С. В. Федорова, Представления p-элементарной формы родом, *Зап. научн. сем. ПОМИ*, 2001, том 276, 276–290

Записки научных
семинаров ПОМИ
Том 276, 2001 г.

С. В. Фёдорова

ПРЕДСТАВЛЕНИЯ p-ЭЛЕМЕНТАРНОЙ ФОРМЫ РОДОМ

Введение

Пусть Q и A – целые симметрические невырожденные положительно определённые квадратичные формы размерностей $n > m \geqslant 1$ соответственно с определителями $d = |Q|$ и $|A|$. Форма A представима формой Q, если имеет целочисленное решение X матричное уравнение $Q[X] =^t XQX = A$, где ${}^tX$ – транспонированная матрица X. Вес представлений формы A родом $[Q]$ определяется равенством

$$n(A, [Q]) = \sum_{i=1}^{h} \sum_{X:\ Q_i[X]=A} \frac{1}{o(Q_i)}, \tag{1}$$

где h – число классов рода $[Q]$, $o(Q_i)$ – порядок группы $O(Q_i)$ целых автоморфизмов формы Q_i. Впервые формула веса представлений формы родом была получена Зигелем (1935 г.) [1]:

$$n(A, [Q]) = \prod_{p=-1,2,3,\dots} \alpha_p(A, Q). \tag{2}$$

В дальнейшем предпринимались многочисленные попытки вычислить локальные плотности $\alpha_p(A, Q)$. Обычно использовались многомерные гауссовы суммы и точная формула для обычной суммы Гаусса, см. [2]. Китаока [3] исследовал локальные плотности $\alpha_p(A, Q)$ (2) и их связи с модулярными формами. Его результаты качественные и оценочные.

Иной подход к вычислению веса представлений формы родом был предложен в [4]. Все представления формы A формой Q можно получить из примитивных представлений $X:\ Q[X] = A$, у которых наибольший общий делитель всех миноров порядка m равен 1. В. Г. Журавлёвым была получена формула веса примитивных представлений формы родом:

$$pn(A,[Q]) = \mathrm{std}(n-m,|G|)\prod_{p|2ad}\alpha_p(A,Q), \qquad (3)$$

где $\mathrm{std}(n-m,|G|)$ – стандартная масса, равная произведению ζ-функции Римана и L-функции Дирихле, a – уровень формы A, то есть наименьшее положительное целое, для которого форма aA^{-1} будет целочисленной. Локальные множители $\alpha_p(A,Q)$ зависят только от p-инвариантов [5] форм A и Q. Формула веса примитивных представлений (3) выявляет важнейшее свойство диофантовых квадратичных систем: среднее количество представлений над кольцом целых чисел $\mathbb{Z}$ некоторой квадратичной формы формами рода сводится к представлениям над локальными кольцами p-адических чисел $\mathbb{Z}_p$ этой же формы любой формой рода.

Вес примитивных представлений для размерности $\dim A \geqslant 2$ впервые был посчитан [4] для взаимно простых a и d с условием $a=|A|$. Особую сложность вычисления локальных множителей $\alpha_p(A,Q)$ представляет случай, когда уровень a и определитель d имеют общие делители p. Свойство примитивности решений уравнения $Q[X]=A$ равносильно целой эквивалентности исходной формы Q форме вида:

$$Q_G^A(C) = \begin{pmatrix} A & C \\ {}^tC & \frac{1}{a}(aA^{-1}[C]+G) \end{pmatrix}, \qquad (4)$$

где G – целочисленная форма размерности $k=n-m$ и определителя $|G| = a^{n-m}|Q|/|A|$, C – сцепляющая матрица. Ветвление представлений формы родом возникает, если уровень a и определитель d имеют общие делители. Форма A и род $[Q]$ неоднозначно определяют род $[G]$ из ортогонального дополнения к A в Q. Над кольцом $\mathbb{Z}_p$ локальный множитель ветвления распадается на сумму по неэквивалентным родам $[G_i]$. Внутри же фиксированного рода $[G]$ возможно существование нескольких неэквивалентных орбит матриц сцепки $\{C_j\}$:

$$\alpha_p(A,Q) = \sum_{[G_i]}\sum_{\{C_j\}}\alpha_p(A,Q,G_i,C_j). \qquad (5)$$

При наложении ограничений на размерность или масштаб составляющих жорданова разложения форм A и Q удаётся по системе инвариантов построить все возникающие роды форм G и орбиты матриц сцепки $\{C\}$.

В работе исследуется ветвление представлений p-элементарных форм A, то есть форм простого уровня $a = \varepsilon p$, где ε – единица кольца $\mathbb{Z}_p$. Очевидно, такие формы имеют жорданово разложение $A = A_1 \oplus pA_p$ над локальным кольцом $\mathbb{Z}_p$. Поясним суть ветвления на примере.

Число примитивных представлений $pr(A, Q)$ формы A одноклассной формой Q из (1) равно

$$pr(A, Q) = o(Q) \cdot pn(A, Q). \tag{6}$$

Квадратичная форма пятимерной решётки корней нулевой суммы A_5 имеет инварианты $d = 6$, $o(A_5) = 1440$, $3_{A_5} = 1^{-4}3^{+1}$, $2_{A_5} = 1^{-4}_{\mathrm{II},0}2^{+1}_{\mathrm{I},7}$. Рассмотрим ветвление представлений над $\mathbb{Z}_3$ бинарной квадратичной формы A бесквадратного нечётного уровня a формой A_5. Пусть форма A над кольцом $\mathbb{Z}_3$ имеет жорданово разложение $A = A_1 \oplus 3A_3$, где A_1, A_3 – произвольные единицы кольца $\mathbb{Z}_3$. Возникает два неэквивалентных рода форм G, имеющих над $\mathbb{Z}_3$ жордановы разложения вида:

$$G^{\mathrm{I}} = G^{\mathrm{I}}_1 \oplus 3G^{\mathrm{I}}_3,\ \dim G^{\mathrm{I}}_3 = 2; \quad G^{\mathrm{II}} = G^{\mathrm{II}}_1 \oplus 3^2 G^{\mathrm{II}}_{3^2},\ \dim G^{\mathrm{II}}_{3^2} = 1.$$

Для них слагаемые локального множителя $\alpha_3(A, A_5)$ (5) соответственно равны [6] $\alpha_3(A, Q, G^{\mathrm{I}}) = (1 + \varepsilon(A_3))/2$, $\alpha_3(A, Q, G^{\mathrm{II}}) = (3^2 - 1)/2$, где $\varepsilon(A_p) = \left(\frac{|A_p|}{p}\right)$ – знак соответствующего блока жорданова разложения, а $\left(\frac{\bullet}{p}\right)$ – символ Лежандра. В результате ветвящийся локальный множитель (5) равен $\alpha_3(A, Q) = 9 + \varepsilon(A_3)$. Число примитивных представлений $pr(A, A_5)$ бинарной формы A формой решётки A_5 равно [6]

$$\begin{aligned} pr(A, A_5) = 30(9 + \varepsilon(A_3)) \prod_{p\|\,|A|,\, p\neq 2,3} \left(p + \left(\frac{6}{p}\right)\varepsilon(A_1)\right) \times \\ \times \prod_{p^2\|\,|A|,\, p\neq 2,3} (p^2 - 1), \end{aligned} \tag{7}$$

где $p^s \| a$ означает, что $p^s | a$, но $p^{s+1} \nmid a$. Методом неопределённых коэффициентов [7] в формуле (7) вычислены локальные множители $\alpha_p(A, Q)$ для простых p с условием $p^2 \|\ |A|$, то есть снято ограничение $a = |A|$ [4].

Инварианты формы шестимерной решётки корней Госсета E_6 равны $d = 3$, $o(E_6) = 2^8 \cdot 3^4 \cdot 5$, $3_{E_6} = 1^{+5}3^{+1}$, $2_{E_6} = 1^{-6}_{\mathrm{II},0}$. Число примитивных представлений тернарной формы A бесквадратного чётного определителя $|A|$ формой решётки E_6 равно [6]

$$pr(A, E_6) = 2^4 \cdot 3^3 \cdot 5 \cdot \alpha_3(A, Q) \prod_{p|a,\, p\neq 2,3} \left(p + \left(\frac{3}{p}\right)\varepsilon(A_1)\right), \qquad (8)$$

где $\alpha_3(A, Q) = (3 - \left(\frac{a}{3}\right))$ для случая $a \nmid 3$ и $\alpha_3(A, Q) = 12(3 - \varepsilon(A_3)$ для ветвления представлений форм $A = 3A_3$. Сравнение двух последних локальных множителей показывает, что появление общих делителей уровня a и определителя d при прочих равных условиях ведёт к увеличению числа представлений форм.

Описание ветвления представлений p-элементарных форм A стало возможным благодаря выявлению всех минимальных неразложимых представлений над $\mathbb{Z}_p$, приведённых в §1. С помощью минимальных неразложимых вложений легко находить условия существования вложений форм $A \hookrightarrow Q$ и число орбит представлений $X : \ Q[X] = A$ над $\mathbb{Z}_p$. Случай представления p-элементарных форм A локально p-одномерными формами Q изучен в [6]. Представлениям локально p-двумерными формами посвящена теорема 2 из §1. Для получения конкретных формул в §2 методом ортогонального дополнения получены новые многоклассные роды квадратичных форм.

§1. Минимальные неразложимые вложения

1.1. Пусть квадратичная форма A размерности m примитивно представима положительно определённой квадратичной формой Q размерности $n > m$, то есть имеет целочисенные решения матричное уравнение $Q[X] = A$ и наибольший общий делитель всех миноров матрицы X порядка m равен единице. Перейдём на инвариантный бескоординатный язык решёток и получим геометрическое описание представлений форм. Решёткой L над кольцом $\mathbb{Z}$ называется свободный $\mathbb{Z}$-модуль конечного ранга с невырожденной симметрической билинейной формой, принимающей целые значения. Представление формы A формой Q тождественно вложению решёток $em : \ L_A \hookrightarrow L_Q$, где L_A и L_Q – решётки, соответствующие формам A и Q. Примитивность вложения будет означать, что L_A/L_Q – свободный $\mathbb{Z}$-модуль. Расширение (4) тождественно склейке решёток $L_Q = L_A \overset{[C]}{\oplus} L_G$, где C – матрица склейки.

Любое вложение решёток распадается на ортогональную сумму минимальных неразложимых вложений $em = em_1 \oplus em_2 \oplus \ldots \oplus em_s$. Пусть форма A p-элементарная, то есть $L_A^*/L_A \bigotimes \mathbb{Z}_p$ является нетривиальной абелевой p-группой, где L_A^* – решётка, двойственная к L_A. Очевидно, что форма A будет p-элементарной тогда и только тогда, когда p входит в a в первой степени, то есть $A = A_1 \oplus pA_p$. Положим, что форма G из расширения (4) имеет жорданово разложение над локальными кольцами $\mathbb{Z}_p$ вида $G = \sum_\alpha p^\alpha G_{p^\alpha}$, $\alpha = 0, 1, 2, \ldots$, а матрица сцепки C разбита на блоки C_α аналогично форме G. Формы G и C связаны сравнением $aA^{-1}[C] \equiv -G (\mathrm{mod}\, a)$, следующим из целочисленности формы расширения $Q_G^A(C)$ (4). Используем результат [7] о квадратичных пространствах V над полем характеристики $\mathrm{char} \neq 2$. Пусть V невырождено, U – подпространство из V, $U^\perp$ и $\mathrm{rad}\, U = U \bigcap U^\perp$ – его ортогональное дополнение и радикал соответственно.

Теорема 1 (Витт, см. [8]). *Любая изометрия σ продолжается до изометрии объемлющих пространств ρ : $\rho|_U = \sigma$. Для фиксированного $\varepsilon = \pm 1$ найдётся продолжение ρ с определителем $|\rho| = \det\ \rho = \varepsilon$ тогда и только тогда, когда $\dim U + \dim \mathrm{rad}\, U < \dim V$.*

Тогда по теореме Витта жордановы составляющие G_{p^α} формы G и форма aA^{-1} разлагается в ортогональные суммы:

$$
\begin{aligned}
&G_{p^\alpha} = 1(r_\alpha^\varepsilon) \oplus J(r_\alpha^0) \oplus g_\alpha,\\
&aA^{-1} = -G_1 \oplus J(r) \oplus e, \quad r = \sum_{\alpha \geqslant 1} r_\alpha, \quad r_\alpha = r_\alpha^\varepsilon \oplus r_\alpha^0,\\
&\dim 1(r_\alpha^\varepsilon) = r_\alpha^\varepsilon, \quad \left(\frac{|1(r_\alpha^\varepsilon)|}{p}\right) = \varepsilon = \pm 1, \quad J(r) = \begin{pmatrix} 0 & 1_r \\ 1_r & 0 \end{pmatrix},
\end{aligned}
\tag{1.1}
$$

где 1_r – единичная матрица размерности r. Числа r_α^ε, r_α^0, ε являются инвариантами орбит $\{C_\alpha\}$. Из разложений форм A и G (1.1) получаем форму расширения $Q_G^A(C)$ вида

$$
\begin{aligned}
&Q_G^A(C) = Q\{r_\alpha\} \oplus A_1 \oplus ae^{-1} \oplus \frac{p^{\alpha_i}}{a} g_{\alpha_i} \oplus \frac{1}{a} G_\alpha,\\
&Q\{r_\alpha\} = J(r_0) \oplus (J(r_{\alpha_i}) \oplus ap^{\alpha_i} 1(r_{\alpha_i}^{\varepsilon_i}) \oplus p^{\alpha_i} J(r_{\alpha_i}^0)),
\end{aligned}
\tag{1.2}
$$

где $\alpha > 1$, $\alpha_i > 1$, $\alpha \neq \alpha_i$. Число орбит $\{X\}$ целых примитивных представлений $Q[X] = A$ равно числу решений $\{r_\alpha\} = \{r_\alpha^\varepsilon,\ r_\alpha^0,\ \varepsilon\}$ равенств (1.2).

Вложение формы A в форму Q распадается на ортогональные суммы двух одномерных и трёх многомерных минимальных неразложимых вложений вида [9]:

$$1^\varepsilon \hookrightarrow 1^\varepsilon, \quad a1^\varepsilon \hookrightarrow a1^\varepsilon, \quad -a1^\varepsilon \hookrightarrow \begin{pmatrix} -a1^\varepsilon & 1 \\ 1 & 0 \end{pmatrix},$$

$$aJ(1) \hookrightarrow \begin{pmatrix} aJ(1) & \begin{matrix} 1 \\ 0 \end{matrix} \\ \begin{matrix} 1 & 0 \end{matrix} & \frac{p^\alpha}{a}1^\varepsilon \end{pmatrix}, \quad aJ(1) \hookrightarrow \begin{pmatrix} aJ(1) & \begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix} \\ \begin{matrix} 1 & 0 \\ 0 & 0 \end{matrix} & \frac{p^\alpha}{a}J(1) \end{pmatrix}, \qquad (1.3)$$

где 1^ε – единица кольца $\mathbb{Z}_p$ и знака ε. По матрице расширения $Q_G^A(C)$ очевидно, что последний тип вложений (1.3) возможен, начиная с форм вида $Q = Q_1 \oplus pQ_p$, $\dim Q_p \geqslant 2$, а предпоследний тип вложений (1.3) реализуется, начиная с форм вида $Q = Q_1 \oplus p^s Q_{p^s}$, $s \geqslant 2$.

1.2. Пусть формы A и Q для всех нечётных простых p, одновременно делящих a и d, над кольцом $\mathbb{Z}_p$ имеют жордановы разложения

$$A = pA_p, \quad \dim A = m; \quad Q = Q_1 \oplus pQ_p, \quad \dim Q_p = 2. \qquad (1.4)$$

Теорема 2. *Если квадратичные формы A и Q удовлетворяют условиям (1.4), то множители ветвления $\alpha_p(A, Q)$ над кольцом $\mathbb{Z}_p$ задаются соотношениями:*

1.
$$\alpha_p(A, Q) = \left(\varepsilon(Q_1) + \left(\frac{-1}{p}\right)^{m-2}\right) \sum_{i=1}^{2} \alpha_p(A, Q, G^{\mathrm{I}}, C_i)$$

при $n - 2m + 2 = 0$;

2.
$$\alpha_p(A, Q) = \sum_{i=1}^{2} \alpha_p(A, Q, G^{\mathrm{I}}, C_i) \quad \text{при} \quad n - 2m + 1 = 0;$$

3.
$$\alpha_p(A, Q) = \sum_{i=1}^{2} \alpha_p(A, Q, G^{\mathrm{I}}, C_i) + \left(\varepsilon(Q_1) + \left(\frac{-1}{p}\right)^{m-1}\right) \alpha_p(A, Q, G^{\mathrm{II}})$$

при $n-2m=0$;

4.

$$\alpha_p(A,Q)=\sum_{i=1}^{2}\alpha_p(A,Q,G^{\mathrm{I}},C_i)+\alpha_p(A,Q,G^{\mathrm{II}})\quad \textit{при}\quad n-2m-1=0;$$

5.

$$\alpha_p(A,Q)=\sum_{i=1}^{2}\alpha_p(A,Q,G^{\mathrm{I}},C_i)+\alpha_p(A,Q,G^{\mathrm{II}})+$$
$$\left(\varepsilon(Q_1)+\left(\frac{-1}{p}\right)^m\right)\alpha_p(A,Q,G^{\mathrm{III}})\quad \textit{при}\quad n-2m-2=0;$$

6.

$$\alpha_p(A,Q)=\sum_{i=1}^{2}\alpha_p(A,Q,G^{\mathrm{I}},C_i)+\alpha_p(A,Q,G^{\mathrm{II}})+\alpha_p(A,Q,G^{\mathrm{III}})$$

при $n-2m-2>0$;

7. $\alpha_p(A,Q)=0$ *в остальных случаях.*

Слагаемые ветвящихся множителей вычисляются посредством формул

$$\alpha_p(A,Q,G^{\mathrm{I}},C_1)=0,\quad \textit{если}\quad m=2\ \ \textit{и}\ \ \varepsilon(A_p)=\varepsilon(Q_p);$$
$$\alpha_p(A,Q,G^{\mathrm{I}},C_2)=0,\quad \textit{если}\quad \varepsilon(Q_p)=-\left(\frac{-1}{p}\right);$$

в остальных случаях для $m=2m'+1$

$$\alpha_p(A,Q,G^{\mathrm{I}},C_1)=\frac{1}{2}p^{s_1}\left(1-(-1)^{\frac{(p-1)(n-4)}{4}}\varepsilon(Q_1)p^{-\frac{n-2m+2}{2}}\right)^{-1}\sigma_1\sigma_3\sigma_5^{-1},$$

$$\alpha_p(A,Q,G^{\mathrm{I}},C_2)=$$
$$=p^{s_2}(1-p^{-(n-2m)})\left(1-(-1)^{\frac{(n+4)(p-1)}{4}}\varepsilon(Q_1)p^{-\frac{n-2m}{2}}\right)^{-1}\sigma_1\sigma_3\sigma_6^{-1},$$

$$\alpha_p(A,Q,G^{\mathrm{II}})=$$
$$=\frac{1}{4}p^{s^3}(1-p^{-(n-2m)})\left(1-(-1)^{\frac{(p-1)(m-1)}{4}}\varepsilon(A_p)p^{-\frac{m-1}{2}}\right)^{-1}\times$$
$$\times\left(1-(-1)^{\frac{(p-1)(n-2)}{4}}\varepsilon(Q_1)p^{-\frac{n-2m}{2}}\right)^{-1}\sigma_1\sigma_3,$$

$$\alpha_p(A,Q,G^{\mathrm{III}}) = \frac{1}{2}p^{s_4}(1-p^{-(n-2m-2)})(1-p^{-(n-2m)})\times$$
$$\times\left(1-(-1)^{\frac{(p-1)(n-2)}{4}}\varepsilon(Q_1)p^{-\frac{n-2m-2}{2}}\right)^{-1}\sigma_3\sigma_7^{-1};$$

для $m = 2m'$

$$\alpha_p(A,Q,G^{\mathrm{I}},C_1) = \frac{1}{2}p^{s_1}\sigma_2\sigma_4\sigma_5^{-1}\sigma_8\sigma_9,$$

$$\alpha_p(A,Q,G^{\mathrm{I}},C_2) = p^{s_2}(1-p^{-(n-2m+1)})\sigma_2\sigma_4\sigma_6^{-1}\sigma_8\sigma_9^{-1},$$

$$\alpha_p(A,Q,G^{\mathrm{II}}) = \frac{1}{4}p^{s_3}(1-p^{-(n-2m+1)})\sigma_4\sigma_8,$$

$$\alpha_p(A,Q,G^{\mathrm{III}}) = \frac{1}{2}p^{s_4}(1-p^{-(n-2m-1)})(1-p^{-(n-2m+1)})\sigma_4\sigma_7^{-1},$$

где

$$s_1 = \frac{m(5-m)+n(m-2)-4}{2}, \quad s_2 = \frac{m(n+m+1)-2}{2},$$

$$s_3 = \frac{m(n-m-1)-2}{2}, \quad s_4 = \frac{n(m+2)-m(m+3)-4}{2},$$

$$\sigma_1 = 1-p^{-(m-1)}, \quad \sigma_2 = 1-p^{-(m-2)},$$

$$\sigma_3 = (1-p^{-(n-2m+2)})\cdots(1-p^{-(n-m-1)}),$$

$$\sigma_4 = (1-p^{-(n-2m+3)})\cdots(1-p^{-(n-m-1)}),$$

$$\sigma_5 = p-\left(\frac{-1}{p}\right), \quad \sigma_6 = p-1, \quad \sigma_7 = (1-(-1)^{\frac{p-1}{2}}\varepsilon(Q_p)p^{-1}),$$

$$\sigma_8 = (1-(-1)^{\frac{(p-1)m'}{2}}\varepsilon(A_p)p^{-m'}),$$

$$\sigma_9 = (1-(-1)^{\frac{(p-1)(m-2)}{4}}\varepsilon(A_p)p^{-\frac{m-2}{2}}).$$

Доказательство. Если в разложении (4) сцепляющую матрицу C выбрать в виде $C = \binom{0}{C_p}$ с блоком C_p высоты $\dim A_p$, то будет верно соотношение

$$pn(A_1 \oplus pA_p, Q) = pn(pA_p, Q \ominus A_1),$$

где $Y = Q \ominus A_1$ любая форма из разложения $Q = A \oplus Y$. Это позволяет, не умаляя общности, ограничить рассмотрение формами вида $A = pA_p$.

Построим целочисленные формы G из ортогонального дополнения к A в Q с определителем $|G| = p^{n-2m+2}$ и размерностью $k = n - m$. Из p-элементарности форм A и Q и формы расширения (1.2) следует, что максимальный масштаб g жорданова разложения над $\mathbb{Z}_p$ формы G не превосходит p^2. Поскольку форма Q из (1.4) является локально p-двумерной, то размерность блока $p^2G_{p^2}$ жорданова разложения формы G не превосходит 2. Возможно три рода форм G из ортогонального дополнения к A в Q вида:

$$G^{\mathrm{I}} = G_1^{\mathrm{I}} \oplus pG_p^{\mathrm{I}}: \quad n(G_1^{\mathrm{I}}) = m-2, \quad n(G_p^{\mathrm{I}}) = n-2m+2;$$

$$G^{\mathrm{II}} = G_1^{\mathrm{II}} \oplus pG_p^{\mathrm{II}} \oplus p^2G_{p^2}^{\mathrm{II}}:$$
$$n(G_1^{\mathrm{II}}) = m-1, \quad n(G_p^{\mathrm{II}}) = n-2m, \quad n(G_{p^2}^{\mathrm{II}}) = 1;$$

$$G^{\mathrm{III}} = G_1^{\mathrm{III}} \oplus pG_p^{\mathrm{III}} \oplus p^2G_{p^2}^{\mathrm{III}}:$$
$$n(G_1^{\mathrm{III}}) = m, \quad n(G_p^{\mathrm{III}}) = n-2m-2, \quad n(G_{p^2}^{\mathrm{III}}) = 2.$$

Инварианты $\{r_\alpha\}$ орбит матриц сцепки $\{C\}$ для каждого фиксированного рода $[G]$ получаем как решение равенств (1.2). Их вид

$$\{C_1(G^{\mathrm{I}})\} = \{r_0^{\varepsilon_0} = m-2,\, r_1^0 = 0\},\ \{C_2(G^{\mathrm{I}})\} = \{r_0^{\varepsilon_0} = m-2,\, r_1^0 = 1\},$$
$$\{C(G^{\mathrm{II}})\} = \{r_0^{\varepsilon_0} = m-1,\, r_1^0 = 0\}, \quad \{C(G^{\mathrm{III}})\} = \{r_0^{\varepsilon_0} = m,\, r_1^0 = 0\}.$$

Для каждой из перечисленных орбит $\{C\}$ строим форму расширения $Q_G^A(C)$, эквивалентную исходной форме Q:

$$\begin{aligned}
Q_{G^{\mathrm{I}}}^A(C_1) &\sim_p \overset{m-2}{\oplus} \begin{pmatrix} p & 1 \\ 1 & 0 \end{pmatrix} \oplus G_p^{\mathrm{I}} \oplus p1_2^{\varepsilon(Q_p)};\\
Q_{G^{\mathrm{I}}}^A(C_2) &\sim_p \overset{m-2}{\oplus} \begin{pmatrix} p & 1 \\ 1 & 0 \end{pmatrix} \oplus G_p^{\mathrm{I}} \oplus pJ(1);\\
Q_{G^{\mathrm{II}}}^A(C) &\sim_p \overset{m-1}{\oplus} \begin{pmatrix} p & 1 \\ 1 & 0 \end{pmatrix} \oplus G_p^{\mathrm{II}} \oplus p1^{\pm} \oplus pG_{p^2}^{\mathrm{II}};\\
Q_{G^{\mathrm{III}}}^A(C) &\sim_p \overset{m}{\oplus} \begin{pmatrix} p & 1 \\ 1 & 0 \end{pmatrix} \oplus G_p^{\mathrm{III}} \oplus pG_{p^2}^{\mathrm{III}},
\end{aligned} \tag{1.5}$$

где 1_n^ε – форма единичного определителя и знака ε над кольцом $\mathbb{Z}_p$. Из (1.5) очевидно, что для существования формы $Q_{G^{\mathrm{I}}}^A(C_2)$ необходимо условие $\varepsilon(Q_p) = \left(\frac{-1}{p}\right)$. Если $m = 2$, то форма $Q_{G^{\mathrm{I}}}^A(C_1)$

существует при условии $\varepsilon(Q_p) = \varepsilon(A_p)$. Эквивалентность форм расширения (1.5) исходной форме Q, в частности, означает совпадение знаков блоков жорданова разложения формы. А именно,

$$\varepsilon(G_1^{\mathrm{I}}) = \varepsilon(G_1^{\mathrm{II}}) = \varepsilon(G_1^{\mathrm{III}}) = \varepsilon(A_p), \quad \varepsilon(G_p^{\mathrm{I}}(C_1)) = \left(\frac{-1}{p}\right)^{m-2} \varepsilon(Q_1),$$
$$\varepsilon(G_p^{\mathrm{I}}(C_2)) = \left(\frac{-1}{p}\right)^{m-2} \varepsilon(Q_1), \quad \varepsilon(G_p^{\mathrm{II}}) = \left(\frac{-1}{p}\right)^{m-1} \varepsilon(Q_1),$$
$$\varepsilon(G_p^{\mathrm{III}}) = \left(\frac{-1}{p}\right)^{m} \varepsilon(Q_1), \quad \varepsilon(G_{p^2}^{\mathrm{III}}) = \varepsilon(Q_p). \tag{1.6}$$

На этом построение родов форм G из ортогонального дополнения к A закончено.

Условия существования представлений формы A родом формы Q следуют из целочисленности формы G, знаков (1.6) и размерностей блоков её жорданова разложения. Локальный множитель $\alpha_p(A, Q)$ над кольцом $\mathbb{Z}_p$ вычисляется по формуле [4]:

$$\alpha_p(A, Q) = \sum_{[G]} c_p(A, Q, G) \cdot m_p(G)/\mathrm{std}_p(G), \tag{1.7}$$

где $c_p(A, Q, G)$ – число орбит матриц сцепки C над кольцом $\mathbb{Z}_p$, $m_p(G)$ – p-масса рода $[G]$, $\mathrm{std}_p(G)$ – стандартная p-масса рода $[G]$.

В двойной орбите форм сцепки $\{C\} = \{{}^tUCV : U \in O(A), V \in O(G)\}$, где $O(\cdot)$ – группа автоморфизмов над локальным кольцом $\mathbb{Z}_p$, выберем представителя $C = \begin{pmatrix} 1_{r_0} & 0 & 0 \\ 0 & 1_{r_1} & 0 \\ 0 & 0 & 0 \end{pmatrix}$. Разобьём на блоки автоморфизмы

$$U = \begin{pmatrix} 1 & 0 \\ 0 & U_1 \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 0 & 0 \\ 0 & V_1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$
$$U_1 \in O(J(r_1) \oplus e), \quad V_1 \in O(J(r_1) \oplus g_1).$$

Из вида автоморфизмов получаем формулу

$$c_p(A, Q, G) = \frac{o(A_p)o(G_p)}{\mathrm{stab}}, \tag{1.8}$$

где stab – порядок стабилизатора орбит матриц C над $\mathbb{Z}_p$, то есть порядок множества пар (U, V) с условием $UCV \equiv C (\bmod p)$. Найдём порядок стабилизатора. Пусть блоки автоморфизмов имеют вид

$$U_1 = \begin{pmatrix} A & B & C \\ D & E & F \\ G & H & J \end{pmatrix}, \qquad V_1 = \begin{pmatrix} A_1 & B_1 & C_1 \\ D_1 & E_1 & F_1 \\ G_1 & H_1 & J_1 \end{pmatrix}.$$

Условие $UCV \equiv C (\mathrm{mod}\ p)$ эквивалентно сравнениям $AA_1 \equiv 1(\mathrm{mod}\ p)$, $D \equiv 0(\mathrm{mod}\ p)$, $G \equiv 0(\mathrm{mod}\ p)$, $B_1 \equiv 0(\mathrm{mod}\ p)$, $C_1 \equiv 0(\bmod p)$. Принадлежность форм U_1 и V_1 группам автоморфизмов форм $J(r_1) \oplus e$, $J(r_1) \oplus g_1$ приводит к результату ${}^tAE \equiv 1(\bmod p)$, $({}^tBE)^s + e[H] \equiv 0(\bmod p)$, ${}^tEC +{}^t HeJ \equiv 0(\bmod p)$, $e[J] \equiv e(\bmod p)$, $F_1 \equiv 0(\mathrm{mod}\ p)$, ${}^tA_1E_1 \equiv 1(\mathrm{mod}\ p)$, $({}^tB_1E_1)^s + g_1[H_1] \equiv (\mathrm{mod}\ p)$, ${}^tE_1C_1 +{}^t H_1g_1J_1 \equiv (\bmod p)$, $g_1[J_1] \equiv g_1(\bmod p)$, $F_1 \equiv 0(\bmod p)$. Обозначение $L^s = L +{}^t L$ использовано для симметризации матриц. Объединяя последние сравнения, получаем параметризацию автоморфизмов U и V матрицами:

$$\begin{aligned} &A, A_1 \in GL_{r_1}(\mathbb{F}_p), \quad H \in M_{m_1-(r_0+2r_1),r_1(\mathbb{F}_p)}, \quad J \in O(e), \\ &S_- \equiv -{}^tS_- \in M_{r_1}(\mathbb{F}_p), \quad F_1 \in M_{r_1,k-2r_1}(\mathbb{F}_p), \quad J_1 \in O(g_1), \end{aligned} \tag{1.9}$$

где $M_{l,n}(\mathbb{F}_p)$ – матрица размерности $l \times n$ с элементами из поля вычетов $\mathbb{F}_p$, $GL_r(\mathbb{F}_p)$ – полная линейная группа невырожденных матриц размерности r над полем вычетов $\mathbb{F}_p$, $k_1 = \dim G_p$. Учитывая $AA_1 \equiv 1(\bmod p)$ из (1.9) получаем

$$\mathrm{stab} = p^{r_1(m+k_1-r_0-3r_1-1)} gl(r_1)o(e)o(g_1), \tag{1.10}$$

где $gl(r)$ – порядок полной линейной группы $GL_r(\mathbb{F}_p)$. Порядок группы автоморфизмов $o(T)$ невырожденной формы T размерности n кольцом $\mathbb{Z}_p$ и порядок группы $GL_r(\mathbb{F}_p)$ равны [4]:

$$\begin{aligned} &o(T) = 2 \cdot p^{\frac{n(n-1)}{2}}(1-p^{-2})\cdots(1-p^{-(n-1)}) \quad \text{для} \quad n = 2n'+1, \\ &o(T) = 2 \cdot p^{\frac{n(n-1)}{2}}(1-p^{-2})\cdots \\ &\qquad\qquad \cdot (1-p^{-(n-2)})\left(1-\left(\frac{(-1)^{n'}|T|}{p}\right)p^{-n'}\right) \text{ для } n = 2n', \\ &gl(r) = p^{r^2}(1-p^{-1})\cdots(1-p^{-r}). \end{aligned} \tag{1.11}$$

Вспомогательные формы e и g_1 для форм с условием (1.4) равны:

$$
\begin{aligned}
&e = A_p \oplus (-G_1^{\mathrm{I}}) = 1_2^{\pm}, \quad g_1 = G_p^{\mathrm{I}} && \text{для} \quad G^{\mathrm{I}}(C_1),\\
&e = 0, \quad g_1 = G_p^{\mathrm{I}} \ominus J(1) && \text{для} \quad G^{\mathrm{I}}(C_2),\\
&e = 1^{\pm}, \quad g_1 = G_p^{\mathrm{II}} && \text{для} \quad G^{\mathrm{II}}(C),\\
&e = 0, \quad g_1 = G_p^{\mathrm{III}} && \text{для} \quad G^{\mathrm{III}}(C). \qquad (1.12)
\end{aligned}
$$

Множители ветвления $\alpha_p(A, Q)$ получаются прямым вычислением из формул (1.7), (1.8), (1.10)–(1.12). Теорема доказана.

§2. Метод ортогональоного дополнения

2.1. Для получения конкретных формул известных форм классических решёток корней оказывается недостаточно. Для получения новых родов квадратичных форм, заданного определителя и размерности, применим метод ортогонального дополнения. Пусть X – орбиты всех примитивных представлений одноклассной формы A' одноклассной формой Q', и пусть существует ортогональное дополнение $K_i \perp X_i$ из некоторого рода $[K]$. Зафиксируем ортогональное дополнеие $K_1 \perp X_1$ для некоторой орбиты $\{X_1\}$. Условия представимости формы K_1 формой Q' носят локальный характер над кольцом $\mathbb{Z}_p$ и зависят только от полной системы p-символов родов $[K]$ и $[Q']$ [7]. Таким образом, вместе с K_1 любая форма из рода $[K]$ представима формой Q'. Так как род формы A' одноклассный, ортогональное дополнение $A_1' \perp K_1$ попадает в род $[A']$, следовательно, класс $\{A_1'\}$ совпадает с A'. Таким образом, классы $\{K_i\}$, содержащиеся в роде $[K]$, образуют полный род.

Для приложений удобно полагать $A' = a$ – число, $Q' = 1_n$ – форма единичной матрицы размерности n. Полученный в результате метода ортогонального дополнения род $[K]$ имеет размерность $n-1$ и определитель a.

2.2. Так, специализацией $A' = \begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$ и $Q' = 1_7$ получен двуклассный род $[Q]$ форм вида $Q_1 = 1 \cdot \mathbb{Z}^3 \oplus 3 \cdot \mathbb{Z}^2$, $Q_2 = 1 \cdot \mathbb{Z}^1 \oplus A_2 \oplus A_2$, где $\mathbb{Z}^n$ – n-мерная кубическая решётка корней, A_n – n-мерная решётка корней нулевой суммы. Инварианты рода $[Q]$ имеют вид $h([Q]) = 2$, $d = 9$, $o(Q_1) = 384$, $o(Q_2) = 576$, $3_{[Q]} = 1^{+3}3^{+2}$,

$2_{[Q]} = 1^{+5}_{\mathrm{I},1}$. Пусть p-элементарная чётная форма A имеет бесквадратный определитель, чётный уровень $a = 2a_1$ и 3-символ вида $3_A = 3^{\varepsilon(A_3)2}$. Поскольку уровень a и определитель d имеют общий делитель 3, то возникает ветвление представлений формы A родом $[Q]$ над кольцом $\mathbb{Z}_3$. По теореме 2 ветвящийся множитель имеет вид

$$\alpha_3(A,Q) = \sum_{i=1}^{2} \alpha_3(A,Q,G^{\mathrm{I}},C_i) + \alpha_3(A,Q,G^{\mathrm{II}}).$$

Так как $m = 2$ и $\varepsilon(Q_3) = -\left(\frac{-1}{3}\right)$, то $\alpha_3(A,Q,G^{\mathrm{I}},C_2) = 0$. Если $\varepsilon(A_3) = -1$, то $\alpha_3(A,Q,G^{\mathrm{I}},C_1) = 0$. Вычисления приводят к результату $\alpha_3(A,Q) = \frac{25}{18}$ для $\varepsilon(A_3) = +1$, $\alpha_3(A,Q) = \frac{4}{9}$ для $\varepsilon(A_3) = -1$. Значение стандартной массы равно $\mathrm{std}(3) = 2^{-1}3^{-1}$ [5], локальный множитель $\alpha_2(A,Q)$ равен [4]

$$\alpha_2(A,Q) = \frac{1}{8}(\frac{1}{4} + \varepsilon_2),$$

где $\varepsilon_2 = \left(\frac{a_1(1-t(A))}{2}\right)$ для $2_A \sim 1^{+1}_{\mathrm{II},0} 2^{\varepsilon(A)1}_{\mathrm{I},t(A)}$. Вес примитивных представлений (3) бинарной формы A родом $[Q]$ равен

$$pn(A,[Q]) = 2^{-4}\cdot 3^{-3}\cdot c\cdot \left(\frac{1}{4} + \left(\frac{a_1(1-t(A))}{2}\right)\right)\times \\ \times \prod_{p||\,|A|, p\neq 2,3} \left(p + \left(\frac{3}{p}\right)\varepsilon(A_1)\right),$$

где $c = 4$ для $\varepsilon(A_3) = -1$, $c = \frac{25}{2}$ для $\varepsilon(A_3) = +1$.

2.3. Специализацией $A' = \begin{pmatrix} 5 & 0 \\ 0 & 5 \end{pmatrix}$, $Q' = 1_7$ методом ортогонального дополнения получен трёхклассный род $[Q]$ форм вида

$$Q_1 = A_4 \oplus 5\cdot\mathbb{Z}^1, \quad Q_2 = \mathbb{Z}^3\oplus 5\cdot\mathbb{Z}^2, \quad Q_3 = 1\cdot\mathbb{Z}^1 \oplus \begin{pmatrix} 2 & 0 & 0 & 1 \\ 0 & 3 & -1 & -3 \\ 0 & -1 & 2 & 1 \\ 1 & -3 & 1 & 6 \end{pmatrix}.$$

Его инварианты имеют вид $h([Q]) = 3$, $d = 25$, $o(Q_1) = 480$, $o(Q_2) = 384$, $o(Q_3) = 64$, $5_{[Q]} = 1^{+3}5^{+2}$, $2_{[Q]} = 1^{+5}_{\mathrm{I},5}$. Пусть бинарная квадратичная форма A с нечётным уровнем a имеет 5-символ вида $5_A = 5^{\varepsilon(A_5)2}$. Тогда возникает ветвление представлений формы

A родом $[Q]$ над кольцом $\mathbb{Z}_5$. Ветвящийся множитель $\alpha_5(A,Q)$ по теореме 2 имеет вид

$$\alpha_5(A,Q)=\sum_{i=1}^{2}\alpha_5(A,Q,G^{\mathrm{I}},C_i)+\alpha_5(A,Q,G^{\mathrm{II}}),$$

где слагаемые правой части заданы соотношениями

$$\alpha_5(A,Q,G^{\mathrm{I}},C_1)=0 \quad \text{для} \quad \varepsilon(A_5)=-1,$$
$$\alpha_5(A,Q,G^{\mathrm{I}},C_1)=\frac{5}{8}\left(1-\frac{1}{5}\varepsilon(A_5)\right) \quad \text{для} \quad \varepsilon(A_5)=+1,$$
$$\alpha_5(A,Q,G^{\mathrm{I}},C_2)=2\cdot 3\cdot 5^5\cdot\left(1-\frac{1}{5}\varepsilon(A_5)\right),$$
$$\alpha_5(A,Q,G^{\mathrm{II}})=\frac{6}{5}\left(1-\frac{1}{5}\varepsilon(A_5)\right).$$

Отсюда прямым вычислением находим значение ветвящегося множителя:

$$\alpha_5(A,Q)=2^{-1}+2^3\cdot 3\cdot 5^{-2}(5^6+1)=15001\frac{23}{50} \quad \text{для} \quad \varepsilon(A_5)=+1,$$
$$\alpha_5(A,Q)=5^{-2}\cdot 6^2(5^6+1)=22501\frac{11}{25} \quad \text{для} \quad \varepsilon(A_5)=-1. \tag{2.13}$$

Локальный множитель $\alpha_2(A,Q)$ определяется соотношением [4]:

$$\alpha_2(A,Q)=\frac{1}{4}(1\pm\frac{1}{2}), \quad \text{если} \quad \mathrm{oct}\equiv\pm1 \quad \text{или} \quad \pm 3 (\mathrm{mod}\, 8), \tag{2.14}$$

где $\mathrm{oct}\equiv 5-t(A_1)(\mathrm{mod}\, 8)$ $(1-t(A_1) \pmod 8)$ для $\left(\frac{-a}{2}\right)=+1$ (-1, соответственно). Вес примитивных представлений формы A родом $[Q]$ равен

$$pn(A,Q)=2^{-1}3^{-1}\alpha_2(A,Q)\alpha_5(A,Q)\times$$
$$\times\prod_{p||\,|A|,p\neq 2,5}\left(p+\left(\frac{5}{p}\right)\varepsilon(A_1)\right)\prod_{p^2||\,|A|,p\neq 2,5}(p^2-1),$$

где $\alpha_2(A,Q)$, $\alpha_5(A,Q)$ приведены в (2.13), (2.14).

Литература

1. C. L. Siegel, *Lectures on the analytical theory of quadratic formes,* Third revised edition, Göttingen, 1963.

2. Дж. Касселс, *Рациональные квадратичные формы,* М., 1982.
3. Y. Kitaoka, *Local densities of quadratic forms,* Advanced Studies in Pure Math. **13** (1988), 433–460.
4. В. Г. Журавлёв, *Представление формы родом квадратичных форм,* Алгебра и анализ **8**, No. 1 (1996), 21–112.
5. Дж. Конвей, Н. Слоэн, *Упаковки шаров, решётки, группы,* т. 1, М., 1990.
6. С. В. Фёдорова, *Примитивные представления бинарной формы непростого определитиля,* Вестник Владимирск. госуд. пед. ун-та, No. 5 (2000), 324–331.
7. С. В. Фёдорова, *Представление форм квадратичными формами. VII* международная конференция. Математика. Экономика. Экология. Образование. Тезисы докладов. Ростов-на-Дону (1999), 107–108.
8. Э. Артин, *Геометрическая алгебра,* М., 1969.
9. В. Г. Журавлёв, *Вложение p-элементарных решёток,* Изв. РАН, Сер. мат. **63**, No. 1 (1999), 77–106.

Владимирский государственный
педагогический университет

Поступило 24 августа 2000 г.