$, нужно использовать таблицы из § 3. Как вычисляются 2-символы форм G и K , покажем на примере вложения формы $A = 2A_2$, $\dim A_2 = 1$, с 2-символом $2_A = 2_{I,3}^{-1}$ в форму $Q = 1_6$. С помощью табл. 3.1, первой формулы из (3.6) и равенств (5.4) составляем вспомогательную таблицу:

G_1	$1_{I,1}^{+1}$	$1_{I,5}^{-1}$	$1_{I,3}^{-1}$	$1_{I,7}^{+1}$
G_2	$1_{I,6}^{-4}$	$1_{I,6}^{+4}$	1_{II}^{+4}	$1_{I,0}^{+4}, 1_{II}^{-4}, 1_{I,0}^{-4}$
G	$1_{I,1}^{+1} 2_{I,6}^{-4}$	$1_{I,5}^{-1} 2_{I,6}^{+4}$	$1_{I,3}^{-1} 2_{II}^{+4}$	$1_{I,3}^{-1} 2_{I,0}^{+4}, 1_{I,0}^{+1} 2_{II}^{-4}, 1_{I,7}^{+1} 2_{I,0}^{-4}$
2_G^{can}	$[1^1 2^{-4}]_7$	$[1^1 2^{-4}]_7$	$[1^1]_7 2_{II}^{-4}$	$[1^1 2^{-4}]_7, [1^1]_7 2_{II}^{-4}, [1^1 2^{-4}]_7$

Хотя для получающихся форм $G = G_1 \oplus 2G_2$ 2-символы принимают шесть различных значений, после приведения их к каноническому виду остаются только два

ТАБЛИЦА 5.2

G/K	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$2_{I,1}^{+1}$	$[1^1]_1$	$[1^1 2^1]_2$	$[1^1 2^2]_3$	$[1^1 2^3]_4$	$[1^1 2^4]_5$	$[1^1 2^5]_6$	$[1^1 2^6]_7$
	$[2^1]_1$	$[1^1 2^1]_2$	$[1^2 2^1]_3$	$[1^3 2^1]_4$	$[1^4 2^1]_5$	$[1^5 2^1]_6$	$[1^6 2^1]_7$
$2_{I,5}^{-1}$	$[1^{-1}]_5$	$[1^1 2^{-1}]_2$	$[1^1 2^{-2}]_3$	$[1^1 2^{-3}]_4$	$[1^1 2^{-4}]_5$	$[1^1 2^{-5}]_6$	$[1^1 2^{-6}]_7$
	$[2^{-1}]_5$	$[1^{-1} 2^1]_2$	$[1^{-2} 2^1]_3$	$[1^{-3} 2^1]_4$	$[1^{-4} 2^1]_5$	$[1^{-5} 2^1]_6$	$[1^{-6} 2^1]_7$
$2_{I,3}^{-1}$		$[1^1 2^{-1}]_4$	$[1^1 2^{-2}]_5$	$[1^1 2^{-3}]_6$	$[1^1 2^{-4}]_7; [1^1]_7 2_{II}^{-4}$	$[1^1 2^{-5}]_0$	$[1^1 2^{-6}]_1$
		$[1^{-1} 2^1]_4$	$[1^{-2} 2^1]_5$	$[1^{-3} 2^1]_6$	$[1^{-4} 2^1]_7; 1_{II}^{-4} [2^1]_7$	$[1^{-5} 2^1]_0$	$[1^{-6} 2^1]_1$
$2_{I,7}^{+1}$		$[1^1 2^1]_4$	$[1^1 2^2]_5$	$[1^1 2^3]_6$	$[1^1 2^4]_7; [1^1]_7 2_{II}^4$	$[1^1 2^5]_0$	$[1^1 2^6]_1$
		$[1^1 2^1]_4$	$[1^2 2^1]_5$	$[1^3 2^1]_6$	$[1^4 2^1]_7; 1_{II}^4 [2^1]_7$	$[1^5 2^1]_0$	$[1^6 2^1]_1$

ТАБЛИЦА 5.3

G/K	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$4_{I,1}^{+1}$	$[1^{-1}]_3 : 4_{II}^{-2}$	$[1^1]_7 [4^3]_5$	$[1^1]_7 [4^4]_6$	$[1^1]_7 [4^5]_7$	$[1^1]_7 [4^6]_0$
	$1_{II}^{-2} : [4^{-1}]_3$	$[1^3]_5 [4^1]_7$	$[1^4]_6 [4^1]_7$	$[1^5]_7 [4^1]_7$	$[1^6]_0 [4^1]_7$
$4_{I,5}^{-1}$	$[1^1]_7 : 4_{II}^{-2}$	$[1^1]_7 [4^{-3}]_1$	$[1^1]_7 [4^{-4}]_2$	$[1^1]_7 [4^{-5}]_3$	$[1^1]_7 [4^{-6}]_4$
	$1_{II}^{-2} : [4^1]_7$	$[1^{-3}]_1 [4^1]_7$	$[1^{-4}]_2 [4^1]_7$	$[1^{-5}]_3 [4^1]_7$	$[1^{-6}]_4 [4^1]_7$
$4_{I,3}^{-1}$	$[1^1]_1 : 4_{II}^{-2}$	$[1^1]_1 [4^{-3}]_1$	$[1^1]_1 [4^{-4}]_2$	$[1^1]_1 [4^{-5}]_3$	$[1^1]_1 [4^{-6}]_4$
	$1_{II}^{-2} : [4^1]_1$	$[1^{-3}]_1 [4^1]_1$	$[1^{-4}]_2 [4^1]_1$	$[1^{-5}]_3 [4^1]_1$	$[1^{-6}]_4 [4^1]_1$
$4_{I,7}^{+1}$	$[1^{-1}]_5 : 4_{II}^{-2}$	$[1^1]_1 [4^3]_5$	$[1^1]_1 [4^4]_6$	$[1^1]_1 [4^5]_7$	$[1^1]_1 [4^6]_0$
	$1_{II}^{-2} : [4^{-1}]_5$	$[1^3]_5 [4^1]_1$	$[1^4]_6 [4^1]_1$	$[1^5]_7 [4^1]_1$	$[1^6]_0 [4^1]_1$

неэквивалентных символа $[1^1 2^{-4}]_7$ и $[1^1]_7 2_{II}^{-4}$. В табл. 5.2 эти символы расположены в верхнем ряду на пересечении строки $2_{I,3}^{-1}$ и столбца $n = 6$. Под ними находятся 2-символы форм K (3.6).

Аналогично получаются табл. 5.3 и 5.4, с помощью таблиц и формул пп. 3.3, 3.4.

Согласно табл. 5.3 примитивные представления чисел $A = 4A_4$ суммой квадратов $Q = 1_n$ возможны только при $n \geq 4$. В табл. 5.4 степень имеет вид $q = 2^\alpha$, $\alpha \geq 3$. Как видно из табл. 5.2 при $n = 6$ и табл. 5.4 при $n = 8$, формы K могут быть двух неэквивалентных над $\mathbb{Z}_2$ видов. Отсюда вытекает существование по крайней мере двух неэквивалентных над $\mathbb{Z}_2$ вложений соответствующих форм A в 1_n .

5.5. Табл. 5.5 и 5.6 содержат вложения в $Q = 1_n$ двумерных форм $A = qA_q$ степеней $q = 1$ и $q = 2$. При вычислении 2-символов форм G и K использованы формулы (5.4), табл. 4.1 и формулы (4.3).

ТАБЛИЦА 5.4

G/K	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$q_{I,1}^{+1}$	$[1^1]_7 : [q^3]_5$ $[1^3]_5 : [q^1]_7$	$[1^1]_7 : [q^4]_6$ $[1^4]_6 : [q^1]_7$	$[1^1]_7 : [q^5]_7$ $[1^5]_7 : [q^1]_7$	$[1^1]_7 : q_{II}^6, [1^1]_7 : [q^6]_0$ $1_{II}^6 : [q^1]_7, [1^6]_0 : [q^1]_7$
$q_{I,5}^{-1}$	$[1^{-1}]_3 : [q^3]_5$ $[1^3]_5 : [q^{-1}]_3$	$[1^{-1}]_3 : [q^4]_6$ $[1^4]_6 : [q^{-1}]_3$	$[1^{-1}]_3 : [q^5]_7$ $[1^5]_7 : [q^{-1}]_3$	$[1^{-1}]_3 : q_{II}^6, [1^{-1}]_3 : [q^6]_0$ $1_{II}^6 : [q^{-1}]_3, [1^6]_0 : [q^{-1}]_3$
$q_{I,3}^{-1}$	$[1^{-1}]_5 : [q^3]_5$ $[1^3]_5 : [q^{-1}]_5$	$[1^{-1}]_5 : [q^4]_6$ $[1^4]_6 : [q^{-1}]_5$	$[1^{-1}]_5 : [q^5]_7$ $[1^5]_7 : [q^{-1}]_5$	$[1^{-1}]_5 : q_{II}^6, [1^{-1}]_5 : [q^6]_0$ $1_{II}^6 : [q^{-1}]_5, [1^6]_0 : [q^{-1}]_5$
$q_{I,7}^{+1}$	$[1^1]_1 : [q^3]_5$ $[1^3]_5 : [q^1]_1$	$[1^1]_1 : [q^4]_6$ $[1^4]_6 : [q^1]_1$	$[1^1]_1 : [q^5]_7$ $[1^5]_7 : [q^1]_1$	$[1^1]_1 : q_{II}^6, [1^1]_1 : [q^6]_0$ $1_{II}^6 : [q^1]_1, [1^6]_0 : [q^1]_1$

ТАБЛИЦА 5.5

G/K	$n = 2$	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$1_{I,0}^{+2}$				$1_{I,5}^{+3}$	$1_{I,6}^{+4}$	$1_{I,7}^{+5}$	$1_{II}^{+6}, 1_{I,0}^{+6}$
$1_{I,4}^{-2}$				$1_{I,1}^{-3}$	$1_{I,2}^{+4}$	$1_{I,3}^{-5}$	$1_{I,4}^{-6}$
$1_{I,2}^{+2}$	1_{II}^{+0}	$1_{I,1}^{+1}$	$1_{I,2}^{+2}$	$1_{I,3}^{+3}$	$1_{I,4}^{+4}$	$1_{I,5}^{+5}$	$1_{I,6}^{+6}$
$1_{I,6}^{-2}$		$1_{I,5}^{-5}$	$1_{I,6}^{-2}$	$1_{I,7}^{-3}$	$1_{II}^{-4}, 1_{I,0}^{-4}$	$1_{I,1}^{-5}$	$1_{I,2}^{-6}$
$1_{I,6}^{+2}$			$1_{I,6}^{+2}$	$1_{I,7}^{+3}$	$1_{II}^{+4}, 1_{I,0}^{+4}$	$1_{I,1}^{+5}$	$1_{I,2}^{+6}$
$1_{I,2}^{-2}$			$1_{I,2}^{-2}$	$1_{I,3}^{-3}$	$1_{I,4}^{-4}$	$1_{I,5}^{-5}$	$1_{I,6}^{-6}$

5.6. Двумерные формы $A = qA_q$ степеней $q = 1, 2$ с четным блоком A_q рассматриваются аналогично. При этом используются формулы вычитания 2-символов (5.4) для составления табл. 5.7 и применяется табл. 4.2 с последующими формулами для вычисления табл. 5.8.

5.7. До конца параграфа все формулы и представления рассматриваются над глобальным кольцом целых чисел $\mathbb{Z}$. Методом ортогонального дополнения в решетках $\mathbb{Z}^n$ получим формы K , для которых род $[K]$ состоит из одного класса. Опираемся будем на следующее утверждение, вытекающее из предложений 8.1 и 8.2.

ПРЕДЛОЖЕНИЕ 5.1. Допустим, что для одноклассной формы Q примитивные представления $Q[X] = A$, где X – $(n \times t)$ -матрица с коэффициентами из $\mathbb{Z}$, образуют r орбит $\{X\}$ из $\gamma \cdot X$, $\gamma \in O_{\mathbb{Z}}(Q)$. Если в этих условиях количество возможных родов K из п. 1.2 также равно r , то все формы $K = A_X^\perp$ разбиваются на r одноклассных родов.

ТАБЛИЦА 5.6

G/K	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
$2_{I,0}^{+2}$		$[1^2 2^1]_5, [1^2 2^{-1}]_5$ $[1^1 2^2]_5, [1^{-1} 2^2]_5$	$[1^2 2^2]_6, [1^2]_6 2_{II}^{+2}$ $[1^2 2^2]_6, 1_{II}^2 [2^2]_6$	$[1^2 2^3]_7$ $[1^3 2^2]_7$	$[1^2 2^4]_0$ $[1^4 2^2]_0$
$2_{I,4}^{-2}$		$[1^2 2^{-1}]_5, [1^2 2^1]_5$ $[1^{-1} 2^2]_5, [1^1 2^2]_5$	$[1^2 2^{-2}]_6, [1^2]_6 2_{II}^{-2}$ $[1^{-2} 2^2]_6, 1_{II}^{-2} [2^2]_6$	$[1^2 2^{-3}]_7$ $[1^{-3} 2^2]_7$	$[1^2 2^{-4}]_0$ $[1^{-4} 2^2]_0$
$2_{I,2}^{+2}$	$1_{I,2}^{+2}$ $2_{I,2}^{+2}$	$[1^2 2^1]_3$ $[1^1 2^2]_3$	$[1^2 2^2]_4$ $[1^2 2^2]_4$	$[1^2 2^3]_5$ $[1^3 2^2]_5$	$[1^2 2^4]_6$ $[1^4 2^2]_6$
$2_{I,6}^{-2}$	$1_{I,6}^{-2}$ $2_{I,6}^{-2}$	$[1^2 2^{-1}]_3, [1^2 2^{-1}]_1$ $[1^{-1} 2^2]_3, [1^{-1} 2^2]_1$	$[1^2 2^{-2}]_4$ $[1^{-2} 2^2]_4$	$[1^2 2^{-3}]_5$ $[1^{-3} 2^2]_5$	$[1^2 2^{-4}]_6$ $[1^{-4} 2^2]_6$
$2_{I,6}^{+2}$	$1_{I,6}^{+2}$ $2_{I,6}^{+2}$	$[1^2 2^1]_7, [1^2 2^1]_3$ $[1^1 2^2]_7, [1^1 2^2]_3$	$[1^2]_0 2_{II}^{+2}, [1^2 2^2]_0$ $1_{II}^{+2} [2^2]_0, [1^2 2^2]_0$	$[1^2 2^3]_1$ $[1^3 2^2]_1$	$[1^2 2^4]_2$ $[1^4 2^2]_2$
$2_{I,2}^{-2}$	$1_{I,2}^{-2}$ $2_{I,2}^{-2}$	$[1^2 2^{-1}]_7$ $[1^{-1} 2^2]_7$	$[1^2]_0 2_{II}^{-2}, [1^2 2^{-2}]_0$ $1_{II}^{-2} [2^2]_0, [1^{-2} 2^2]_0$	$[1^2 2^{-3}]_1$ $[1^{-3} 2^2]_1$	$[1^2 2^{-4}]_2$ $[1^{-4} 2^2]_2$

ТАБЛИЦА 5.7

G/K	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$
1_{II}^{+2}			$1_{I,5}^{+3}$	$1_{I,6}^{+4}$	$1_{I,7}^{+5}$	$1_{I,0}^{+6}$
1_{II}^{-2}	$1_{I,3}^{-1}$	$1_{I,4}^{-2}$	$1_{I,5}^{-3}$	$1_{I,6}^{-4}$	$1_{I,7}^{-5}$	$1_{I,0}^{-6}$

ТАБЛИЦА 5.8

G/K	$n = 6$	$n = 7$	$n = 8$
2_{II}^{+2}	$1_{II}^2 [2^2]_6$ $[1^2]_6 2_{II}^2$	$1_{II}^2 [2^2]_7$ $[1^2]_7 2_{II}^2$	$1_{II}^2 [2^4]_0$ $[1^4]_0 2_{II}^2$
2_{II}^{-2}	$1_{II}^2 [2^{-2}]_6$ $[1^{-2}]_6 2_{II}^2$	$1_{II}^2 [2^3]_5, 1_{II}^2 [2^{-3}]_3$ $[1^3]_5 2_{II}^2, [1^{-3}]_3 2_{II}^2$	$1_{II}^2 [2^4]_6, 1_{II}^2 [2^{-4}]_4$ $[1^4]_6 2_{II}^2, [1^{-4}]_4 2_{II}^2$

Группа автоморфизмов $O_{\mathbb{Z}}(1_n)$ порождается $n!$ перестановками и 2^n переменными знаков координат. Это позволяет легко определять количество орбит примитивных представлений $1_n[X] = a$ одномерной формы или числа $A = a$. В табл. 5.9 для $a \leq 50$ содержатся приведенные представители орбит $X = (\dots)$ (каждая цифра – координата) и локальные символы ортогональных к ним одноклассных форм K . Сокращение $(\dots x_i^\alpha \dots)$ означает, что у данного вектора координата x_i

ТАБЛИЦА 5.9

$a = 0$	$(0^9)1_{I,0}^8$
$a = 1$	$(10^2)1_{I,2}^2; (10^3)1_{I,3}^3; (10^4)1_{I,4}^4; (10^5)1_{I,5}^5; (10^6)1_{I,6}^6; (10^7)1_{I,7}^7$
$a = 2$	$(1^20)[1^12^1]_2; (1^20^2)[1^22^1]_3; (1^20^3)[1^32^1]_4; (1^20^4)[1^42^1]_5;$ $(1^20^5)[1^52^1]_6; (1^20^6)[1^62^1]_7$
$a = 3$	$(1^3)1_{II}^{-2}, 1^{-1}3^{-1}; (1^30)1_{I,1}^{-3}, 1^{-2}3^{-1}; (1^30^2)1_{I,2}^{-4}, 1^{-3}3^{-1};$ $(1^30^3)1_{I,3}^{-5}, 1^{-4}3^{-1}; (1^30^4)1_{I,4}^{-6}, 1^{-5}3^{-1}; (1^30^5)1_{I,5}^{-7}, 1^{-6}3^{-1}$
$a = 4$	$(1^4)1_{II}^{-2} : [4^{-1}]_3; (1^40)[1^3]_5[4^1]_7; (1^40^2)[1^4]_6[4^1]_7; (1^40^3)[1^5]_7[4^1]_7;$ $(1^40^4)[1^6]_0[4^1]_7$
$a = 5$	$(120)1_{I,6}^{-2}, 1^15^1; (120^2)1_{I,7}^{-3}, 1^25^1; (120^3)1_{I,0}^{-4}, 1^35^1; (1^5)1_{II}^{-4}, 1^35^1$
$a = 6$	$(1^22)[1^{-1}2^{-1}]_4, 1^{-1}3^1; (1^220)[1^{-2}2^1]_5, 1^{-2}3^1; (1^220^2)[1^{-3}2^1]_6, 1^{-3}3^1;$ $(1^220^3)[1^{-4}2^1]_7, 1^{-4}3^1; (1^6)1_{II}^{-4}[2^1]_7, 1^{-4}3^1$
$a = 7$	$(1^32)1_{I,5}^3, 1^{-2}7^{-1}; (1^320)1_{I,6}^4, 1^{-3}7^{-1}; (1^320^2)1_{I,7}^5, 1^{-4}7^{-1};$ $(1^320^3)1_{I,0}^6, 1^{-5}7^{-1}; (1^7)1_{II}^6, 1^{-5}7^{-1}$
$a = 8$	$(1^42)[1^3]_5 : [8^1]_7; (1^420)[1^4]_6 : [8^1]_7; (1^420^2)[1^5]_7 : [8^1]_7;$ $(1^420^3)[1^6]_0 : [8^1]_7; (1^8)1_{II}^6 : [8^1]_7$
$a = 9$	$(12^2)1_{I,2}^2, 1^{-1}9^{-1}; (12^20)1_{I,3}^3, 1^{-2}9^{-1}; (12^20^2)1_{I,4}^4, 1^{-3}9^{-1}$
$a = 10$	$(130)[1^{-1}2^1]_2, 1^15^{-1}$
$a = 11$	$(1^23)1_{II}^{-2}, 1^{-1}11^{-1}; (1^230)1_{I,1}^{-3}, 1^{-2}11^{-1}$
$a = 12$	$(1^33)1_{II}^{-2} : [4^{-1}]_1, 1^{-2}3^{-1}; (1^330)[1^{-3}]_1[4^1]_1, 1^{-3}3^{-1}$
$a = 13$	$(230)1_{I,6}^{-2}, 1^113^1; (1^43)1_{II}^{-4}, 1^313^1$
$a = 14$	$(123)[1^12^1]_4, 1^{-1}7^{-1}; (1230)[1^22^1]_5, 1^{-2}7^{-1}$
$a = 15$	$(1^223)1_{I,5}^3, 1^{-2}3^1, 1^25^{-1}; (1^2230)1_{I,6}^4, 1^{-3}3^1, 1^35^{-1}$
$a = 16$	$(1^323)[1^3]_5 : [16^1]_7; (1^3230)[1^4]_6 : [16^1]_7$
$a = 18$	$(1^24)[1^12^1]_2, 1^{-1}9^1$
$a = 19$	$(13^2)1_{II}^{-2}$
$a = 20$	$(1^23^2)1_{II}^{-2} : [4^1]_7, 1^25^1$
$a = 21$	$(124)1_{I,6}^{-2}, 1^13^{-1}, 1^{-1}7^1$
$a = 22$	$(23^2)[1^{-1}2^1]_4, 1^{-1}11^1$

ТАБЛИЦА 5.9(ПРОДОЛЖЕНИЕ)

$a = 23$	$(123^2)1_{I,5}^3, 1^{-2}23^{-1}$
$a = 25$	$(340)1_{I,2}^2, 1^125^1$
$a = 27$	$(1^25)1_{II}^{-2}, 1^{-1}27^{-1}$
$a = 30$	$(125)[1^12^1]_4, 1^{-1}3^{-1}, 1^15^1$
$a = 35$	$(135)1_{II}^{-2}, 1^{-1}5^{-1}, 1^{-1}7^1$
$a = 36$	$(1^235)1_{II}^{-2} : [4^{-1}]_3, 1^{-2}9^{-1}$
$a = 37$	$(160)1_{I,6}^{-2}, 1^137^1$
$a = 42$	$(145)[1^{-1}2^1]_2, 1^{-1}3^1, 1^{-1}7^1$
$a = 43$	$(3^25)1_{II}^{-2}, 1^{-1}43^{-1}$
$a = 44$	$(13^25)1_{II}^{-2} : [4^1]_1, 1^{-2}11^{-1}$
$a = 45$	$(245)1_{I,6}^{-2}, 1^15^1, 1^{-1}9^1$
$a = 46$	$(136)[1^12^1]_4, 1^{-1}23^{-1}$
$a = 49$	$(236)1_{I,2}^2, 1^{-1}49^{-1}$

повторяется α раз. Рядом стоящие локальные символы вычисляются на основании табл. 5.1–5.4 и формулы (2.4).

ТАБЛИЦА 5.10

d	A	K
3	A_2	$1_{k-1} \oplus (3), k \leq 6$
4	(2^02)	$1_{k-2} \oplus (2^02), k \leq 6$
5	(2^13)	$1_{k-2} \oplus (2^13), k \leq 6$
6	(2^03)	$1_{k-1} \oplus (6), k \leq 3; A_2 \oplus (2)$
8	(3^13)	$1_{k-3} \oplus (2^13^12), k \leq 6$
	(2^04)	$1_{k-2} \oplus (2^04), k \leq 4$
9	(2^15)	$1_{k-1} \oplus (9), k \leq 3; 1_{k-2} \oplus (3^03), k \leq 4; A_2 \oplus A_2$
10	(2^05)	$1_{k-2} \oplus (2^05), k \leq 3; (2^12^04^{-1})_{II}; (2) \oplus A_4$

5.8. Вложения бинарных форм A или двумерных решеток в $\mathbb{Z}^n$ порождают новые ортогональные к ним формы K из п. 1.2. При этом необходимо наложить запрет на представимость 1 формой A , иначе от A отщепнется над $\mathbb{Z}$ прямое слагаемое 1 и мы вернемся к формам K из табл. 5.9.

Табл. 5.10 содержит приведенные бинарные формы $A = \begin{pmatrix} a & b \\ b & c \end{pmatrix} = (a^b \ c)$ с опре-

делителями $d = |A| \leq 10$ и 35 новых одноклассных форм K . Сами вложения $X : 1_n[X] = A$ легко восстанавливаются по A и K . Использованы сокращения: A_n для форм решеток, ортогональных к вектору (1^n) в $\mathbb{Z}^n$, например $A_2 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ – форма гексагональной решетки; и $(a^b \ c^f \ g^h)$ для тернарных форм с главной диагональю $(a \ c \ g)$ и дополнительной $(b \ f)$.

§ 6. Решетка корней E_8

6.1. *Решетка Госсета E_8* – это 8-мерная алмазная решетка, единственная четная унимодулярная решетка минимальной размерности. Она задает наплотнейшую из известных решетчатую упаковку шарами пространства $\mathbb{R}^8$. В *четной системе координат* решетка E_8 состоит из векторов $(x_1, \dots, x_8)$, все координаты которых – целые $x_i \in \mathbb{Z}$ или все полуцелые $x_i \in \mathbb{Z} + \frac{1}{2}$, и в последнем случае $x_1 + \dots + x_8 \equiv 0 \pmod{2}$. Векторы

$$(20^7), \ (-110^6), \ (0-110^5), \ \dots, \ (0^5-110), \ \left(\frac{1^8}{2}\right)$$

образуют базис E_8 , и по ним вычисляется матрица Грама $Q_{E_8} = (e_i \cdot e_j)$. Решетка E_8 имеет инварианты: определитель $d = 1$, число классов $h = 1$, число автоморфизмов $o(E_8) = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7$ и 2-символ 1_{II}^{+8} .

6.2. Форма Q_{E_8} четная, и поэтому она представляет над $\mathbb{Z}_2$ только четные формы A . Ограничимся $A = qA_q$, где $q = 2^\alpha$, $\alpha \geq 1$, и A_q – нечетное число, и вычислим с помощью табл. 3.1–3.3 2-символы ортогональных к вложениям A в Q_{E_8} форм K из п. 1.2. В табл. 6.1 указаны 2-символы форм $A = 2A_2$ и K , а в табл. 6.2 – форм $A = qA_q$, $\alpha \geq 2$. Отметим, что при вложении A в четные формы Q_{II} возникают одни и те же минимальные сцепляющие формы $J(qA_q)$, являющиеся в данном случае четными (см. табл. 3.2, 3.3).

ТАБЛИЦА 6.1

A	K
$2_{\text{I},1}^{+1}$	$1_{\text{II}}^{+6} 2_{\text{I},7}^{+1}$
$2_{\text{I},5}^{-1}$	$1_{\text{II}}^{-6} 2_{\text{I},7}^{+1}$
$2_{\text{I},3}^{-1}$	$1_{\text{II}}^{-6} 2_{\text{I},1}^{+1}$
$2_{\text{I},7}^{+1}$	$1_{\text{II}}^{+6} 2_{\text{I},1}^{+1}$

ТАБЛИЦА 6.2

A	K
$q_{\text{I},1}^{+1}$	$1_{\text{II}}^{+6} q_{\text{I},7}^{+1}$
$q_{\text{I},5}^{-1}$	$1_{\text{II}}^{+6} q_{\text{I},3}^{-1}$
$q_{\text{I},3}^{-1}$	$1_{\text{II}}^{+6} q_{\text{I},5}^{-1}$
$q_{\text{I},7}^{+1}$	$1_{\text{II}}^{+6} q_{\text{I},1}^{+1}$

6.3. Для нахождения одноклассных форм K подрешеток из E_8 применим метод п. 5.7, рассматривая над $\mathbb{Z}$ примитивные представления $X : Q_{E_8}[X] = a$ четных чисел $A = a$. Представления чисел $a = 2, 4, 6, 10, 12$ одноорбитные, а для $a = 8$ существуют две орбиты, одна из которых содержит $X = (2^2 0^6)$ – удвоенный вектор для $X_1 = (1^2 0^6)$ из E_8 . Следовательно, для $a = 8$ примитивные представления

ТАБЛИЦА 6.3

a	n	ν	M_k	K
2	240	$(\frac{1}{2}^8)$	E_7	$1_{\Pi}^6 2_{I,7}^1$
4	2160	$(2\ 0^7)$	D_7	$1_{\Pi}^6 4_{I,7}^1$
6	6720	$(2\ 1^2\ 0^5)$	$(2) \oplus E_6$	$1_{\Pi}^{-6} 2_{I,1}^1, 1^{-6} 3^1$
8	1780	$(2\ 1^4\ 0^3)$	A_7	$1_{\Pi}^6 8_{I,7}^1$
10	30240	$(3\ 1\ 0^6)$	$D_6 \oplus^{[1\frac{1}{2}]} (10)$	$1_{\Pi}^{-6} 2_{I,7}^1, 1^6 5^{-1}$
12	60480	$(2^3\ 0^5)$	$A_2 \oplus D_5$	$1_{\Pi}^6 4_{I,5}^{-1}, 1^{-6} 3^{-1}$

также образуют одну орбиту. По предложению 5.1 для указанных a ортогональные формы K (п. 1.2) одноклассные, и поскольку они представляются четной формой Q_{E_8} , то все K четные.

В табл. 6.3 векторы $v = (x_1, \dots, x_8)$ из E_8 с нормой $v \cdot v = x_1^2 + \dots + x_8^2$ содержат минимальное количество ненулевых координат, а столбец n дает число всех векторов v нормы a . В столбце M_K указаны по классификации [7] подрешетки из E_8 , ортогональные вектору v . В столбце K p -символы матриц Грама K вычисляются по табл. 6.1, 6.2 и формуле (2.4). Из шести решеток четыре $E_7, D_7, A_7, D_6 \oplus^{[1\frac{1}{2}]} (10)$ неразложимы над $\mathbb{Z}$.

Часть II. Ортогональные дополнения и формула веса представлений

§ 7. Ортогональные дополнения решеток

7.1. Рассмотрим представление

$$Q[X] = A \quad (7.1)$$

формы $A = \begin{pmatrix} A' & B \\ t_B & A'' \end{pmatrix}$, и пусть $X = (X' X'')$ разбито соответствующим образом. Из примитивности X вытекает разложение

$$X = U(Y' Y'') = \left(\begin{array}{ccc|ccc} 1 & & & * & & \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 1 & & \\ & & & & \ddots & \\ & & & & & 1 \\ \hline & & & 0 & & 0 \end{array} \right)$$

для некоторой матрицы $U \in \text{GL}_n(\mathbb{Z})$. Поэтому в X отдельные блоки $X' = UY'$ и $X'' = UY''$ также примитивны. Обратное утверждение для произвольных форм A неверно.

Наиболее важными для нас будут формы $A = \begin{pmatrix} A' & 0 \\ 0 & A'' \end{pmatrix}$ – прямые суммы двух форм A' и A'' . В этом случае матричное уравнение (7.1) распадается в систему

$$\begin{aligned} Q[X'] &= A', \\ {}^t X' Q X'' &= 0, \quad Q[X''] = A''. \end{aligned} \quad (7.2)$$

ЛЕММА 7.1. *При условии взаимной простоты определителей $|A'|$ и $|A''|$ представление X (7.1) примитивно тогда и только тогда, когда примитивны представления X' и X'' (7.2).*

ДОКАЗАТЕЛЬСТВО. Осталось проверить обратное утверждение. По условию для любого простого p по крайней мере один из определителей $|A'|$ или $|A''|$ не делится на p . Если это $|A'|$, то из первого представления (7.2), с точностью до эквивалентности над $\mathbb{Z}_p$, можем считать

$$Q = \begin{pmatrix} A' & 0 \\ 0 & Q'' \end{pmatrix}, \quad X' = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad X'' = \begin{pmatrix} X_2 \\ X_1 \end{pmatrix}.$$

Из ортогональности же ${}^t X' Q X'' = 0$ вытекает $X_2 = 0$ и, таким образом, $X = (X' X'') = \begin{pmatrix} 1 & 0 \\ 0 & X_1 \end{pmatrix}$ примитивно над всеми локальными кольцами $\mathbb{Z}_p$, а значит, и над $\mathbb{Z}$.

7.2. Предположим, что форма Q положительно определенная и определители форм Q , A' и A'' попарно взаимно простые. Обозначим $\text{pn}(A, Q; G)$ количество примитивных представлений X (7.1), для которых $K = K_X$ – ортогональное дополнение $K \perp X$ – удовлетворяет условию

$$\{K\} = \{aG^{-1}\} \quad (7.3)$$

(см. (1.11)). Здесь $\{\cdot\}$ обозначает класс эквивалентности форм над $\mathbb{Z}$. Используя (7.2) и лемму 7.1, получим разбиение

$$\text{pn}(A, Q; G) = \sum_{X'} \text{pn}(A'', K'; G) = \sum_{\{X'\}} |\{X'\}| \text{pn}(A'', K'; G),$$

где X' пробегает все примитивные представления $Q[X'] = A'$, $\{X'\}$ – соответствующая $O(Q)$ -орбита, где $O(Q) = O_{\mathbb{Z}}(Q)$, $|\{X'\}|$ – порядок орбиты и $K' = K'_{X'} \perp X'$. Поскольку порядок орбиты можно представить в виде

$$|\{X'\}| = \frac{o(Q)}{\text{stab}(X')}, \quad (7.4)$$

где $o(Q)$ и $\text{stab}(X')$ – порядки группы $O(Q)$ и стабилизатора $\text{Stab}(X')$ соответственно, то последнее равенство для $\text{pn}(A, Q; G)$ преобразуем к виду

$$\begin{aligned} \frac{\text{pn}(A, Q; G)}{o(Q)} &= \sum_{\{X'\}} \text{stab}(X')^{-1} \text{pn}(A'', K'; G) \\ &= \sum_{[K']} \sum_{\{K'_i\} \in [K']} \left(\sum_{\{X'\} \rightarrow \{K'_i\}} \text{stab}(X')^{-1} \right) \text{pn}(A'', K'_i; G). \end{aligned} \quad (7.5)$$

Теперь $[K']$ пробегает все роды форм $K' \perp X'$ и стрелка означает совпадение классов $\{K'_{X'}\} = \{K'_i\}$.

При условии одноклассности $h(Q) = 1$ рода $[Q]$ выражение, стоящее слева в уравнении (7.5), есть вес представлений формы A родом $[Q]$, ассоциированных с родом $[G]$. Если $h(Q) > 1$, то вес представлений получается суммированием по всем классам $\{Q_j\}$ из рода $[Q]$. Интересующие нас формы $Q = 1_n$ и E_8 одноклассные. Этим случаем и ограничимся. Для веса представлений $\text{pn}(A, Q; G)/o(Q)$ имеется общая формула [1, с. 102], и вместе с (7.5) они образуют источник необозримого числа формул для представлений конкретными формами.

7.3. Покажем, как действует указанная схема. Возьмем бинарную форму $A = \begin{pmatrix} A' & 0 \\ 0 & A'' \end{pmatrix} = \begin{pmatrix} 3 & 0 \\ 0 & A'' \end{pmatrix}$ и вложим ее в $Q = 1_7$. По табл. 5.9 для $a = A' = 3$ существует единственная орбита $\{X'\}$ с представителем $X' = (1^3 0^4)$. Порядок его стабилизатора равен $\text{stab}(X') = 3! \cdot 4! \cdot 2^4 = 2^8 \cdot 3^2$, ортогональное дополнение $K' = K'_{X'} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \oplus 1_4$, а формула (7.5) принимает вид

$$\frac{\text{pn}(A, Q; G)}{o(Q)} = \frac{\text{pn}(A'', K'; G)}{2^8 \cdot 3^2}. \quad (7.6)$$

Ограничимся нечетным бесквадратным блоком $A'' \not\equiv 0 \pmod{3}$. Согласно [1, формула (13.34)] вес представлений равен

$$\frac{\text{pn}(A, Q; G)}{o(Q)} = \frac{1}{2^4 \cdot 3^2 \cdot 5} \alpha_2(A, Q) (3^2 + \varepsilon_3) \prod_{p|A''} (p^2 + \varepsilon_p), \quad (7.7)$$

где

$$\varepsilon_3 = \varepsilon_1(A) \left(\frac{-1}{3} \right) = \left(\frac{-A''}{3} \right) = - \left(\frac{A''}{3} \right), \quad \varepsilon_p = \varepsilon_1(A) \left(\frac{-1}{p} \right) = \left(\frac{-3}{p} \right) = \left(\frac{p}{3} \right)$$

для $p \neq 3$. Четный множитель $\alpha_2(A, Q)$ вычисляется по формуле [1, (13.31)]

$$\alpha_2(A, Q) = \frac{1}{4} (1 \pm 2^{-2})$$

для $\text{oct} \equiv \pm 1$ или $\text{oct} \equiv \pm 3 \pmod{8}$ соответственно, где октановое число имеет вид

$$\text{oct} = \text{oct}(A, Q) \equiv t_1(Q) - t_1(A) + (4) \pmod{8}.$$

Здесь (4) означает 0 или 4 согласно условию $\left(\frac{3A''}{2}\right) = +1$ или $\left(\frac{3A''}{2}\right) = -1$, а странности у форм $Q = 1_7$ и $A = \begin{pmatrix} 3 & 0 \\ 0 & A'' \end{pmatrix}$ будут $t_1(Q) = t_1(1_7) = 7$, $t_1(A) = 3 + A''$. Вычисления показывают, что всегда $\text{oct} \equiv \pm 1 \pmod{8}$. Поэтому множителю $\alpha_2(A, Q)$ отвечает знак $+$, и $\alpha_2(A, Q) = 5/2^4$. Так как странности $t_1(Q)$ и $t_1(A)$ не сравнимы по $\text{mod } 8$, вложения форм A в Q не ветвятся. А так как по условию определитель $|A| = 3|A''|$ бесквадратный, то $\text{pn}(A'', K'; G) = n(A'', K')$, т.е. равен числу всех представлений формы A'' формой K' . Отсюда и из равенств (7.6), (7.7) вытекает следующий результат.

УТВЕРЖДЕНИЕ 7.1. Для нечетного бесквадратного числа A'' , не делящегося на 3, уравнение

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2x_5^2 + 2x_5x_6 + 2x_6^2 = A'' \quad (7.8)$$

имеет число целых решений $x_i \in \mathbb{Z}$, равное

$$n(A'', K') = \left(9 - \left(\frac{A''}{3}\right)\right) \prod_{p|A''} \left(p^2 + \left(\frac{p}{3}\right)\right). \quad (7.9)$$

Второй пример касается вложений формы $A = \begin{pmatrix} A' & 0 \\ 0 & A'' \end{pmatrix}$, где $A' = A_2 = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ — гексагональная форма и $\dim A'' = 1$. Чтобы коразмерности совпадали, возьмем $Q = 1_8$. Данный случай двойствен первому: $A_2 \perp 3$ для объемлющей тернарной формы 1_3 . Представления $Q[X'] = A'$ имеют одну орбиту $\{X'\}$ с представителем

$$X' = \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

для которого порядок стабилизатора равен $\text{stab}(X') = 2^5 \cdot 5! = 2^8 \cdot 3 \cdot 5$.

В прежних ограничениях на A'' сохраняется формула (7.7) с $\varepsilon_3 = \varepsilon_1(A) \left(\frac{-1}{3}\right) = \left(\frac{-1}{3}\right) \left(\frac{A''}{3}\right) \left(\frac{-1}{3}\right) = \left(\frac{A''}{3}\right)$ и $\varepsilon_p = \left(\frac{p}{3}\right)$ для простых $p \neq 3$. Странность $t_1(Q)$ равна нулю, а странность $t_1(A)$ равна A'' , $\text{ост} \equiv \pm 3 \pmod{8}$, множителю $\alpha_2(A, Q)$ соответствует знак $-$, и поэтому $\alpha_2(A, Q) = 3/2^4$. Для X' ортогональным дополнением будет $K = 3 \oplus 1_5$, что приводит к следующему результату.

УТВЕРЖДЕНИЕ 7.2. Для нечетного бесквадратного числа A'' , не делящегося на 3, уравнение

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + 3x_6^2 = A'' \quad (7.10)$$

имеет число решений

$$n(A'', K') = \left(9 + \left(\frac{A''}{3}\right)\right) \prod_{p|A''} \left(p^2 + \left(\frac{p}{3}\right)\right). \quad (7.11)$$

§ 8. Разделения родов. Неоднородные уравнения

Многоорбитные представления с ортогональными дополнениями из разных родов типичны и поэтому особенно интересны.

8.1. Рассмотрим представления $Q[X] = A$ одноклассной формой $Q = 1_6$ тернарной формы A бесквадратного определителя $|A|$. Вес представлений вычисляется по формуле [2, (13.34)]:

$$\frac{\text{pn}(A, Q; G)}{o(Q)} = \frac{1}{6} \alpha_2(A, Q; G) \prod_{\substack{p| |A| \\ p \neq 2}} (p + \varepsilon_1(A)). \quad (8.1)$$

Начнем со специализации $A = \begin{pmatrix} A' & 0 \\ 0 & A'' \end{pmatrix}$ с блоком $A' = 14$ и с блоком A'' , имеющим определитель $|A''|$, не делящийся на 2 и 7. Представления $X': Q[X'] = A'$ — распадаются на три орбиты с представителями

$${}^tX'_1 = (123000), \quad {}^tX'_2 = (112220), \quad {}^tX'_\Pi = (111113).$$

Ортогональные дополнения K'_i имеют определитель $|K'_i| = 14$ (1.13) и принадлежат двум родам: $K'_1, K'_2 \in [K'_I]$ — нечетному и $K'_\Pi \in [K'_\Pi]$ — четному роду. Для $p = 7$ эти роды имеют общий p -символ, равный $1^{-4}7^{-1}$ (2.4), а для $p = 2$ табл. 5.2 содержит символы $[1^4 2^1]_7$ для K'_I и $1^4_\Pi [2^1]_7$ для K'_Π . Подбирая минимальные базисы, находим матрицы Грама

$$K'_1 = 1_3 \oplus \begin{pmatrix} 3 & 1 \\ 1 & 5 \end{pmatrix}, \quad K'_2 = 1 \oplus 2 \oplus \begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 3 \end{pmatrix}, \quad K'_\Pi = \begin{pmatrix} 2 & 1 & 1 & 1 & 0 \\ 1 & 2 & 1 & 1 & 0 \\ 1 & 1 & 2 & 1 & 1 \\ 1 & 1 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 4 \end{pmatrix}.$$

Форма K'_2 не представляет единичную форму 1_3 , поэтому она не эквивалентна форме K'_1 . Форма $K'_\Pi = A_4 \oplus \begin{smallmatrix} [2 \frac{1}{5}] \\ 1 \end{smallmatrix} 70$ не приводима над $\mathbb{Z}$ [6].

Левая часть формулы (8.1) может включать представления всеми тремя формами K'_1, K'_2, K'_Π . Выбирая G , разведем эти формы на два рода. Минимальные вложения $J(A) = A'' \oplus J(A')$ находим по табл. 3.1. Разности $Q \ominus J(A)$ будут нечетными для A''_I с 2-символами $1_{I,4}^{-2}, 1_{I,2}^{\pm 2}$, или, более кратко, странность

$$t(A'') \equiv 2 \quad \text{или} \quad t(A'') \equiv 4 \pmod{8}. \quad (8.2)$$

Для $1_{I,4}^{-2}$ ортогональное дополнение K_I будет иметь 2-символ $[1^2 2^{-1}]_2$, для $1_{I,2}^{+2}$ — символ $[1^2 2^1]_1$ и для $1_{I,2}^{-2}$ — символ $[1^2 2^{-1}]_5$. Итак, разность $K_I = K'_I \ominus A''_I$ — снова нечетная форма, если блок A''_I удовлетворяет условию (8.2). Если же блок A''_Π четный, то разность $K_\Pi = K'_\Pi \ominus A''_\Pi$ четная, а разность $K'_I \ominus A''_\Pi$ нечетная. Если теперь положить $G = G_I$, где G_I отвечает форме K_I в силу (1.11), и соответственно $G = G_\Pi$, то левая часть формулы (8.1) будет содержать представления только одним родом $[K'_I]$ или $[K'_\Pi]$.

8.2. Для нечетного блока $A'' = A''_I$ по формуле (13.23) из [1] находим

$$\alpha_2(A_I, Q; G_I) = \frac{1}{8}(4 + \varepsilon_2), \quad \text{где} \quad \varepsilon_2 = \left(\frac{|A''|}{2} \right) \left(\frac{t(Q) - t(A)}{2} \right)$$

и $t(A)$ определяется из канонического 2-символа $2_A^{\text{can}} = [1^2 2^{* \cdot 1}]_{t(A)}$. Форма $A_I = A''_I \oplus 2 \cdot 7$ имеет символ $2_A = 1_{I,t}^{\varepsilon \cdot 2}$, где $\varepsilon = \left(\frac{|A''|}{2} \right)$, $t = t(A'')$. Странность $t(A)$ сравнима с 1, 5, 7 (mod 8) для A'' с символами $1_{I,2}^{+2}, 1_{I,2}^{-2}, 1_{I,4}^{-2}$ соответственно. Тогда $\varepsilon_2 = -1$ во всех этих случаях и $\alpha_2(A_I, Q; G_I) = 3/8$ для A_I с блоком A''_I (8.2). Аналогично, используя инварианты G_Π , находим $\alpha_2(A_\Pi, Q; G_\Pi) = 1/4$.

В силу (7.5) левая часть (8.1) редуцируется к представлениям формами K'_i :

$$\begin{aligned} \frac{\text{pn}(A_I, Q; G_I)}{o(Q)} &= \frac{\text{pn}(A'_I, K'_1; G_I)}{\text{stab}(X'_1)} + \frac{\text{pn}(A'_I, K'_2; G_I)}{\text{stab}(X'_2)}, \\ \frac{\text{pn}(A_{II}, Q; G_{II})}{o(Q)} &= \frac{\text{pn}(A''_{II}, K''_{II}; G_{II})}{\text{stab}(X'_{II})}, \end{aligned} \quad (8.3)$$

где порядки стабилизаторов равны $\text{stab}(X'_1) = 2^3 \cdot 3! = 48$, $\text{stab}(X'_2) = 2 \cdot 2! \cdot 3! = 24$, $\text{stab}(X'_{II}) = 5! = 120$. Ниже будет доказана формула (11.2), позволяющая находить порядки групп автоморфизмов

$$o(K'_i) = c(A', Q; G_i) \text{stab}(X'_i).$$

Для одноклассной формы $Q = 1_6$ получаем

$$c(A', Q; G_i) = c_2(A', Q; G_i) c_7(A', Q; G_i) = 1 \cdot 2 = 2$$

(см. ниже), что дает $o(K'_1) = 96$, $o(K'_2) = 48$, $o(K'_{II}) = 240$.

Осталось еще найти знаки $\varepsilon_1(A)$ в (8.1). Поскольку форма $A = A'' \oplus 1_4$, то $\varepsilon_1(A) = \left(\frac{|A''|}{7}\right)$ для $p = 7$ и $\varepsilon_1(A) = \varepsilon_1(A'') \left(\frac{14}{p}\right)$ для $p \neq 7$, делящих $|A''|$. По условию определитель $|A|$ бесквадратный и любое представление $X'' : K'_i[X''] = A''$ примитивное. Это обстоятельство и отсутствие ветвления позволяют заменить $\text{pn}(A'', K'_i; G_i)$ на число всех представлений $n(A'', K'_i)$ формы A'' формой K'_i . Объединяя (8.1) и (8.3), приходим к следующим формулам:

$$n(A'_I, K'_1) + 2n(A'_I, K'_2) = 3 \left(7 + \left(\frac{|A''|}{7} \right) \right) \prod_{p| |A''|} \left(p + \varepsilon_1(A'') \left(\frac{14}{p} \right) \right), \quad (8.4)$$

$$n(A''_{II}, K''_{II}) = 5 \left(7 + \left(\frac{|A''|}{7} \right) \right) \prod_{p| |A''|} \left(p + \varepsilon_1(A'') \left(\frac{14}{p} \right) \right), \quad (8.5)$$

где бинарные формы A''_i имеют бесквадратный определитель $|A''_i|$, не делящийся на 2 и 7, и нечетная форма A''_I удовлетворяет условию (8.2).

8.3. Применим ту же схему к нечетной тернарной форме

$$A = A_I = \begin{pmatrix} A' & B \\ {}^t B & A'' \end{pmatrix} = \begin{pmatrix} 2 & 1 & 0 \\ 1 & 2 & b \\ 0 & b & c \end{pmatrix}$$

положительно бесквадратного определителя $|A| = 3c - 2b^2$, не делящегося на 2 и 3, и, следовательно, $2 \nmid c$ и $3 \nmid b$. Снова вкладываем ее в форму $Q = 1_6$. Над $\mathbb{Z}_2$ форма A эквивалентна $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \oplus 3|A|$, и ее странность есть

$$t(A) \equiv 3|A| \pmod{8}. \quad (8.6)$$

Разность $Q \ominus A$ имеет странность $6 - 3|A| \not\equiv 0 \pmod{8}$. Поэтому для любого представления $X : Q[X] = A$ ортогональное дополнение K_I нечетное и род $[K_I]$, а значит, и род $[G_I]$ определены единственным образом. По формуле (13.34) из [1] находим

$$\frac{\text{pn}(A_I, Q; G_I)}{o(Q)} = \frac{1}{6} \alpha_2(A_I, Q; G_I) \prod_{p \mid |A|} (p + \varepsilon_1(A)), \quad (8.7)$$

а по формуле (13.31) из [1] получаем

$$\alpha_2(A_I, Q; G_I) = \frac{1}{8} (2 \pm 1)$$

при условиях $\text{oct} \equiv \pm 1$ или $\text{oct} \equiv \pm 3 \pmod{8}$ соответственно. Для $\left(\frac{|A|}{2}\right) = +1$ или $\left(\frac{|A|}{2}\right) = -1$ октановое число удовлетворяет сравнениям $\text{oct} \equiv t(Q) - t(A)$ или $\text{oct} \equiv t(Q) - t(A) + 4$ соответственно. Перебором находим $\text{oct} \equiv 1$ или $\text{oct} \equiv 3$, если $|A| \equiv 3$ или $|A| \equiv 1 \pmod{4}$.

Представления $Q[X'] = A' = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ образуют одну орбиту (см. табл. 5.10) с представителем

$${}^t X' = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Порядок его стабилизатора равен $\text{stab}(X') = 2^2 \cdot 3! = 48$. Левая часть равенства (8.7) примет вид

$$\frac{\text{pn}(A_I, Q; G_I)}{o(Q)} = \frac{\text{pn}_{X'}(A_I, Q; G_I)}{\text{stab}(X')}, \quad (8.8)$$

где $\text{pn}_{X'}(A_I, Q; G_I)$ есть число представлений $X = (X'X'') : Q[X] = A$ с фиксированным блоком X' . Матричное уравнение преобразуется к неоднородному уравнению

$$x_1^2 + x_2^2 + x_3^2 + 3x_4^2 - 2bx_4 = e, \quad (8.9)$$

где $e = c - b^2$. В новых обозначениях определитель формы A равен $b^2 + 3e$. Из (8.7) и (8.8) вытекает следующий результат.

УТВЕРЖДЕНИЕ 8.1. *Если бесквадратное число $|A| = b^2 + 3e > 0$ не делится на 2 и 3, то количество целых решений уравнения (8.9) равно*

$$n_{X'}(A_I, Q) = \left(2 - \left(\frac{-1}{|A|}\right)\right) \prod_{p \mid |A|} \left(p + \left(\frac{3}{p}\right)\right). \quad (8.10)$$

Отметим, что однородная часть $x_1^2 + x_2^2 + x_3^2 + 3x_4^2$ из (8.9) есть ортогональное дополнение K_I для X' и отказ от прямой суммы при выборе формы A приводит к замене K_I неоднородной формой.

Вид определителя формы A может быть источником постановки арифметических задач. Например, бинарная форма $A = \begin{pmatrix} 2 & p \\ p & p^2 + p \end{pmatrix}$, где p – нечетное простое число, имеет определитель $|A| = p(p + 2)$. Если p будет младшим близнецом, то $p + 2$ также простое и $|A|$ имеет ровно два простых делителя. Вкладывая форму A в тернарную форму $Q = 1_3$, а это возможно при $p \equiv 1 \pmod{8}$, придем к

неоднородному бинарному уравнению, аналогичному (8.9), из которого вытекает представление

$$p = \frac{2x_1^2 + x_2^2}{2x_1 + 1}.$$

Количество таких представлений равно восьми. Этот факт легко получить с помощью однородной формы $x_1^2 + 2x_2^2$. В общем же случае неоднородные формы имеют собственную область.

§ 9. Полнота рода

9.1. ПРЕДЛОЖЕНИЕ 9.1. Пусть $\{X'_i\}$ – орбиты всех примитивных вложений X'_i одноклассной формы A' в одноклассную форму Q , и пусть существует ортогональное дополнение $K'_1 \perp X'_1$ из некоторого рода $[K']$. Тогда классы $\{K'_i\}$, содержащиеся в $[K']$, образуют весь род.

ДОКАЗАТЕЛЬСТВО. Форма K'_1 представляется формой Q , и условия представимости родом $[Q]$, а значит, и Q носят локальный характер [1]. Поэтому вместе с K'_1 любая другая форма K'_j из рода $[K'] = [K'_1]$ также обладает данным свойством. Так как $A' \perp K'_1$ и из локальных рассуждений [1] вытекает существование вложений K'_j в Q , для которых ортогональное дополнение $A'_j \perp K'_j$ попадает в род $[A']$, то класс $\{A'_j\}$ совпадает с $\{A'\}$.

ЗАМЕЧАНИЕ 9.1. При малых размерностях $m = \dim A'$ условие $h(A') = 1$ неограничительно. Доказательство в одномерном случае, когда A' – числа, не вызывает затруднений.

9.2. Отказ от одноклассности $h(A') = 1$ заставляет искать ей замену в ограничениях на определитель формы A' . Один из вариантов:

$$Q = 1_n, \quad n \leq 8, \quad |A'| = p'_1 \dots p'_r \quad \text{и} \quad |A''| = p''_1 \dots p''_s \quad (9.1)$$

– бесквадратные нечетные взаимно простые определители, $A'' = A'_1$ – нечетная форма. Для представлений $X' : Q[X'] = A'$ все классы $\{K'_{X'}\}$ п. 7.2 принадлежат единственному нечетному роду $[K'_I]$ и еще, возможно, одному четному роду $[K'_{II}]$. Форма A'_1 не представима родом $[K'_{II}]$, и для $A = \begin{pmatrix} A' & 0 \\ 0 & A'' \end{pmatrix}$ по формуле (7.5) имеем

$$\frac{\text{pn}(A, Q; G)}{o(Q)} = \sum_{\{K'_i\} \in [K'_I]} \left(\sum_{\{X' \rightarrow \{K'_i\}\}} \text{stab}(X')^{-1} \right) \text{pn}(A'', K'_i; G). \quad (9.2)$$

Пусть $m = \dim A$ и $n - m = 1$. В данных условиях вес вычисляется по формуле (13.34) из [1]:

$$\frac{\text{pn}(A, Q; G)}{o(Q)} = \alpha_2(A, Q),$$

если A представима формой Q . Для веса представлений родом $[K'_I]$ та же формула принимает вид

$$\sum_{\{K'_i\} \in [K'_I]} o(K'_i)^{-1} \text{pn}(A'', K'_i; G) = 2^{-\alpha(|K'|)} \alpha_2(A'', K'_I),$$

где $\alpha(|K'|) = \alpha(|A'|) = r$ – количество нечетных простых делителей определителя $|K'| = |A'|$. Согласно формуле (12.17) из [1] оба $\alpha_2(\cdot)$ равны и ненулевые. Из (9.2) и двух последних формул вытекает соотношение

$$\begin{aligned} \sum_{\{K'_i\} \in [K'_1]} \left(\sum_{\{X'\} \rightarrow \{K'_i\}} \text{stab}(X')^{-1} \right) \text{pn}(A'', K'_i; G) \\ = 2^{\alpha(|A'|)} \sum_{\{K'_i\} \in [K'_1]} o(K'_i)^{-1} \text{pn}(A'', K'_i; G) \end{aligned} \quad (9.3)$$

при условии (9.1) и $n - m = 1$. Фиксируем произвольную форму $K' = K'_j$ и найдем форму A'' коразмерности один, представимую формой K' и не представимую любой другой формой K'_i , $i \neq j$. Ограничения (9.1) на форму A'' не допускают применение результата Китаока [8]. Рассуждение проведем, уменьшая размерность $k = n - \dim A'$ форм K'_i определителя $|K'| = p'_1 \dots p'_r$.

В случае $k \geq 5$ выберем простое $p'' = p'_1$, отличное от любого p'_i (9.1), $p'' \equiv 1 \pmod{4}$, если количество простых $p'_i \equiv 3 \pmod{4}$ нечетное, и $p'' \equiv 3 \pmod{4}$ в противном случае. Простое p'' представимо над всеми $\mathbb{Z}_p$ формой K' . Если $k \geq 4$ и p'' больше некоторого N , зависящего от K' , то p'' представимо (примитивно) формой K' и над $\mathbb{Z}$ [5, с. 224]. Для $X'' : K'[X''] = p''$ форма $K'' \perp X''$ нечетная, если p'' не сравнима со странностью $t(K') \pmod{8}$. Наложим данное ограничение при выборе p'' . Если $k - 1 \geq 5$, процесс повторяем.

Для $k = 4$ любое простое $p'' \geq N$ представимо формой K' над $\mathbb{Z}$. Обозначим $\varepsilon_i = \varepsilon_1(K')$ знаки в p'_i -символах $1^{\varepsilon_i}(p'_i)^{\pm 1}$ формы K' . Форму K'' можем выбрать нечетной с помощью p'' , и ее p'_i -знаки суть $\varepsilon_1(K'') = \varepsilon_i\left(\frac{p''}{p'_i}\right)$. Для простого p'' по (2.4) форма K'' имеет разложение: $K'' = (K' \ominus J(p'')) \oplus (-p'')$, и ее p'' -знак равен

$$\varepsilon = \varepsilon_1(K'') = \varepsilon_1(K')\varepsilon_1(J(p'')) = \left(\frac{p'_1 \dots p'_r}{p''}\right) \cdot \left(\frac{-1}{p''}\right).$$

Нам нужно найти p'' , для которого приведенные знаки равнялись бы $-\left(\frac{-1}{p'_i}\right)$, $i = 1, \dots, r$, и $-\left(\frac{-1}{p''}\right)$, или

$$\left(\frac{p''}{p'_i}\right) = \varepsilon_i\left(\frac{-1}{p'_i}\right), \quad i = 1, \dots, r, \quad \left(\frac{p'_1 \dots p'_r}{p''}\right) = -1. \quad (9.4)$$

Принимая во внимание закон взаимности, получаем

$$\left(\frac{p'_i}{p''}\right) = \delta(p'_i, p'')\left(\frac{p''}{p'_i}\right),$$

где $\delta(p'_i, p'') = -1$ для $p'_i \equiv p'' \equiv 3 \pmod{4}$ и $\delta(p'_i, p'') = 1$ в оставшихся случаях. Второе условие (9.4) преобразуем к виду

$$\prod_i \left(-\varepsilon_i\left(\frac{-1}{p'_i}\right)\right) \prod_{p'_i \equiv 3 \pmod{4}} \delta(p'_i, p'') = -1. \quad (9.5)$$

Если количество простых $p'_i \equiv 3 \pmod{4}$ нечетно, простое p'' с условием (9.5) существует. В противном случае наложим на K' ограничение

$$\prod_i \left(-\varepsilon_i \left(\frac{-1}{p'_i} \right) \right) = -1, \quad (9.6)$$

если $\dim K' = 4$ и количество $p'_i \equiv 3 \pmod{4}$ четное. Для размерностей $\dim K' \geq 5$ можно свести рассуждение к нечетному случаю.

При $k = 3$ на знаки $\varepsilon_1(K') = \varepsilon_i$ формы $K' = K'_1$, имеющей определитель $|K'| = p'_1 \dots p'_r$, наложим ограничение

$$\varepsilon_1(K') = -\left(\frac{-1}{p'_i} \right), \quad i = 1, \dots, r. \quad (9.7)$$

Если $K' = \begin{pmatrix} a & b & f \\ b & c & e \\ f & e & d \end{pmatrix}$ и существует простое p , делящее наибольший общий делитель (a, b, c) , то такое p делит $|K'|$, $p \neq 2$, $p = p'_i$ и p делит f и e . Иначе, например,

$$K' \sim_p \begin{pmatrix} a & f \\ f & d \end{pmatrix} \oplus pK'_p$$

и $\varepsilon_1(K') = \left(\frac{-f^2}{p} \right) = \left(\frac{-1}{p} \right)$, что противоречит условию (9.2). Следовательно, бинарная форма $\begin{pmatrix} a & b \\ b & c \end{pmatrix}$ примитивна и примитивны формы $\begin{pmatrix} a & f \\ f & d \end{pmatrix}$, $\begin{pmatrix} c & e \\ e & d \end{pmatrix}$. Одна из этих форм нечетная. Она представляет нечетное простое $p'' \not\equiv t_1(K') \pmod{8}$, отличное от всех p'_i , $i = 1, \dots, r$. Тогда бинарная форма $K'' \perp X''$ нечетная с определителем $|K''| = p'_1 \dots p'_r p''$.

В последнем нетривиальном случае $k = 2$ нечетная бинарная форма $K' = K'_1$ (или четная) всегда представляет нечетное простое p'' , отличное от p'_i (или $2p''$).

Идея разделения классов в роде $[K'_1]$ основана на редуцировании к бинарным формам. Пусть фиксирована форма $K' = K'_1$ и $K'_1[X''_1] = p''_1, \dots, K'_s[X''_s] = p''_s -$ представления нечетного простого $p = p''_1$, отличного от всех p'_i , классами $\{K'_i\}$ из рода $[K'_1]$.

Решения уравнения (1.3) образуют двухэлементную $O_{\mathbb{Z}}(G)$ -орбиту $\{C\}$. По [1, теорема 2.1] существует биекция

$$\{X''\} \xrightarrow{\sim} \{G\} \quad (9.8)$$

между $O_{\mathbb{Z}}(K'_i)$ -орбитами $\{X''\}$ представлений p всеми классами рода $[K'_1]$ и классами $\{G\}$ форм $\{G\}$, для которых форма $Q_G^p(C)$ (1.4) эквивалентна какой-либо форме K'_i . Если размерность $k \geq 4$, то все классы $\{G\}$ принадлежат нечетному роду $[G_I]$ и, возможно, четному роду $[G_{II}]$. При $k = 3$ возможны все три комбинации. По формуле (1.11) формы $K'' \perp X''_i$ и G связаны соотношением $K'' = aG^{-1}[U]$, где $a = p$, aG^{-1} и U – целые матрицы и $|K''| = |aG^{-1}|$. Следовательно,

$$K'' \sim_{\mathbb{Z}} aG^{-1} \quad (9.9)$$

и существует биекция

$$\{G\} \xrightarrow{\sim} \{K''\}. \quad (9.10)$$

Композиция (9.8) и (9.10) задает новую биекцию

$$\{X''\} \xrightarrow{\sim} \{K''\}, \text{ где } K'' \perp X''. \quad (9.11)$$

Продолжая выбирать $p = p_2'', \dots$ и отсекая четные роды $[K_{II}'']$, доходим до некоторой бинарной формы K'' , нечетной или четной, представимой формой $K' = K_1'$. Все такие формы принадлежат одному из двух родов $[K_I'']$ или $[K_{II}'']$. На последнем шаге выбираем число $q = p''$ или $q = 2p''$, представимое формой K'' . В этом случае такое число q представимо единственной формой K'' . Диагональная форма $A'' = \text{diag}(p_1'', p_2'', \dots, q)$ представляется только формой $K' = K_1'$.

ЗАМЕЧАНИЕ 9.2. Из приведенной конструкции не вытекает биекция $\{X\} \xrightarrow{\sim} \{K_j''\}$ между орбитами представлений формы A'' родом $[K_1']$ и классами бинарных форм K_j'' . Но конструкция проливает свет на то, как эти $2^{k-2}h$ орбиты $\{X\}$ устроены, где h – число классов $\{K_j''\}$.

ПРЕДЛОЖЕНИЕ 9.2. Пусть форма $Q = 1_n$, $n \leq 8$, представляет форму A' нечетного бесквадратного определителя, $Q[X'] = A'$, и пусть род $[K_1']$ ортогональной к X' нечетной формы K_1' удовлетворяет условиям (9.6) или (9.7), если размерность k формы K_1' равна 4 или 3. Тогда ортогональные дополнения K_i' из $[K_1']$ всех представлений формы A' формой Q образуют полный род $[K_1']$.

ДОКАЗАТЕЛЬСТВО. В правой части формулы (9.3) присутствуют все классы $\{K_i'\}$ форм рода $[K_1']$. По доказанному существует форма A'' размерности $k - 1$, представимая только произвольной фиксированной формой K_j' из рода $[K_1']$. Левая часть формулы (9.3) ненулевая тогда и только тогда, когда ненулевой будет сумма

$$\sum_{\{X'\} \rightarrow \{K_j'\}} \text{stab}(X')^{-1}, \quad (9.12)$$

что равносильно появлению формы K_j' , ортогональной к некоторому представлению X' формы A' формой Q .

ЗАМЕЧАНИЕ 9.3. В терминах тета-рядов $\theta^{k-1}(Z, K_i')$ рода $k - 1$ и веса $k/2$ существование указанной формы A'' означает их линейную независимость. Ранее, с другой идеей, доказательство линейной независимости получил Китаока [8].

§ 10. Орбитальная масс-формула

Из доказательства предложения 9.2 сразу же вытекает равенство взвешенной суммы орбит (9.12) и взвешенного числа $2^{\alpha(|A'|)} o(K_i')^{-1}$ делителей определителя формы A' . Если мы откажемся от требования полноты рода, то равенство приобретет естественную общность.

10.1. Снова исходим из формы Q , примитивно представляющей форму A' с взаимно простым с $|Q|$ определителем $|A'|$. Если $Q[X'] = A'$, обозначим $K' = K'_{X'}$ ортогональную к представлению X' форму, и пусть ее род разбит на классы $[K'] = \bigcup_i \{K'_i\}$. Принадлежность формы $K'_{X'}$ классу $\{K'_i\}$ по-прежнему изображаем стрелкой, т.е. $\{X'\} \rightarrow \{K'_i\}$. Пусть $C(A', Q; G_i)$ обозначает множество решений $C \bmod A$ сравнения (см. п. 1.1)

$$E[C] \equiv -G_i \pmod{a}, \quad (10.1)$$

где $E = a(A')^{-1}$, $\{G_i\}$ соответствует классу $\{K'_i\}$ по (8.10) и форма (1.4) $Q_{G_i}^A(C) \sim Q$. Для орбит $\{X'\} \rightarrow \{K'_i\}$ существует биекция [1, с. 38]

$$\{X'\} \xrightarrow{\sim} \{C\} \quad (10.2)$$

с орбитами $\{C\} = \{CM \bmod A : M \in O_{\mathbb{Z}}(G_i)\}$ решений C из множества $C(A', Q; G_i)$. *Порядок* орбиты $\{C\}$ равен

$$|\{C\}| = o(G_i) / \text{stab}(C), \quad (10.3)$$

где $\text{stab}(C)$ – порядок стабилизатора $\text{Stab}(C)$, состоящего из автоморфизмов M группы $O_{\mathbb{Z}}(G_i)$ с условием $CM \equiv C \pmod{A}$. Из доказательства теоремы 2.1 из [1] следует, что биекцию (10.2) между орбитами можно поднять до изоморфизма их групп стабилизаторов

$$\text{Stab}(X') \xrightarrow{\sim} \text{Stab}(C). \quad (10.4)$$

Разбивая решения $C(A', Q; G_i)$ на орбиты $\{C\}$ и затем используя (10.3) и (10.4), приходим к равенству

$$c(A', Q; G_i) = \sum_{\{X'\} \rightarrow \{K'_i\}} o(G_i) \text{stab}(X')^{-1}.$$

Из него естественно возникает интересующая нас сумма (9.12):

$$\sum_{\{X'\} \rightarrow \{K'_i\}} \text{stab}(X')^{-1} = c(A', Q; G_i) o(G_i)^{-1}. \quad (10.5)$$

Это равенство есть *орбитальная масс-формула* для веса орбит $\{X'\}$ примитивных представлений $Q[X'] = A'$ с ортогональными дополнениями $K'_{X'}$ из класса $\{K'_i\}$. Формула (10.5) справедлива только при условии существования представлений X' .

ЗАМЕЧАНИЕ 10.1. Для *неопределенных* форм Q масс-формулу нужно преобразовать к виду

$$\sum_{\{X'\} \rightarrow \{K'_i\}} [O(G_i) : \text{Stab}(X')] = c(A', Q; G_i). \quad (10.6)$$

При этом считаем стабилизатор $\text{Stab}(X')$ вложенным в группу автоморфизмов $O_{\mathbb{Z}}(G_i)$ относительно изоморфизма (10.4).

10.2. Число решений $c(A', Q; G)$ сравнения (9.1) факторизуется:

$$c(A', Q; G) = \prod_{p|a} c_p(A', Q; G), \quad (10.7)$$

для одноклассных форм Q . Множители $c_p(A', Q; G)$ представляют собой число решений $C \bmod A' \mathbb{Z}_p$ сравнений

$$E[C] \equiv -G \pmod{p^\alpha \mathbb{Z}_p} \quad (10.8)$$

с условием $Q_G^{A'}(C) \sim_p Q$, а p^α – наибольшая степень, входящая в ступень a формы A' . Для четной $Q = Q_\Pi$ и $p = 2$ предполагается, что матрица $2^{-\alpha}(E[C] + G)$ имеет четную диагональ. Определители $|Q|$ и $|A'|$ по-прежнему считаются взаимно простыми. В [1, с. 60] для нечетных p доказано, что

$$c_p(A', Q; G) = o(q(A')), \quad (10.9)$$

т.е. равно порядку группы автоморфизмов $O(q(A'))$ [1, (10.17)], состоящей из матриц $U \bmod A_{\geq p}$, где $A' = A_1 \oplus A_{\geq p}$ (см. п. 2.1), из $\text{GL}(\mathbb{Z})$, удовлетворяющих сравнению $A_{\geq p}^{-1}[U] \equiv A_{\geq p}^{-1} \pmod{\mathbb{Z}_p}$.

Для нечетных p согласно [1, с. 83] $o(q(A')) = 2$ в случае $\dim A_{\geq p} = 1$ и $o(q(A')) = 2(p - (\frac{-|A_p|}{p}))$, когда блок $A_{\geq p} = pA_p$ двумерный.

Для $p = 2$ рассмотрим только формы $Q = 1_n$, $n \leq 8$, и E_8 . В случае $Q = 1_n$ из табл. 5.1 вытекает равенство $c_2(A', Q; G) = 1$ для $2_{A'} = 1_{I,t}^{\pm 1}$. Если 2-символ равен $2_{A'} = 2_{I,t}^{\pm 1}$, по табл. 5.2 находим формы G и для числа решений сравнения (10.8) получаем равенство $c_2(A', Q; G) = 1$ для размерностей $n \geq 3$. Аналогично, при $2_{A'} = 4_{I,t}^{\pm 1}$ по табл. 5.3 находим $c_2(A', Q; G) = 2$ для $n \geq 4$, и при $2_{A'} = q_{I,t}^{\pm 1}$ из табл. 5.4 получаем $c_2(A', Q; G) = 4$ для $n \geq 5$. В двумерном случае $2_{A'} = 1_{I,t}^{\pm 2}$ или $2_{A'} = 1_{\Pi}^{\pm 2}$ всегда $c_2(A', Q; G) = 1$, а для $2_{A'} = 2_{I,t}^{\pm 2}$ согласно п. 4.1 $C = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, поэтому $c_2(A', Q; G) = 2$. Трудный случай четных форм A' с 2-символами $2_{A'} = 2_{\Pi}^{\pm 2}$ опускаем. Для формы A' решетки E_8 будем иметь $c_2(A', Q; G) = 1$ или $c_2(A', Q; G) = 2$ соответственно для $2_{A'} = 2_{I,t}^{\pm 1}$ или $2_{A'} = q_{I,t}^{\pm 1}$ степени $q = 2^\alpha$, $\alpha \geq 2$.

Полученные формулы объединяет

ЛЕММА 10.1. Если форма $A' = A_1 \oplus A_{\geq p}$ имеет определитель $|A'|$, взаимно простой с $|Q|$, то для числа решений $c_p(A', Q; G)$ сравнения (10.8) выполняются следующие равенства.

Для p нечетного:

$$\begin{aligned} c_p(A', Q; G) &= 2, & \text{если } A_{\geq p} &= p^\alpha A_{p^\alpha}, \quad \dim A_{p^\alpha} = 1, \\ c_p(A', Q; G) &= 2 \left(p - \left(\frac{-|A_p|}{p} \right) \right), & \text{если } A_{\geq p} &= pA_p, \quad \dim A_p = 2. \end{aligned} \quad (10.10)$$

Для $p = 2$ и любой формы Q :

$$c_2(A', Q; G) = 1, \quad \text{если } |A'| \not\equiv 0 \pmod{2}; \quad (10.11)$$

для $Q = 1_n$, $n \leq 8$:

$$\begin{aligned} c_2(A', Q; G) &= 1, \quad \text{если } A_{\geq 2} = 2A_2, \quad \dim A_2 = 1, \quad n \geq 3, \\ c_2(A', Q; G) &= 2, \quad \text{если } A_{\geq 2} = 4A_4, \quad \dim A_4 = 1, \quad n \geq 4, \\ c_2(A', Q; G) &= 4, \quad \text{если } A_{\geq 2} = qA_q, \quad q = 2^\alpha, \quad \alpha \geq 3, \quad \dim A_q = 1, \quad n \geq 5, \\ c_2(A', Q; G) &= 2, \quad \text{если } A_{\geq 2} = 2A_2, \quad \dim A_2 = 2; \end{aligned} \quad (10.12)$$

для $Q = E_8$:

$$\begin{aligned} c_2(A', Q; G) &= 1, \quad \text{если } A_{\geq 2} = 2A_2, \quad \dim A_2 = 1, \\ c_2(A', Q; G) &= 2, \quad \text{если } A_{\geq 2} = qA_q, \quad q = 2^\alpha, \quad \alpha \geq 2, \quad \dim A_q = 1. \end{aligned} \quad (10.13)$$

10.3. Просуммируем равенства (10.5) по классам $\{K'_i\}$ произвольного рода $[K']$ ортогональных дополнений K'_i примитивных представлений $Q[X'] = A'$:

$$\sum_{\{K'_i\} \in [K']} \sum_{\{X'\} \rightarrow \{K'_i\}} \text{stab}(X')^{-1} = \sum_{\{G_i\} \in [G]} c(A', Q; G_i) o(G_i)^{-1}. \quad (10.14)$$

Для одноклассных форм Q ввиду (10.7) и (10.8) множители $c(A', Q; G_i)$ зависят лишь от локальных характеристик G_i над $\mathbb{Z}_p$, т.е. от рода $[G_i]$. Сумму из $o(G_i)^{-1}$ для всех классов рода $[G]$ можно заменить на *массу*

$$m(K') = \sum_{\{K'_i\} \in [K']} o(K'_i)^{-1} \quad (10.15)$$

рода $[K']$ (см. [1, с. 83]), так как формы G_i и K'_i имеют изоморфные группы автоморфизмов в силу эквивалентности (9.9).

ТЕОРЕМА 10.1. В условиях одноклассности $h(Q) = 1$ формы Q и взаимной простоты определителей $|Q|$ и $|A'|$ выполняется орбитальная масс-формула

$$\sum_{\{X'\} \rightarrow [K']} \text{stab}(X')^{-1} = c(A', Q; G) m(K'), \quad (10.16)$$

если классы ортогональных дополнений $K'_{X'} \perp X'$ примитивных представлений $X' : Q[X'] = A'$ образуют полный род $[K']$. Множитель $c(A', Q; G)$ вычисляется по формуле (10.7) и лемме 10.1.

ЗАМЕЧАНИЕ 10.2. Формулу (10.16) можно использовать для проверки полноты списка орбит $\{X'\}$ примитивных представлений $Q[X'] = A'$, а массу рода $m(K')$ вычислять по известной масс-формуле [7].

В случае, когда орбиты $\{X'\}$ легко находить, например для форм $Q = 1_n$ с простой группой автоморфизмов $O(1_n)$, получаем практически альтернативный способ вычисления массы рода $m(K')$.

§ 11. Порядки групп автоморфизмов

11.1. Порядки стабилизаторов $\text{stab}(X')$ примитивных представлений X' : $Q[X'] = A'$ вычисляются непосредственно или по формуле

$$\text{stab}(X') = o(Q)/n(A', Q), \quad (11.1)$$

если представления X' образуют одну орбиту и $n(A', Q)$ – длина орбиты $|\{X'\}|$ или количество представлений формы A' формой Q . Зная порядок стабилизатора, по формуле (10.5) можно находить порядки групп автоморфизмов $O_{\mathbb{Z}}(K'_i)$, изоморфных по (9.9) группам $O_{\mathbb{Z}}(G_i)$.

ПРЕДЛОЖЕНИЕ 11.1. Если формы Q и A' имеют взаимно простые определители, примитивные представления $X' : Q[X'] = A'$ образуют одну орбиту $\{X'\}$, то порядок группы автоморфизмов ортогонального дополнения $K' \perp X'$ вычисляется по формуле

$$o(K') = c(A', Q; G) \text{stab}(X'). \quad (11.2)$$

11.2. Табл. 6.3 содержит полный список подрешеток M коразмерности 1 из E_8 , ортогональных одномерным решеткам четной нормы $A' = a \leq 12$. С помощью формул (11.1) и (11.2) вычислим их группы автоморфизмов.

Пусть Q_{E_8} – матрица Грама решетки E_8 . Уравнение $Q_{E_8}[X'] = A'$ для $A' = 2$ имеет по табл. 6.3 число решений $n(2, Q_{E_8}) = 240 = 2^4 \cdot 3 \cdot 5$. Все они образуют одну орбиту $\{X'\}$ с представителем $(\frac{1}{2}, \frac{8}{2})$, для которого ортогональное дополнение есть плотнейшая известная решетка Госсета E_7 . Объемлющая решетка E_8 имеет группу автоморфизмов порядка [6, с. 157]

$$o(E_8) = 2^{14} \cdot 3^5 \cdot 5^2 \cdot 7.$$

По формуле (11.1) находим порядок стабилизатора

$$\text{stab}(X') = o(E_8)/n(2, Q_{E_8}) = 2^{10} \cdot 3^4 \cdot 5 \cdot 7,$$

а по формулам (10.7) и (10.13) – множитель $c(2, Q_{E_8}; G) = 1$. Таким образом, формула (11.2) дает известный порядок [6, с. 162]

$$o(E_7) = 2^{10} \cdot 3^4 \cdot 5 \cdot 7$$

для решетки E_7 .

Опустим вычисления для $A' = 4$ и $A' = 8$. Их ортогональные дополнения – известные шахматная решетка D_7 и решетка с нулевой суммой A_7 .

Перейдем к $A' = 6$ с ортогональным дополнением $(2) \oplus E_6$ – прямой суммой одномерной решетки (2) и шестимерной решетки Госсета E_6 , имеющей определитель, равный 3. Так как $n(6, Q_{E_8}) = 2^6 \cdot 3 \cdot 5 \cdot 7$, то

$$\text{stab}(X') = o(E_8)/n(6, Q_{E_8}) = 2^8 \cdot 3^4 \cdot 5,$$

что совпадает с порядком $o(E_6) = 2^8 \cdot 3^4 \cdot 5$ [6, с. 164]. Согласно формулам (10.7), (10.10) и (10.13) имеем

$$c(6, Q_{E_8}; G) = c_2(6, Q_{E_8}; G) \cdot c_3(6, Q_{E_8}; G) = 2.$$

Тогда по формуле (11.2) получаем соотношение

$$o((2) \oplus E_6) = 2^9 \cdot 3^4 \cdot 5 = 2 \cdot o(E_6),$$

следствием которого является тот факт, что группа автоморфизмов суммы решеток $(2) \oplus E_6$ есть прямое произведение групп автоморфизмов ее составляющих подрешеток (2) и E_6 .

Для оставшихся $A' = 10$ и $A' = 12$ находим, что их ортогональные дополнения: $D_6 \oplus^{[1\frac{1}{2}]}(10)$ – четная неразложимая решетка определителя 10 и $A_2 \oplus D_5$ с гексагональной составляющей A_2 , имеют равные порядки групп автоморфизмов

$$\begin{aligned} o(D_6 \oplus^{[1\frac{1}{2}]}(10)) &= 2^{10} \cdot 3^2 \cdot 5, \\ o(A_2 \oplus D_5) &= 2^{10} \cdot 3^2 \cdot 5 = o(A_2) \cdot o(D_5). \end{aligned}$$

§ 12. Дополнение до полного рода

Ватсон [9] нашел все четные одноклассные $h(K) = 1$ кватернарные формы K с *ограничением*: если p^2 делит определитель $|K|$ и $p^{-2}|K| \equiv 0$ или $p^{-2}|K| \equiv 1 \pmod{4}$, то K эквивалентна над $\mathbb{Z}_p$ прямой сумме $K_1 \oplus pK_p$ бинарных форм K_1 и K_p . Список Ватсона содержит 27 таких форм K , среди них содержится форма

$$K = \begin{pmatrix} 2 & 1 & 0 & 1 \\ 1 & 2 & 0 & 1 \\ 0 & 0 & 2 & 1 \\ 1 & 1 & 1 & 4 \end{pmatrix}, \quad (12.1)$$

имеющая определитель $|K| = 17$, с p -символами $2_K = 1_{\Pi}^{+4}$, $17_K = 1^{-3}17^{-1}$. Покажем, как можно проверить одноклассность рода $[K]$ формы (12.1).

Вложим форму K в форму $Q = 1_n$ минимальной возможной размерности n . Формы 1_n для $n \leq 8$ одноклассные, и вложение над $\mathbb{Z}$ существует тогда и только тогда, когда существуют вложения над всеми $\mathbb{Z}_p$. Для $p = 2$ находим разности 2-символов из п. 2.3:

$$1_{I,5}^{+5} \ominus 1_{\Pi}^{+4} = 1_{I,5}^{+1}, \quad 1_{I,6}^{+6} \ominus 1_{\Pi}^{+4} = 1_{I,6}^{+2}.$$

Существует только второй символ, значит, $n \geq 6$. Для $p = 17$ форма K эквивалентна над $\mathbb{Z}_{17}$ прямой сумме $K_1 \oplus pK_p$ с блоками размерностей $\dim K_1 = 3$ и $\dim K_p = 1$. Минимальное вложение для таких форм K имеет вид [4]

$$K \xhookrightarrow{\mathbb{Z}_p} \left(\begin{array}{c|ccc} K_1 & & & \\ \hline & pK_p & 1 & \\ & & 1 & 0 \end{array} \right) = K_1 \oplus \begin{pmatrix} pK_p & 1 \\ 1 & 0 \end{pmatrix}.$$

Размерность вложения равна пяти, и $\left(\frac{|K_1|}{17}\right)\left(\frac{-1}{17}\right) = -1$. Поскольку $\left(\frac{1_n}{17}\right) = +1$, то снова получим $n \geq 6$. Представление $X'': 1_6[X''] = K$ – находим прямым вычислением:

$${}^t X'' = \begin{pmatrix} 11 & 00 & 00 \\ 10 & 10 & 00 \\ 00 & 00 & 11 \\ 01 & 11 & 10 \end{pmatrix}.$$

Двумерное ортогональное дополнение A' для K вычисляем по его базису

$${}^t X' = \begin{pmatrix} 0 & 0 & 0 & 1 & -1 & 1 \\ -1 & 1 & 1 & -1 & -1 & 1 \end{pmatrix}$$

Он дает форму $A' = \begin{pmatrix} 3 & 1 \\ 1 & 6 \end{pmatrix}$, имеющую определитель $|A'| = 17$, совпадающий с определителем самой формы K . Это указывает на правильность выбора базиса X' . Полученная форма A' одноклассная, $h(A') = 1$. Группа автоморфизмов $O_{\mathbb{Z}}(1_n)$ порождается $n!$ перестановками и 2^n сменами знаков. Используя эти автоморфизмы, выбираем более симметричное представление

$${}^t X'_{\text{sym}} = \begin{pmatrix} 11 & -10 & 00 \\ \underbrace{11}_{2!} & 1 \underbrace{11}_{3!} \end{pmatrix}$$

формы A' формой 1_6 . Для него $\text{stab}(X'_{\text{sym}}) = 2! \cdot 3! = 12$.

Проверим, что представления $X': 1_6[X'] = A'$ образуют одну орбиту $\{X'\}$. Для второй строки в ${}^t X'_{\text{sym}}$ существует еще только один вариант $(1 \ 1 \ 2 \ 0 \ 0 \ 0)$. Ортогональное дополнение $K \perp X'$ четное. Следовательно, в представлении X' не должно быть ни одного нулевого столбца $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$. Отсутствие же его не совместимо с условием, что скалярное произведение строк в X' равно 1. Из предложения 9.1 вытекает одноклассность $h(K) = 1$ формы Ватсона (12.1). Что касается ее автоморфизмов, то по формулам (11.2), (10.7) и (10.10) $o(K) = 2 \cdot 12 = 24$.

В более общей ситуации приведенный метод позволяет по одному представителю K находить полный список форм рода $[K]$, т.е. восстанавливать род по отдельному представителю. Форма K (12.1) есть ортогональное дополнение в $Q = 1_6$ бинарной формы $A' = \begin{pmatrix} 3 & 1 \\ 1 & 6 \end{pmatrix}$. Этот факт дает основание для классификации форм K и объясняет важность знания унимодулярных решеток $\mathbb{Z}^n$, E_n и др. Еще одним важным обстоятельством является возможность исходное уравнение $K[X] = a$ записать в виде симметричной и удобной для вычислений системы

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 + x_6^2 &= a, \\ x_1 + x_2 + x_3 + x_4 + x_5 + x_6 &= 0, \\ x_1 + x_2 - x_3 &= 0. \end{aligned}$$

Отсюда, например, сразу видно, что M_K – подрешетка из A_5 , ортогональная вектору $(1 \ 1 \ -1 \ 0 \ 0 \ 0)$.

Заключение

В [1] доказана общая формула для веса примитивных представлений

$$\text{pn}(A, [Q]; G) = m(G) \cdot c(A, [Q]; G)$$

формы A родом положительно определенных квадратичных форм $[Q]$, ассоциированных с дополнительным родом $[G]$ (см. ниже (3.1)). В правой части стоят вес $m(G)$ рода $[G]$ и конечное произведение

$$c(A, [Q]; G) = c_{-1}(A, Q; G) \prod_{p|2ad} c_p(A, Q; G).$$

Локальные множители c_p равны числу склеивающих векторов $\bar{c} \bmod a\mathbb{Z}_p$ с условием

$$L_Q^p = L_A^p \oplus^{[\bar{c}]} L_K^p,$$

L_*^p обозначают локальные решетки соответствующих квадратичных форм. Если степень a формы A и определитель d формы Q не делятся на простое число $p \neq 2$, то форма K эквивалентна над $\mathbb{Z}_p$ форме aG^{-1} и решетка L_K^p ортогональна вложенной в L_Q^p решетке L_A^p .

Решение задачи о нахождении числа всех представлений $n(A, [Q])$ формы A родом $[Q]$ состоит из пяти основных структурных составляющих.

1. Редукция $n(A, [Q])$ к примитивным представлениям $\text{pn}(A, [Q])$ (см. [1, с. 48]).
2. Разбиение всех примитивных представлений

$$\text{pn}(A, [Q]) = \sum_{[G]} \text{pn}(A, [Q]; G) \quad (3.1)$$

родами $[G]$ с условием, что $A \oplus^{[*]} K$ эквивалентна над $\mathbb{Z}$ какой-либо форме из рода $[Q]$.

3. Разложение в произведение

$$\text{pn}(A, [Q]; G) = m(G) c_{-1}(A, Q; G) \prod_{p|2ad} c_p(A, Q; G)$$

веса $m(G)$ рода $[G]$ – конечного произведения гамма-функций, дзета-функций Римана и L -функций Дирихле квадратичного характера – и конечного числа локальных множителей c_p .

4. Разбиение множителей c_p локальными вложениями решеток $\text{em}: L_A^p \hookrightarrow L_Q^p$ с фиксированной ортогонально дополнительной решеткой L_K^p .

5. Разложение вложений em в прямую ортогональную сумму локальных минимальных неразложимых вложений:

$$\text{em} = \text{em}_{\min}^{(1)} \oplus^{\perp} \cdots \oplus^{\perp} \text{em}_{\min}^{(s)}.$$

В [2]–[4] классифицированы локальные минимальные вложения

$$\mathrm{em}_{\min}: L_A^p \hookrightarrow L_Q^p$$

и построена теория ветвления вложений локальных решеток.

Приведенная схема 1–5 сводит вычисление веса представлений $n(A, [Q])$ к классификации минимальных неразложимых вложений $\mathrm{em}_{\min}$ и проясняет причины трудностей, возникающих при вычислении локальных множителей c_p . Можно сказать, что для вычисления множителей c_p нужно знать строение всех решений $X \in \mathrm{Mat}_{n,m}(\mathbb{Z})$ матричного уравнения $Q[X] = A$ над локальным кольцом $\mathbb{Z}_p$. Особенно сложно устроены решения X в случае ветвления, когда определители $|Q|$ и $|A|$ одновременно делятся на p .

Рассмотренный в статье метод дополнения может стать основой альтернативного [2]–[4] подхода для изучения ветвления. Суть его состоит в том, чтобы взять форму $\tilde{Q}$, например, кубической решетки $\mathbb{Z}^k$ подходящей размерности k или решетки Госсета E_8 и рассмотреть матричное уравнение

$$\tilde{Q}[\tilde{X}] = \tilde{A}. \quad (3.2)$$

Далее, выбрать специализацию $\tilde{A} = \begin{pmatrix} A' & 0 \\ 0 & A \end{pmatrix}$, приводящую к такому вложению $\mathrm{em}: L_{A'}^p \hookrightarrow L_{\tilde{Q}}^p$, чтобы к решетке $L_{A'}^p$ ортогонально дополнительной была решетка $L_{\tilde{Q}}^p$. Нетривиальным будет переход от уравнения (3.2) к исходному уравнению $Q[X] = A$ (ср. (7.2)). Для него потребуются расширение леммы 7.1 на случай не взаимно простых определителей $|A'| = |Q|$ и $|A|$.

Список литературы

1. Журавлев В. Г. Представление формы родом квадратичных форм // Алгебра и анализ. 1996. Т. 8. № 1. С. 21–112.
2. Журавлев В. Г. Орбиты представлений чисел локальными квадратичными формами // Тр. МИРАН. 1997. Т. 218. С. 151–164.
3. Журавлев В. Г. Вложение p -элементарных решеток // Изв. РАН. Сер. матем. 1999. Т. 63. № 1. С. 77–106.
4. Журавлев В. Г. Примитивные вложения в локальные решетки простого определителя // Алгебра и анализ. 1999. Т. 11. № 1. С. 87–117.
5. Касселс Дж. Рациональные квадратичные формы. М.: Мир, 1982.
6. Конвей Дж., Слоэн Н. Упаковки шаров, решетки и группы. М.: Мир, 1990.
7. Conway J., Sloan N. Quadratic forms of small determinant // Proc. R. Soc. Lond. 1988. V. 418. P. 17–41.
8. Kitaoka Y. Lectures on Siegel modular Forms and Representation by Quadratic Forms. Berlin: Springer, 1986.
9. Watson G. One-class genera of positive quaternary quadratic forms // Acta Arithmetica. 1974. V. 24. P. 461–475.

Поступило в редакцию
25.XI.1999