Общероссийский математический портал

В. Г. Журавлев, Вложение p -элементарных решеток, *Изв. РАН. Сер. матем.*, 1999, том 63, выпуск 1, 77–106

DOI: <https://doi.org/10.4213/im229>

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

Параметры загрузки:

IP: 18.234.156.22

26 апреля 2023 г., 15:58:22

УДК 511

В. Г. Журавлёв

Вложение p -элементарных решеток

Исследуется ветвление вложений локальных решеток или квадратичных форм над кольцом целых p -адических чисел $\mathbb{Z}_p$. Доказано, что каждое примитивное вложение однозначно раскладывается в ортогональную сумму минимальных неразложимых вложений и для p -элементарных решеток построены все такие вложения. Теория ветвления позволяет находить количество орбит представлений форм и, в частности, чисел другими квадратичными формами над кольцом $\mathbb{Z}_p$, а в формуле веса представлений формы родом квадратичных форм позволяет вычислить локальные множители.

Библиография: 7 наименований.

Введение

В [2] доказана формула для веса целых представлений

$$Q[b] = {}^t b \cdot Qb = A \quad (0.1)$$

квадратичной формы A размерности m положительно определенными формами Q размерности $n > m$ некоторого рода $\mathcal{F}$, b берется из множества $(n \times m)$ -матриц $M_{n,m}(\mathbb{Z})$ с коэффициентами из кольца целых рациональных чисел $\mathbb{Z}$. Вес примитивных представлений формы A родом $\mathcal{F}$, ассоциированных с формами рода $\mathcal{G}$, определяется равенством

$$\text{rp}^+(A; \mathcal{F}, \mathcal{G}) = \sum_{\{Q\}^+ \subset \mathcal{F}} \sum_b \frac{1}{o^+(Q)}, \quad (0.2)$$

где b пробегает примитивные представления (0.1) с условием, что соответствующая форма $G = G(b)$ из ортогонального дополнения к A принадлежит заданному роду $\mathcal{G}$, $o^+(Q)$ – порядок группы целых собственных автоморфизмов формы Q . Формула из [2]

$$\text{rp}^+(A; \mathcal{F}, \mathcal{G}) = m^+(\mathcal{G})c(A; \mathcal{F}, \mathcal{G}) \quad (0.3)$$

выражает вес примитивных представлений (0.2) через собственную массу рода

$$m^+(\mathcal{G}) = \sum_{\{G\}^+ \subset \mathcal{G}} \frac{1}{o^+(G)}$$

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (грант 96-01-00502).

и конечное произведение $c(A; \mathcal{F}, \mathcal{G})$ вида

$$c(A; \mathcal{F}, \mathcal{G}) = \prod_{p|2ad} c_p(A; Q, G)$$

для некоторых форм Q из $\mathcal{F}$ и G из $\mathcal{G}$. Произведение берется по всем простым делителям $2ad$, где a – *степень* формы A и d – *определитель* формы Q .

Случай взаимно простых a и d исследован в [2], и там, например, показано, что для нечетных p , не делящих d , локальный множитель $c_p(A; Q, G)$ равен порядку группы автоморфизмов

$$O_p(q(A)) = \{U / \text{mod } A \in \text{GL}_m(\mathbb{Z}_p) : A^{-1}[U] \equiv A^{-1} \pmod{\mathbb{Z}_p}\}$$

дискриминантной формы A^{-1} над кольцом целых p -адических чисел $\mathbb{Z}_p$, и для этих групп найден порядок.

Формула веса примитивных представлений (0.3), аналогично формуле Зигеля [6], 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 $\mathbb{Z}_p$ этой же формы любой формой рода.

Наиболее трудным для изучения является случай a и d с общими делителями. В этом случае имеет место *ветвление* представлений (0.1), когда форма A и род $\mathcal{F}$ перестают однозначно определять род $\mathcal{G}$ форм $G = G(b)$. В частности, это проявляется в разбиении на различные *орбиты* $\{b\}$ множества примитивных представлений $b : Q[b] = A$ над локальными кольцами $\mathbb{Z}_p$ для простых p , делящих одновременно a и d . Все орбиты разбиваются на множества $\text{pb}_{Q,A}(\{G\})$, нумеруемые конечным числом классов $\{G\} = \{G\}_{\mathbb{Z}_p}$, и это дает “грубую” классификацию орбит. Внутри же указанных множеств существует взаимно однозначное соответствие между орбитами $\{b\}$ и $O(G)$ -*орбитами* $\{C\}$ сцепляющих формы A и G матриц C – это “тонкая” классификация орбит $\{b\}$.

Для *одномерных* форм A небольших степеней полная классификация орбит приведена в [7]. Оказалось, что даже в одномерном случае число орбит $\{b\}$ может быть сколь угодно большим. В качестве примера можно привести квадратичное уравнение

$$x_1^2 + px_2^2 + p^2x_3^2 + p^3x_4^2 = p^3, \quad x_i \in \mathbb{Z}_p,$$

множество решений которого состоит из $(7p - 3)/4$ или $(5p + 1)/4$ орбит соответственно условию $p \equiv 1 \pmod{4}$ или $p \equiv 3 \pmod{4}$.

В данной работе рассматривается ветвление представлений *p-элементарных форм* A , т.е. форм простой степени $a = \varepsilon p$ с единицей ε из $\mathbb{Z}_p^\times$ для нечетных p . В основном тексте используются удобные для вычислений квадратичные формы и их матрицы. Общие же конструкции становятся более прозрачными, если использовать бескоординатный язык решеток. Чтобы избежать усложнений, ограничимся локальными кольцами $\mathbb{Z}_p$, хотя большая часть приводимых ниже построений допускает и кольцо целых чисел $\mathbb{Z}$.

0.1. Обозначим L_A целую невырожденную $\mathbb{Z}_p$ -решетку с квадратичной формой (матрицей) A размерности m и уровня a . Аналогично, пусть $L_{\frac{1}{a}G}$ – решетка (не обязательно целая) с целой невырожденной формой G размерности k . Рассмотрим прямую ортогональную сумму

$$L = L_A \oplus L_{\frac{1}{a}G}$$

– решетку размерности $n = m + k$ с квадратичной формой $A \oplus \frac{1}{a}G$, и определим для нее расширение

$$L^* = L_A^* \oplus L_{\frac{1}{a}G},$$

где $L_A^* = A^{-1} \cdot L_A$ – двойственная для L_A решетка. Пусть

$$\text{pr}: L^* \rightarrow L_{\frac{1}{a}G}$$

– ортогональная проекция на вторую компоненту и $L'_{\frac{1}{a}G}$ – любое ее целое сечение с условиями

$$\begin{aligned} \text{pr}: L'_{\frac{1}{a}G} &\xrightarrow{\sim} L_{\frac{1}{a}G} \quad - \text{биекция } \mathbb{Z}_p\text{-модулей,} \\ L'_{\frac{1}{a}G} &- \text{целая подрешетка из } L^*. \end{aligned} \quad (0.4)$$

Тогда

$$L' = L_A + L'_{\frac{1}{a}G} \quad (0.5)$$

– прямая (не обязательно ортогональная) сумма $\mathbb{Z}_p$ -модулей из L^* . Более того, из включений $(L_A, L'_{\frac{1}{a}G}) \subset (L_A, L^*) = (L_A, L_A^*) \subset \mathbb{Z}_p$ вытекает, что L' – целая подрешетка из L^* максимальной размерности $\dim L' = m + k = n$. Два сечения сравнимы: $L'_{\frac{1}{a}G} \equiv L''_{\frac{1}{a}G} \pmod{L_A}$, если разности между их элементами с совпадающими образами в $L'_{\frac{1}{a}G}$ принадлежат решетке L_A . Нетрудно заметить, что сечения сравнимы $\text{mod } L_A$ тогда и только тогда, когда они дают одну и ту же решетку: $L' = L''$ (см. (0.2)). В эту целую решетку примитивно вкладывается

$$\text{em}: L_A \hookrightarrow L' \quad (0.6)$$

– исходная решетка L_A , т.е. (0.6) – инъективный гомоморфизм модулей, сохраняющий квадратичные формы. Примитивность означает, что $L'/\text{em}(L_A) \simeq L'_{\frac{1}{a}G}$ – свободный $\mathbb{Z}_p$ -модуль. Выбирая различные целые формы G и сечения $L'_{\frac{1}{a}G}$ (см. (0.4)), можно получить все примитивные вложения решетки L_A .

0.2. Существует каноническое соответствие между сечениями и сцепляющими гомоморфизмами модулей

$$C: L_{\frac{1}{a}G} \rightarrow L_A^*. \quad (0.7)$$

Любой гомоморфизм C дает сечение $L'_{\frac{1}{a}G} = (C \oplus \text{id})L_{\frac{1}{a}G}$ как график в ортогональной сумме $L^* = L_A^* \oplus L_{\frac{1}{a}G}$ над решеткой $L_{\frac{1}{a}G}$. Обратное утверждение вытекает

из биективности проекции pr (см. (0.4)). Используя сцепляющие гомоморфизмы C , легко заметить, что условие целостности сечения $L'_{\frac{1}{a}G}$ равносильно целостности квадратичной формы

$$\left(A^{-1} \oplus \frac{1}{a}G\right)[C \oplus \text{id}] = A^{-1}[C] + \frac{1}{a}G, \quad (0.8)$$

а условие $L'_{\frac{1}{a}G} \equiv L''_{\frac{1}{a}G} \pmod{L_A}$ равносильно сравнению для гомоморфизмов $C' \equiv C'' \pmod{L_A}$. Группы автоморфизмов $O(A)$ и $O(G)$ решеток L_A и L_G действуют на множестве гомоморфизмов (0.7): $C \mapsto {}^tUCV$, где ${}^tU \in O(A^{-1})$. Обозначим $\{C\}$ орбиту $C \pmod{L_A}$. Для любого гомоморфизма из орбиты форма (0.8) целая, и, таким образом, получаем целые сечения

$$L_{\frac{1}{a}G}(C) = (C \oplus \text{id})L_{\frac{1}{a}G} \subset L^*$$

и порождаемые ими примитивные вложения решетки L_A

$$C: L_A \hookrightarrow L_{\frac{1}{a}G}^A(C) = L_A + L_{\frac{1}{a}G}(C). \quad (0.9)$$

0.3. Фиксируем целую решетку L_Q с формой Q размерности n . Если $\text{em}: L_A \hookrightarrow L_Q$ – какое-то примитивное вложение, то найдутся целая форма G и гомоморфизм C (см. (0.4)), расщепляющие вложение em в композицию:

$$\text{em}: L_A \xrightarrow{(0.6)} L_{\frac{1}{a}G}^A(C) \xrightarrow{\sim} L_Q, \quad (0.10)$$

где вторая стрелка – изоморфизм решеток. Более того, для орбит $\{\text{em}\}$ относительно групп $O(A)$ и $O(Q)$ отображение

$$\{\text{em}\} \xrightarrow{\sim} \{C\} \quad (0.11)$$

есть биекция. В теории чисел задача вложения решеток обычно формулируется в координатной форме:

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

где $b \in M_{n,m}(\mathbb{Z}_p)$ – примитивная матрица, т.е. матрица с единичными элементарными делителями. Биекция (0.11) трансформируется в биекцию

$$\{b\} \xrightarrow{\sim} \{C\}, \quad (0.12)$$

где $\{b\}$ – также двойные орбиты относительно групп $O(Q)$ и $O(A)$. Отсюда сразу вытекает конечность числа орбит примитивных вложений $\text{em}: L_A \hookrightarrow L_Q$ или орбит $\{b\}$ представлений формы A формой Q , поскольку A и Q однозначно определяют определитель формы G из (0.10). Нахождение же числа орбит $\{C\}$, а ввиду (0.12) и орбит $\{b\}$, сводится к описанию ортогональных групп $O(A)$ и $O(G)$ над кольцом вычетов $\mathbb{Z}_p/a\mathbb{Z}_p$.

0.4. Классифицировать примитивные вложения решетки L_A значит согласно (0.11) классифицировать орбиты $\{C\}$ сцепляющих гомоморфизмов C (см. (0.7)). С этой целью выделяется ортогональное ядро гомоморфизма C и его ортогональное дополнение разлагается в сумму максимально возможной длины:

$$C = \text{Ker } C \oplus C_{\min}, \quad C_{\min} = \bigoplus_i C_i,$$

где

$$C_{\min}: L_A \hookrightarrow L_{\frac{1}{a}G_{\min}}^A(C_{\min})$$

– *минимальное* вложение, распадающееся в ортогональную сумму *минимальных неразложимых* вложений

$$C_i: L_{A_i} \hookrightarrow L_{\frac{1}{a}G_i}^{A_i}(C_i)$$

решеток из разложения $L_A = \bigoplus_i L_{A_i}$. Для фиксированного уровня a таких вложений C_i , с точностью до изоморфизма, конечное число, и из них можно получить любое вложение решетки L_A . Минимальные неразложимые вложения можно рассматривать как аналог простых чисел или неприводимых представлений.

0.5. Имеет арифметический смысл и общее число $c_p(A; Q, G)$ всех сцепляющих гомоморфизмов $C \bmod L$ из разложения (0.10). Для его выявления перейдем к примитивным представлениям b (см. (0.1)) над кольцом $\mathbb{Z}$. Аналогично (0.10) примитивному представлению b ставится в соответствие собственный класс $\{G(b)\}^+$ целых положительно определенных форм с определителем

$$\det G = \frac{a^{n-m}d}{\det A}.$$

Как уже отмечалось, вес $\text{pn}^+(A; \mathcal{F}, \mathcal{G})$ (см. (0.2)) примитивных представлений формы A родом $\mathcal{F}$, ассоциированных с формами рода $\mathcal{G}$, вычисляется по формуле (0.3) с локальными множителями, равными $c_p(A; Q, G)$. Если множество $\text{pb}_{Q,A}(\{G\})$ одноорбитное, то вычисление множителя $c_p(A; Q, G)$ сводится к изучению прямого произведения локальных групп автоморфизмов дискриминантных форм A^{-1} , G^{-1} и некоторых его централизаторов.

Формула (0.3) напоминает формулу Зигеля [6], где вместо локальных множителей $c_p(A; Q, G)$ участвуют локальные плотности $\alpha_p(A; Q)$.

0.6. В статье рассматриваются вложения локальных *нечетных* p -элементарных решеток L_A . В этом случае проблемы, сформулированные в пп. 0.3–0.5, удаётся решить полностью.

Для p -элементарной формы A и любой $\mathbb{Z}_p$ -целой невырожденной формы Q определены (теорема 5.1) все возможные формы G из разложения (0.10), вычислены инварианты орбит $\{b\}$ примитивных представлений $Q[b] = A$, $b \in M_{n,m}(\mathbb{Z}_p)$, и найдено число таких орбит $\{b\}$.

Минимальные неразложимые вложения p -элементарных решеток L_A имеют размерности не более четырех. Все они выявлены в теореме 6.1. Доказано, что примитивные вложения $L_A \hookrightarrow L_Q$ однозначно распадаются в ортогональную сумму минимальных неразложимых вложений.

Инварианты орбит $\{C\}$ сцепляющих гомоморфизмов C (см. (0.7)) используются для вычисления локальных множителей $c_p(A; Q, G)$. В теореме 7.1 доказана формула, выражающая множители $c_p(A; Q, G)$ через порядки полной линейной и некоторых ортогональных групп над конечным простым полем.

0.7. Наш метод отличается от *метода склейки* (см., например, [4, с. 132], [5]) асимметрией конструкции соединения форм A и G , проявляющейся в направленности сцепляющих гомоморфизмов $C: L_{\frac{1}{a}G} \rightarrow L_A^*$. Сравним задачу вложения (0.7) решетки L_A в решетку L_Q с задачей дополнения подрешетки $L_A \oplus L_G$ до полной решетки L_Q . Во втором случае роли решеток L_A и L_G симметричны, а в первом они таковы только для унимодулярных решеток L_Q .

Несколько слов об обозначениях. Используемый язык линейной алгебры элементарен и конструктивен. Однако на определенном этапе формулы обрастают многочисленными индексами. Сами по себе индексы несущественны, имеет значение лишь их взаимное положение. Упрощают сложные выражения диаграммы, делающие прозрачными отношения входящих в них элементов. Поскольку диаграммы имеют вид раскрашенных деревьев, то по техническим причинам они здесь не приводятся.

§ 1. Орбиты примитивных представлений

Дается краткое изложение результатов работы [2] для локальных колец $\mathbb{Z}_p$. Дополнительно для двойных орбит представлений квадратичных форм формами большей размерности приводится параметризация орбитами сцепляющих гомоморфизмов.

1.1. Пусть $Q = {}^tQ$ – симметрическая невырожденная матрица порядка n из множества матриц $M_n(\mathbb{Z}_p)$ с коэффициентами из кольца целых p -адических чисел $\mathbb{Z}_p$, и пусть $A = {}^tA$ – невырожденная матрица из множества $M_m(\mathbb{Z}_p)$ размерности $1 \leq m < n$. Матрица Q представляет A , если уравнение

$$Q[b] = {}^tbQb = A \quad (1.1)$$

имеет решение b на множестве $(n \times m)$ -матриц $M_{n,m}(\mathbb{Z}_p)$. Так, если размерность $m = 1$, т.е. A – число, то приходим к задаче о представлении в локальном кольце $\mathbb{Z}_p$ числа A квадратичной формой $Q[X]$. Поскольку мы ищем решения b из $M_{n,m}(\mathbb{Z}_p)$, то можно отождествить квадратичные формы с их матрицами и говорить только о формах.

1.2. Среди всех решений b матричного уравнения (1.1) выделяются примитивные решения, к которым сводится общий случай. Решение b *примитивно*, если наибольший общий делитель $d(b)$ миноров порядка m матрицы b равен 1. Примитивность b равносильна существованию *дополнительной* матрицы e из $M_{n,k}(\mathbb{Z}_p)$ для $k = n - m$ с условием, что *расширенная* матрица $B = (b \ e)$ принадлежит унимодулярной группе $SL_n^\pm(\mathbb{Z}_p)$ матриц M с коэффициентами из $\mathbb{Z}_p$ и определителем $|M| = \pm 1$.

1.3. Итак, пусть Q и A – невырожденные целые матрицы и b – примитивное представление формы A формой Q , т.е. решение матричного уравнения (1.1). Тогда форма Q эквивалентна относительно группы $\mathrm{SL}_n^{\pm}(\mathbb{Z}_p)$ целой форме

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

$(Q \sim Q_B)$, которая преобразованием, вообще говоря, рациональным,

$$M_C = \begin{pmatrix} 1_m & -A^{-1}C \\ 0 & 1_k \end{pmatrix}$$

из группы $\mathrm{SL}_n(\mathbb{Q}_p)$ разлагается в прямую сумму $Q_B[M_C] = \begin{pmatrix} A & 0 \\ 0 & G' \end{pmatrix}$ форм A и $G' = Q' - A^{-1}[C]$.

Здесь и далее *целое* и *рациональное* – синонимы p -целого и p -рационального. Обозначим a p -уровень формы A . Это – целое число, для которого целой будет матрица $E = a \cdot A^{-1}$, но не матрица $\frac{a}{p}A^{-1}$. Следовательно,

$$aQ_B[M_C] = \begin{pmatrix} aA & 0 \\ 0 & G \end{pmatrix}, \quad G = G_{Q,A}(B) = aQ' - E[C], \quad (1.2)$$

G – целая симметрическая невырожденная матрица порядка $k = n - m > 0$. Поскольку матрица Q целая, то C содержится во множестве c_G^A решений матричного сравнения

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

Обратно, для произвольного решения C сравнения (1.3) матрица

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

будет целой. Согласно формуле (1.2) определитель

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

формы G является инвариантом: $|G|$ не зависит от выбора примитивного представления b (1.1). В то же время сама форма G (см. (1.2)) и решение C сравнения (1.3) зависят не только от b , но и от выбора расширенной матрицы $B = (be)$.

1.4. Чтобы описать эту зависимость, рассмотрим всю совокупность B_b матриц $B = (b^*)$ из группы $\mathrm{SL}_n^\pm(\mathbb{Z}_p)$ с данными первыми m столбцами b . Прежде всего заметим, что если фиксировать какую-то матрицу $B = (be)$, то любая другая матрица B^* из B_b получается умножением справа B на подходящую матрицу $T = \begin{pmatrix} 1_m & S \\ 0 & V \end{pmatrix}$ из группы $\mathrm{SL}_n^\pm(\mathbb{Z}_p)$ с блоками S из $M_{m,k}(\mathbb{Z}_p)$ и V из $\mathrm{SL}_k^\pm(\mathbb{Z}_p)$. Разложение $B^* = BT$ определяет *биекцию* $B^* \xrightarrow{\sim} T$ между множествами B_b и подгруппой матриц T указанного вида. Используя разложение $B^* = BT$, находим форму

$$Q_{B^*} = \begin{pmatrix} A & C^* \\ {}_t C^* & Q'^{*} \end{pmatrix} = Q_B[T],$$

откуда вытекает формула

$$C^* = T(C), \quad T(C) = AS + CV. \quad (1.6)$$

Для вычисления формы G^* из разложения $aQ_{B^*}[M_{C^*}] = \begin{pmatrix} aA & 0 \\ 0 & G^* \end{pmatrix}$ заметим, что $M_{C^*} = T^{-1}M_C \begin{pmatrix} 1 & 0 \\ 0 & V \end{pmatrix}$. Поэтому можем записать

$$aQ_{B^*}[M_{C^*}] = aQ_B[M_C] \left[\begin{pmatrix} 1 & 0 \\ 0 & V \end{pmatrix} \right],$$

и, следовательно,

$$G^* = G[V], \quad V \in \mathrm{SL}_k^\pm(\mathbb{Z}_p), \quad (1.7)$$

т.е. G^* принадлежит классу $\{G\}$ формы G относительно группы $\mathrm{SL}_k^\pm(\mathbb{Z}_p)$ и этот класс $\{G\}$ не зависит от выбора расширенной матрицы $B = (be)$. Отображение

$$\begin{array}{ccc} [Q, A]: b & \longrightarrow & \{G\} \\ & \searrow & \nearrow \\ & B_b & \end{array}$$

задает для множества $\mathrm{pb}_{Q,A}$ примитивных представлений b (1.1) разбиение

$$\mathrm{pb}_{Q,A} = \sum_{\{G\}} \mathrm{pb}_{Q,A}(\{G\}) \quad (1.8)$$

на классы $\mathrm{pb}_{Q,A}(\{G\}) = [Q, A]^{-1}(\{G\})$. При этом $\{G\}$ пробегает только классы форм с определителем $|G|$ (1.5), а значит, разбиение (1.8) конечное.

1.5. Для фиксированной формы G выделим из B_b подмножество $B_{b,G}$ матриц B , отображающихся в $G_{Q,A}(B) = G$ (1.2). Теперь произвольная матрица $B^* = BT$ принадлежит $B_{b,G}$ тогда и только тогда, когда у матрицы $T = \begin{pmatrix} 1 & S \\ 0 & V \end{pmatrix}$ блок V в силу формулы (1.7) удовлетворяет условию $G^* = G[V] = G$, т.е. V принадлежит ортогональной группе $O(G) = O_{\mathbb{Z}_p}(G)$ квадратичной формы G над кольцом $\mathbb{Z}_p$. Группа T_G таких матриц T действует по формуле (1.6) на множестве решений c_G^A сравнения (1.3) и разбивает его на орбиты $\text{cl}(C) = \{T(C) : T \in T_G\}$. Если представление b из $\text{pb}_{Q,A}(\{G\})$ в последовательности отображений

$$b \mapsto B_{b,G} \mapsto \text{cl}(C)$$

заменить на γb , где γ – любой элемент из ортогональной группы $O(Q)$, то ввиду равенства $Q_{\gamma B} = Q_B$ представление γb снова принадлежит $\text{pb}_{Q,A}(\{G\})$ и отображается в прежнюю орбиту $\gamma b \mapsto B_{\gamma b,G} \mapsto \text{cl}(C)$. Более того, мы получаем биекцию между орбитами

$$\text{pb}_{Q,A}(\{G\}) \supset \langle b \rangle \xrightarrow[\sim]{[Q,A,G]} \text{cl}(C) \subset c_G^A(Q), \quad (1.9)$$

где $\langle b \rangle = \{\gamma b : \gamma \in O(Q)\}$ и $c_G^A(Q)$ – подмножество из c_G^A матриц C с условием, что форма $Q_G^A(C)$ (1.4) принадлежит классу $\{Q\}$.

1.6. Для любого преобразования $T = \begin{pmatrix} 1 & S \\ 0 & V \end{pmatrix}$ из группы T_G образ $T(C)$ сравним с CV по $\text{mod } A$, где V пробегает всю группу $O(G)$, и сравнение означает, что матрица $A^{-1}(T(C) - CV)$ целая. Это сравнение приводит нас к орбитам $\langle C \rangle = \{CV / \text{mod } A : V \in O(G)\}$ из множества $C_G^A = c_G^A / \text{mod } A$ и к биекции между орбитами

$$c_G^A(Q) \supset \text{cl}(C) \xrightarrow[\sim]{\text{mod } A} \langle C \rangle \subset C_G^A(Q),$$

где $C_G^A(Q)$ состоит из классов $C / \text{mod } A \in C_G^A$, для которых $Q_G^A(C) \sim Q$. Соединяя указанную биекцию с биекцией (1.9), получаем новую, более удобную для вычислений биекцию

$$\text{pb}_{Q,A}(\{G\}) \subset \langle b \rangle \xrightarrow[\sim]{[Q,A,G]/\text{mod } A} \langle C \rangle \subset C_G^A(Q). \quad (1.10)$$

Как следствие из конечности числа решений $\text{mod } A$ сравнения (1.3) и конечности разбиения (1.8) вытекает конечность числа орбит $\langle b \rangle : Q[b] = A$ для случая невырожденных квадратичных форм Q , A и локальных колец $\mathbb{Z}_p$.

1.7. На представления b (1.1) действует вместе с $O(Q)$ и группа $O(A)$, поскольку $Q[bU] = A[U] = A$ для матрицы U из $O(A)$. Оставаясь в условиях п. 1.5, считаем форму G фиксированной, и для b его расширенная матрица $B = (b \ e)$ принадлежит $B_{b,G}$. Тогда для $B_U = B \begin{pmatrix} U & 0 \\ 0 & 1 \end{pmatrix} = (bU | e)$ согласно п. 1.3 находим

$$Q_{B_U} = Q_B \left[\begin{pmatrix} U & 0 \\ 0 & 1 \end{pmatrix} \right] = \left(\begin{array}{c|c} A & {}^t U C \\ \hline {}^t C U & \frac{1}{a}(E[{}^t U C] + G) \end{array} \right). \quad (1.11)$$

Относительно доказательства (1.11) заметим, что условие $A[U] = A$ равносильно $A^{-1}[{}^tU] = A^{-1}$ и отображение

$$O(A) \xrightarrow{\sim} O(E): A \mapsto {}^tA \quad \text{для } E = aA^{-1} \quad (1.12)$$

– антиавтоморфизм. Из формулы (1.11) заключаем, что для bU расширенная матрица B_U принадлежит множеству $B_{bU, G}$, отображающемуся согласно п. 1.5 в орбиту $\text{cl}({}^tU C)$. Поэтому действие ортогональной группы $O(A)$ сохраняет биекцию (1.10):

$$\text{pb}_{Q, A}(\{G\}) \supset \langle bU \rangle \xrightarrow{\sim} \langle {}^tU C \rangle \subset C_G^A(Q). \quad (1.13)$$

Последнее включение вытекает из формулы (1.11) и из того, что форма (1.4)

$$Q_G^A({}^tU C) = Q_{B_U} = Q_B \left[\begin{pmatrix} U & 0 \\ 0 & 1 \end{pmatrix} \right]$$

эквивалентна форме Q_B , а по предположению $Q_B \sim Q$. Вводя *двойные орбиты*

$$\begin{aligned} \{b\} &= \{\gamma bU : \gamma \in O(Q), U \in O(A)\}, \\ \{C\} &= \{{}^tU CV / \text{mod } A : U \in O(A), V \in O(G)\} \end{aligned} \quad (1.14)$$

ортогональных групп $O(\cdot) = O_{\mathbb{Z}_p}(\cdot)$, из (1.10) и (1.13) получаем

ПРЕДЛОЖЕНИЕ 1.1. *Биекцию (1.10) можно поднять до биекции*

$$\text{pb}_{Q, A}(\{G\}) \supset \{b\} \xrightarrow[\sim]{[Q, A, G] / \text{mod } A} \{C\} \subset C_G^A(Q) \quad (1.15)$$

двойных орбит $\{b\}$ примитивных представлений $b : Q[b] = A$ и орбит $\{C\}$ из множества C_G^A решений $\text{mod } A$ сравнения $E[C] \equiv -G \pmod{a\mathbb{Z}_p}$. Оба множества из (1.15) пусты, если определитель $|G|$ отличен от (1.5).

Таким образом, двойные орбиты $\{b\}$ параметризуются классами форм $\{G\}$ и двойными орбитами $\{C\}$ решений отвечающему G сравнению (1.3).

§ 2. Сцепляющие матрицы

Рассматриваются матрицы сцепляющих гомоморфизмов C (0.7), и для их двойных орбит $\{C\}$ находится полная система инвариантов.

2.1. В уравнении $Q[b] = A$, в матрице $Q_G^A(C)$ и в других конструкциях из § 1 формы A, Q, G можно заменять эквивалентными формами A', Q', G' . Так, например, важное в приложениях число элементов $c(A; Q, G)$ множества $C_G^A(Q)$ п. 1.6 сохраняется при такой замене:

$$c(A; Q, G) = c(A'; Q', G'),$$

т.е. является функцией классов $\{A\}, \{Q\}, \{G\}$. Далее, можем считать

$$A = \begin{pmatrix} A_0 & 0 \\ 0 & A_1 \end{pmatrix} = A_0 \oplus A_1, \quad \text{где } |A_0| \not\equiv 0 \pmod{p\mathbb{Z}_p},$$

или, короче, $|A_0| \not\equiv 0(p)$, $A_1 = pA_p$, а также считать, что матрицы из C_G^A выбираются в виде $C = \begin{pmatrix} 0 \\ C_1 \end{pmatrix}$. Тогда форма (1.4) разлагается в прямую сумму:

$$Q_G^A(C) = A_0 \oplus Q_G^{A_1}(C_1),$$

при этом $c(A; Q, G) = c(A_1; Q \ominus A_0, G)$, где разность $Q \ominus A_0$ есть любая форма X из разложения $Q \sim A_0 \oplus X$. Если X не существует, то $c(A; Q, G) = 0$. Поэтому общая задача нахождения $\{G\}$ и $\{C\}$ сводится к случаю форм $A = pA_p$.

2.2. Начиная с этого места, полагаем $A = pA_p$, $|A_p| \not\equiv 0(p)$ и p – нечетное простое число.

ЗАМЕЧАНИЕ. Может показаться, что для таких форм A все представления b (1.1) примитивные. Однако пример

$$\left(\begin{array}{cc|c} 0 & 1 & \\ \hline 1 & 0 & \\ \hline & & * \end{array} \right) \left[\begin{pmatrix} 1 & 0 \\ 0 & p \\ 0 & 0 \end{pmatrix} \right] = \begin{pmatrix} 0 & p \\ p & 0 \end{pmatrix}$$

опровергает это предположение.

Выбираем уровень $a = p \cdot \{a\}$ с произвольной единицей $\{a\}$ кольца $\mathbb{Z}_p$; и тогда форма $E = aA^{-1}$ имеет определитель $|E| \not\equiv 0(p)$. Пусть $G = \bigoplus_{\alpha} G_{\alpha}$ с блоками $G_{\alpha} = p^{\alpha} G_{p^{\alpha}}$, $\alpha \geq 0$, $|G_{p^{\alpha}}| \not\equiv 0(p)$, размерностей $\dim G_{\alpha} = k_{\alpha} \geq 1$, и, значит, $\dim G = k = \sum_{\alpha} k_{\alpha}$. В этом случае согласно (1.3)

$$E[C] \equiv -G(p), \quad \text{где } C = (C_0 | C_1 | \dots) / \text{mod } p \in M_{m,k}(\mathbb{Z}_p) \quad (2.1)$$

– сцепляющие матрицы – разбиты на блоки аналогично форме G . Наша цель – описать орбиты $\{C\} = \{UCV / \text{mod } p : U \in O(E), V \in O(G)\}$ решений сравнения (2.1).

2.3. Нам потребуются некоторые результаты [1] о квадратичных пространствах V над полем характеристики $\text{char} \neq 2$. Пусть V невырожденно, $|V| = \det V \neq 0$, U – подпространство из V , $U^{\perp}$ и $\text{rad } U = U \cap U^{\perp}$ – его *ортогональное дополнение* и *радикал* соответственно. Имеют место следующие утверждения:

$$\begin{aligned} U^{\perp\perp} &= U, \quad \text{rad } U = \text{rad } U^{\perp}; \\ \dim V &= \dim U + \dim U^{\perp}; \\ V &= U \oplus U^{\perp}, \quad \text{если } |U| \neq 0; \end{aligned} \quad (2.2)$$

здесь $\oplus$ – ортогональная сумма; обратно, если $V = U \oplus W$, то $|U| \neq 0$, $|W| \neq 0$ и $W = U^{\perp}$.

Еще потребуется один результат о продолжении изометрий $\sigma: U \xrightarrow{\sim} U'$ двух подпространств U и U' до изометрии $\rho: V \xrightarrow{\sim} V'$ содержащих их невырожденных пространств V и V' .

ТЕОРЕМА ВИТТА. 1) Любая изометрия σ продолжается до изометрии объемлющих пространств ρ : $\rho|_U = \sigma$.

2) Для фиксированного $\varepsilon = \pm 1$ найдется продолжение ρ с определителем $|\rho| = \det \rho = \varepsilon$ тогда и только тогда, когда $\dim U + \dim \text{rad } U < \dim V$.

2.4. Согласно (2.1) $E[C_0] \equiv -G_0(p)$ с $|G_0| \not\equiv 0(p)$. По теореме Витта можем считать

$$E = \begin{pmatrix} -G_0 & 0 \\ 0 & e \end{pmatrix} = -G_0 \oplus e$$

и после замены $C \mapsto UC / \text{mod } p$ с подходящим U из ортогональной группы $O(E)$

считать $C = \begin{pmatrix} 1 & * \\ 0 & C' \end{pmatrix}$, где $1 = 1_{k_0}$ и второй блок имеет $k_{>0} = k_1 + k_2 + \dots$

столбцов. Теперь сравнение $E[C] \equiv \begin{pmatrix} -G_0 & 0 \\ 0 & 0 \end{pmatrix} (p)$ равносильно условиям

$$C = \begin{pmatrix} 1 & 0 \\ 0 & C' \end{pmatrix}, \quad C' = (C_1 | C_2 | \dots), \quad e[C'] \equiv 0(p).$$

Пусть блок $C' / \text{mod } p$ имеет ранг $r_p(C') = r = r_{>0}$. Снова по теореме Витта, после замены $C' \mapsto UC' / \text{mod } p$ с $U \in O(e)$, можем предположить

$$E = -G_0 \oplus J(r) \oplus e,$$

где $J(r) = \begin{pmatrix} 0 & 1_r \\ 1_r & 0 \end{pmatrix}$ – гиперболическая форма размерности $2r$ и $C' = \begin{pmatrix} C^r \\ 0 \end{pmatrix}$ с блоком $C^r = (C_1 | C_2 | \dots)$ высоты r и ранга $r_p(C^r) = r$. Из последнего сравнения для C следует, что блок C^r может быть любым по $\text{mod } p$ с условием $r_p(C^r) = r$. Для любых u из полной линейной группы $\text{GL}_r = \text{GL}_r(\mathbb{Z}_p)$ матрицы $U = \text{diag}(u, {}^t u^{-1})$ принадлежат ортогональной группе $O(J(r))$ и $U \begin{pmatrix} C^r \\ 0 \end{pmatrix} = \begin{pmatrix} u C^r \\ 0 \end{pmatrix}$.

Теперь задача об орбитах $\{C\}$ п. 2.2 свелась к орбитам $\langle C^r \rangle$ вида $u C^r V / \text{mod } p$, где $u \in \text{GL}_r$, $V \in O(G_{>0})$ для формы $G_{>0} = \bigoplus_{\alpha>0} G_\alpha$. Ранг $r_p(C^r) = r$ является инвариантом орбиты $\langle C^r \rangle$. Пусть $C^r = (C_1 | \dots | C_\alpha | \dots | 0)$, где $r_p(C_\alpha) = r_\alpha > 0$ для максимального номера $\alpha = \alpha_1$. Заменяя $C_\alpha \mapsto u C_\alpha / \text{mod } p$ с $u \in \text{GL}_r$, получаем $C_\alpha = \begin{pmatrix} 0 \\ C'_\alpha \end{pmatrix}$ с блоком C'_α высоты $r_\alpha = r_p(C'_\alpha)$. Итак, орбита $\langle C^r \rangle$ содержит матрицу вида

$$C^r = \left(\dots \left| \begin{matrix} C''_\beta \\ C'_\beta \end{matrix} \right| \dots \left| \begin{matrix} 0 \\ C'_\alpha \end{matrix} \right| \dots \left| \begin{matrix} 0 \\ 0 \end{matrix} \right| \right).$$

У матрицы $V = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ из ортогональной группы $O\left(\begin{pmatrix} G_\beta & 0 \\ 0 & G_\alpha \end{pmatrix}\right)$, $\beta < \alpha$, можно взять любые блоки: $C \in M(\mathbb{Z}_p)$, $A \in O(G_{p^\beta} / \text{mod } p)$, $D \in O(G_{p^\alpha} / \text{mod } p)$, а блок $B \equiv 0(p)$ определяется выбранными C, A, D единственным образом. Имеем

$$\left(\begin{matrix} C''_\beta & 0 \\ C'_\beta & C'_\alpha \end{matrix} \right) V \equiv \left(\begin{matrix} C''_\beta A & 0 \\ C'_\beta A + C'_\alpha C & C'_\alpha D \end{matrix} \right) \pmod{p}, \quad (2.3)$$

где $r_p(C'_\alpha D) = r_\alpha$, и мы хотим добиться выполнения сравнения

$$C'_\beta A + C'_\alpha C \equiv 0(p).$$

Выберем $V \equiv \begin{pmatrix} 1 & 0 \\ C & 1 \end{pmatrix} (p)$, где блок C может быть любой целой матрицей. Так как столбцы матрицы C'_α содержат базис $\bmod p$ размерности r_α , то разрешимо сравнение $C'_\alpha C \equiv -C'_\beta (p)$. Поэтому можем считать $C'_\beta = 0$ для всех $\beta < \alpha$. Аналогично поступаем с блоком C''_{α_2} ранга $r_p(C''_{\alpha_2}) = r_{\alpha_2} > 0$ для максимального $\alpha_2 < \alpha_1$ и т.д. Получаем в орбите $\langle C^r \rangle$ матрицу вида

$$C^r = \left(\begin{array}{c|c|c|c|c|c|c} & C_{\alpha_s} & & 0 & & 0 & \\ \cdots & 0 & \cdots & C_{\alpha_2} & \cdots & 0 & \cdots \\ & 0 & & 0 & & C_{\alpha_1} & \end{array} \right), \quad (2.4)$$

$$\alpha_s < \cdots < \alpha_2 < \alpha_1,$$

где пустые места заполнены нулями, блоки C_{α_i} имеют размеры $r_{\alpha_i} \times k_{\alpha_i}$ и ранги $r_p(C_{\alpha_i}) = r_{\alpha_i}$, $i = 1, \dots, s$.

2.5. Пусть V – квадратичное пространство над полем $\mathbb{F}_p = \mathbb{Z}_p/p\mathbb{Z}_p$, $p \neq 2$, с билинейной формой $(\cdot, \cdot)$, и пусть $U = U_{\max}$ – максимальное невырожденное подпространство из V . Согласно (2.2) $V = U \oplus W$ с $W = U^\perp$. Если $U' = U'_{\max}$ – другое такое же подпространство, то проекция

$$\text{pr}: U' \xrightarrow{\sim} U \quad (2.5)$$

есть изометрия. Действительно, пусть $\{u'_i\}$ будет базисом U' и $u'_i = u_i + w_i$ с $u_i \in U$, $w_i \in W$. Тогда $\text{pr}(u'_i) = u_i$ и $(u'_i, u'_j) = (u_i, u_j) + (w_i, w_j)$. Если существует анизотропный вектор $w \in W$: $(w, w) \neq 0$, то определитель подпространства $U \oplus \{w\}$ будет $|U| \cdot (w, w) \neq 0$ и, значит, U не максимальное. Отсюда заключаем, что $W = W_{\text{isot}}$ есть изотропное подпространство V , т.е. $(w, w') = 0$ для любых $w, w' \in W$. Следовательно, $(u'_i, u'_j) = (u_i, u_j)$ и векторы $\{u_i\}$ линейно независимы. Поэтому $\dim U' \leq \dim U$, а по симметрии $\dim U' = \dim U$, и тогда проекция (2.5) – изометрия. В частности, размерность подпространства $U = U_{\max}$ есть инвариант квадратичного пространства V .

2.6. Если же V само является подпространством невырожденного пространства M , $|M| \neq 0$, то по (2.2) $M = U \oplus M_1$ и W содержится в $M_1 = U^\perp(M)$ – ортогональном дополнении U в M . Итак, имеем

$$W \subset M_1, \quad |M_1| \neq 0, \quad W = W_{\text{isot}}.$$

Возьмем вектор $w \neq 0$ из W , и пусть w ортогонален M_1 . Поднимем w до базиса $w, m_1, \dots, m_s$ пространства M_1 . Относительно этого базиса $|M_1| = 0$. Противоречие приводит к существованию вектора $w' \in M_1$, неортогонального к вектору w . Можем считать $(w, w') = 1$, и, следовательно, равенство

$$(w' + \lambda w, w' + \lambda w) = (w', w') + 2\lambda = 0$$

выполняется для $\lambda = -(w', w')/2$. После замены $w' \mapsto w' + \lambda w$ имеем $(w, w) = (w', w') = 0$, $(w, w') = 1$. Это означает, что $\{w, w'\}$ – гиперболическая плоскость с квадратичной формой $J(1) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, $|J(1)| = -1$. По индукции получаем разложение в ортогональную сумму $M_1 = \widetilde{W} \oplus \widetilde{W}^\perp$, где $\widetilde{W} = W + W'$ – гиперболическое подпространство (прямая неортогональная сумма) с формой $J(s) = \begin{pmatrix} 0 & 1_s \\ 1_s & 0 \end{pmatrix}$, где $s = \dim W$. Теперь, возвращаясь к подпространствам $V \subset M$, $|M| \neq 0$, $U = U_{\max} \subset V$, $|U| \neq 0$, получаем разложения

$$V = U \oplus W \subset M = [U \oplus (W + W')] \oplus M_1, \quad (2.6)$$

где подпространство $U = U_{\max}$ с точностью до изометрии определяется единственным образом.

2.7. Рассмотрим любой из $(r_\alpha \times k_\alpha)$ -блоков C_α (2.4) ранга $r_p(C_\alpha) = r_\alpha$. Когда u пробегает группу GL_{r_α} , строки с матриц $uC_\alpha / \bmod p$ дают все базисы некоторого r_α -мерного подпространства $V = V_\alpha$ квадратичного пространства $M = M_{1, k_\alpha}(\mathbb{F}_p)$ с формой $G_{p^\alpha}^{-1}[{}^t c] / \bmod p$. Согласно (2.6) максимальное невырожденное подпространство $U = U_{\max}$ из V с точностью до изометрии определяется единственным образом, т.е. однозначно определен класс ограничения квадратичной формы пространства V на подпространство U , для которого размерность r_α^ε и знак $\varepsilon = \pm 1$ – полная система инвариантов [3]. Тогда по (2.6) и размерность $r_\alpha^0 = r_\alpha - r_\alpha^\varepsilon$ изотропного подпространства $W = W_{\mathrm{isot}}$ из V – также инвариант. Поэтому орбита $\langle C_\alpha \rangle$ из матриц $uC_\alpha V / \bmod p$ с $u \in \mathrm{GL}_{r_\alpha}$, $V \in O(G_{p^\alpha})$ содержит представителя $C_\alpha = (1_{r_\alpha} 0)$, и по теореме Витта можем считать

$$G_{p^\alpha}^{-1} = (1_\alpha^\varepsilon)^{-1} \oplus J_\alpha \oplus g_\alpha^{-1},$$

т.е. $G_{p^\alpha} = 1_\alpha^\varepsilon \oplus J_\alpha \oplus g_\alpha$, где $r_\alpha = r_\alpha^\varepsilon + r_\alpha^0$, $1_\alpha^\varepsilon = 1(r_\alpha^\varepsilon)$ – некоторая целая фиксированная форма размерности $\dim 1_\alpha^\varepsilon = r_\alpha^\varepsilon$, определитель которой удовлетворяет условию $\left(\frac{|1_\alpha^\varepsilon|}{p}\right) = \varepsilon = \pm 1$ (здесь $\left(\frac{\cdot}{p}\right)$ – символ Лежандра, а ε – знак невырожденной формы 1_α^ε), $J_\alpha = J(r_\alpha^0)$ – гиперболическая форма размерности $2r_\alpha^0$. Числа r_α^ε , r_α^0 , ε есть инварианты орбиты $\langle C_\alpha \rangle$.

2.8. Соберем полученные результаты. Согласно пп. 2.4 и 2.7 в каждой орбите $\{C\}$ п. 2.2 решений сравнения $E[C] \equiv -G(p)$ ранга $r_p(C) = r_0 + r_{>0}$, $r_0 = k_0$, есть представитель вида

$$C = \left(\begin{array}{c|c} 1 & \\ \hline & C^r \\ & 0 \\ \hline & 0 \end{array} \right) \begin{array}{l} (k_0) \\ (r) \\ (r) \end{array}, \quad (2.7)$$

C^r – матрица (2.4) с $r = r_{>0}$ и блоками $C_\alpha = (1_{r_\alpha} 0)$, где $\alpha \geq 1$ и $\sum_{\alpha \geq 1} r_\alpha = r_{>0}$. При этом формы имеют разложения

$$E = -G_0 \oplus J(r) \oplus e, \quad G = \bigoplus_{\alpha} G_\alpha, \quad G_{p^\alpha} = 1_\alpha^\varepsilon \oplus J_\alpha \oplus g_\alpha, \quad \alpha \geq 1, \quad (2.8)$$

где $\dim 1_\alpha^\varepsilon = r_\alpha^\varepsilon$, $\dim J_\alpha = 2r_\alpha^0$ и $r_\alpha^\varepsilon + r_\alpha^0 = r_\alpha$. Теперь необходимо показать, что система $\{r_\alpha\} = \{r_\alpha^\varepsilon, r_\alpha^0, \varepsilon = \varepsilon_\alpha : \alpha \geq 1\}$ образует полную систему инвариантов орбит $\{C\}$ (1.14). Для этого потребуются дополнительные сведения об ортогональных преобразованиях над локальными кольцами.

§3. Ортогональные группы над локальными кольцами

Все группы определены над кольцом $\mathbb{Z}_p$, $p \neq 2$.

3.1. Пусть дана квадратичная форма $Q = q_1 E_1 \oplus \dots \oplus q_s E_s$ с невырожденными блоками $|E_i| \not\equiv 0(p)$, $q_i | q_{i+1}$ и $1 \leq q_1 < q_2 < \dots < q_s$. Для X из ортогональной группы $O(Q)$ условие $Q[X] = Q$ эквивалентно системе матричных равенств

$${}^t X_i Q X_j = \delta_{ij} q_i E_i, \quad X = (X_1 | \dots | X_s) = (x_{ij}). \quad (3.1)$$

Аналогично двублочному случаю п. 2.4 опишем блочную структуру общих ортогональных преобразований X . Начнем с ряда лемм.

ЛЕММА 3.1. Пусть для фиксированного $j \leq s$ блоки $x_{ij} \equiv 0(q_j/q_i)$ для всех $i < j$. Тогда блок x_{jj} принадлежит $O(E_j/q'_j)$ – ортогональной группе по $\bmod q'_j$, $q'_j = \min(q_j/q_{j-1}, q_{j+1}/q_j)$ для $1 < j < s$ и $q'_1 = q_2/q_1$, $q'_s = q_s/q_{s-1}$.

ДОКАЗАТЕЛЬСТВО. По (3.1) $Q[X_j] = \sum_i q_i E_i[x_{ij}] = q_j E_j$ и $q_i E_i[x_{ij}] \equiv 0(q_j^2/q_i)$ для $i < j$. Отсюда $E_j[x_{jj}] \equiv E_j(q'_j)$.

ЛЕММА 3.2. Если $X \in O(Q)$, то $x_{jj} \in O(E_j/q'_j)$ и $x_{ij} \equiv 0(q_j/q_i)$ для $1 \leq i < j \leq s$.

ДОКАЗАТЕЛЬСТВО. По лемме 3.1 $x_{11} \in O(E_1/q'_1)$ и для $(i, j) = (1, 2)$ ввиду (3.1) ${}^t X_1 Q X_2 \equiv {}^t x_{11} q_1 E_1 x_{12} \equiv 0(q_2)$, откуда $x_{12} \equiv 0(q_2/q_1)$ и по лемме 3.1 $x_{22} \in O(E_2/q'_2)$. Переходим к блоку X_3 . Из (3.1) для $(i, j) = (1, 3)$ следует $x_{13} \equiv 0(q_2/q_1)$, а для $(i, j) = (2, 3)$ следует $x_{23} \equiv 0(q'_2)$. Возвращаемся к $(i, j) = (1, 3)$ и получаем более сильное сравнение $x_{13} \equiv 0(q_2^2/q_1^2, q_3/q_1)$. Теперь из (3.1) для $(i, j) = (2, 3)$ вытекает также более сильное сравнение $x_{23} \equiv 0(q_2^2/q_1^2, q_3/q_2)$. Двигаясь по циклу $(1, 3) \rightarrow (2, 3) \rightarrow (1, 3) \rightarrow \dots$, получаем требуемое сравнение для блоков x_{13} , x_{23} и затем по лемме 3.1 получаем $x_{33} \in O(E_3/q'_3)$. Для блока X_4 схема доказательства такова: $(1, 4) \rightarrow (2, 4) \rightarrow (3, 4) \rightarrow (1, 4) \rightarrow \dots$. После этого шага становится понятной схема для оставшихся блоков X_j , $4 < j \leq s$.

3.2. Приведем еще один результат из [2, с. 80].

ЛЕММА 3.3. Пусть $q = p^\alpha$, $\alpha \geq 1$, $E \equiv E' \equiv E''(q)$ – целые невырожденные по $\bmod p$ формы и R – целая матрица размерности m . Тогда любое $\bar{x} \in O(E/q)$ поднимается до $x \equiv \bar{x}(q)$, $x \in \mathbb{Z}_p^m$ – решения матричного уравнения $E'[x] + q(Rx)^s = E''$, где $(Rx)^s = Rx + {}^t x^t R$. Таких $x / \bmod p^r q$, когда $\bar{x}$ фиксировано, будет $p^{(r-1)\langle m \rangle}$ с $\langle m \rangle = m(m-1)/2$, и, значит, сравнение $E'[x] + q(Rx)^s \equiv E''(p^r q)$ имеет $p^{(r-1)\langle m \rangle} o(E/q)$ решений, где $o(E/q) = |O(E/q)|$ – порядок ортогональной группы $O(E/q)$.

3.3. Переходим к описанию блоков для ортогональных матриц X . В столбце $X_1 = (x_{i1})$ выбираем произвольными блоки с $i \geq 2$. Из равенства $Q[X_1] = q_1 E_1$ (3.1) следует $E_1[x_{11}] \equiv E_1(q'_1)$, а по лемме 3.3 любое $\bar{x}_{11} \in O(E_1/q'_1)$ поднимается ($x_{11} \equiv \bar{x}_{11}(q'_1)$) до решения $x_{11} \in M(\mathbb{Z}_p)$ матричного уравнения $Q[X_1] = q_1 E_1$ с прежними блоками x_{i1} , $i \geq 2$.

В следующем столбце $X_2 = (x_{i2})$ берем произвольными блоки для $i \geq 3$. Из равенства (3.1) для $(i, j) = (1, 2)$ следует $x_{12} = (q_2/q_1)x'_{12}$ с целыми $x'_{12} = A_{12}x_{22} + B_{12}$. Подставляем x_{12} в равенство $Q[X_2] = q_2 E_2$ (3.1). По лемме 3.1 $E_2[x_{22}] \equiv E_2(q'_2)$, и, следовательно, последнее равенство имеет вид равенства из леммы 3.3. Это означает, что любое $\bar{x}_{22} \in O(E_2/q'_2)$ поднимается ($x_{22} \equiv \bar{x}_{22}(q'_2)$) до решения $x_{22} \in M(\mathbb{Z}_p)$ уравнения $Q[X_2] = q_2 E_2$. После этого находим x_{12} .

Переходим к описанию столбца $X_3 = (x_{i3}) = \begin{pmatrix} Y_3 \\ Z_3 \end{pmatrix}$, где $Y_3 = \begin{pmatrix} x_{13} \\ x_{23} \end{pmatrix}$ и блоки x_{i3} , $i \geq 4$, произвольны. Согласно (3.1) записываем

$${}^t(X_1 X_2) Q X_3 = 0, \quad X_1 X_2 = \begin{pmatrix} x_{11} & x_{12} \\ x_{21} & x_{22} \\ * & * \end{pmatrix} = \begin{pmatrix} Y_{12} \\ Z_{12} \end{pmatrix}, \quad |Y_{12}| \not\equiv 0(p),$$

т.е.

$${}^t Y_{12} \begin{pmatrix} q_1 E_1 & 0 \\ 0 & q_2 E_2 \end{pmatrix} Y_3 + {}^t Z_{12} \begin{pmatrix} q_3 E_3 & & \\ & \ddots & \\ & & q_s E_s \end{pmatrix} Z_3 = 0. \quad (3.2)$$

Здесь $Y_3 = \begin{pmatrix} q_3/q_1 & 0 \\ 0 & q_3/q_2 \end{pmatrix} Y'_3$ с целым $Y'_3 = \begin{pmatrix} x'_{13} \\ x'_{23} \end{pmatrix}$. Подставляя его в (3.2), получаем $Y'_3 = A Z_3$, или, в другой записи, $x'_{13} = A_{13}x_{33} + B_{13}$, $x'_{23} = A_{23}x_{33} + B_{23}$. Теперь подставляем эти значения в равенство (3.1) $Q[X_3] = q_3 E_3$ и вспоминаем, что по лемме 3.1 $E_3[x_{33}] \equiv E_3(q'_3)$. Приходим к равенству из леммы 3.3 для $q = q'_3$. Следовательно, любое $\bar{x}_{33} \in O(E_3/q'_3)$ поднимается до $x_{33} \equiv \bar{x}_{33}(q'_3)$ – решения $x_{33} \in M(\mathbb{Z}_p)$ уравнения $Q[X_3] = q_3 E_3$. Затем по нему находим блоки x_{13} , x_{23} и, таким образом, весь столбец X_3 построен.

Оставшиеся столбцы $X_4, \dots, X_s$ строим аналогично. Итак, доказано

ПРЕДЛОЖЕНИЕ 3.1. Любое преобразование $X = (x_{ij})$ из ортогональной группы $O(Q)$ над кольцом $\mathbb{Z}_p$, $p \neq 2$, может быть построено по следующей схеме:

- 1) нижнедиагональные блоки x_{ij} , $i > j$, выбираем произвольными;
- 2) диагональные блоки x_{jj} , $1 \leq j \leq s$, получаем подъемом $x_{jj} \equiv \bar{x}_{jj}(q'_j)$ произвольно выбранных элементов $\bar{x}_{jj} \in O(E_j/q'_j)$; полученные блоки x_{jj} зависят от ранее выбранных блоков x_{ij} , $i > j$;
- 3) верхнедиагональные блоки x_{ij} , $i < j$, удовлетворяют сравнениям $x_{ij} \equiv 0(q_j/q_i)$ и определяются единственным образом предыдущими блоками x_{ij} , $i \geq j$.

СЛЕДСТВИЕ 3.1. Для любого ортогонального преобразования

$$X = \begin{pmatrix} x_{11} & * \\ * & X_{22} \end{pmatrix}$$

из группы $O(Q)$ существует преобразование $X' = (x'_{ij})$, $2 \leq i, j \leq s$, из группы $O(Q_{>1})$ для $Q_{>1} = q_2 E_2 \oplus \dots \oplus q_s E_s$, удовлетворяющие сравнениям: $x'_{jj} \equiv x_{jj}(q'_j)$ для $2 \leq j \leq s$ и $x'_{ij} \equiv 0(q_j/q_i)$ для $i < j$, и, следовательно, выполняется общее сравнение

$$X' \equiv X_{22} \left(\min_{1 \leq i \leq s-1} q_{i+1}/q_i \right).$$

ДОКАЗАТЕЛЬСТВО. По предложению 3.1, 1) можем нижнедиагональные блоки x_{ij} , $i > j \geq 2$, для X' взять такими же, как у X , а по 3) для любого X' его верхнедиагональные блоки всегда удовлетворяют указанным сравнениям. По определению из леммы 3.1 модули q'_j , $2 \leq j \leq s$, для формы Q не превосходят соответствующих модулей меньшей формы $Q_{>1}$. Отсюда и из 2) получаем сравнения для диагональных блоков.

§ 4. Инварианты $\{r_\alpha\}$

Покажем, что определенное в п. 2.8 множество $\{r_\alpha\}$ образует полную систему инвариантов орбит $\{C\}$ решений сравнения $E[C] \equiv -G \pmod{p}$, т.е. $\{r_\alpha\}$

- 1) являются инвариантами орбит;
- 2) разделяют указанные орбиты.

Более того, $\{r_\alpha\}$ будут параметрами, ограниченными лишь условием существования квадратичных форм (2.8).

4.1. Для любой матрицы $U = (U_{ij})$, $1 \leq i, j \leq 4$, из ортогональной группы $O(E)$ с разделением на блоки, аналогичным разбиению формы E (2.8), и для представителя C_1 из орбиты $\{C\}$ (2.7) вида $C_1 = UC$ имеем совпадение рангов $r_p(C_1) = r_p(C)$. Поэтому согласно п. 2.4 можем считать $C_1 = \begin{pmatrix} 1 & 0 \\ 0 & C' \end{pmatrix}$, где $1 = 1_{k_0}$, $C' = \begin{pmatrix} C_1^r \\ 0 \end{pmatrix}$ и C_1^r – блок высоты и ранга $r = r_{>0}$. Пусть $V = \begin{pmatrix} V_{11} & V_{12} \\ V_{21} & V_{22} \end{pmatrix}$ будет матрицей из ортогональной группы $O(G)$ формы $G = \begin{pmatrix} G_0 & 0 \\ 0 & G_{>0} \end{pmatrix}$ (2.8). Согласно предложению 3.1, 3) имеем сравнение

$$C_1 V \equiv \begin{pmatrix} V_{11} & 0 \\ C_1^r V_{21} & C_1^r V_{22} \\ 0 & 0 \end{pmatrix} \pmod{p}.$$

По условию $C_1 \in \{C\}$, поэтому $UC \equiv C_1 V(p)$ для некоторых $U \in O(E)$ и $V \in O(G)$. Из сравнения $U_{ij} C^r \equiv 0(p)$ и условия $r_p(C^r) = r$ вытекает сравнение $U_{ij} \equiv 0(p)$. Следовательно, можем записать

$$U = (U_1 U_2 U_3 U_4) \text{ с блоком } (U_1 U_2) = \begin{pmatrix} U_{11} & 0 \\ U_{21} & U_{22} \\ 0 & 0 \end{pmatrix}.$$

Так как $E[U] = E$ и форма E имеет вид (2.8), то ${}^tU_2 EU_3 \equiv {}^tU_{22} U_{33} \equiv 1_r \pmod{p}$ и, значит, $|U_{22}| \not\equiv 0(p)$. Возвращаясь к сравнению $UC \equiv C_1 V(p)$, выводим для блоков C^r , C_1^r сравнение $U_{22} C^r \equiv C_1^r V_{22}(p)$ с $|U_{22}| \not\equiv 0(p)$. По следствию 3.1 существует ортогональное преобразование V'_{22} из группы $O(G_{>0})$ с условием $V'_{22} \equiv V_{22}(p)$. Из этих двух сравнений вытекает следующее утверждение. Если матрица C_1 принадлежит орбите $\{C\}$ (2.7), то ее блок C_1^r принадлежит орбите $\langle C^r \rangle$ п. 2.4.

4.2. Пусть $C^r = (\dots |C_s| \dots |C_2| \dots |C_1| \dots)$ – матрица (2.3), у которой в отмеченных столбцах стоят блоки $C_\alpha = (1_{r_\alpha} 0)$ (2.7). Берем произвольные $U \in \text{GL}(\mathbb{Z}_p)$ и $V \in O(G_{>0})$. По предложению 3.1 записываем

$$V \equiv \begin{pmatrix} \ddots & & & * \\ & x_s & & \\ & & \ddots & \\ & & & x_1 \\ * & & & \ddots \end{pmatrix} \pmod{p}$$

для некоторых $x_i \in O(G_{p^{\alpha_i}}/p)$. Покажем, что блок C_1^r имеет те же параметры $\{r_\alpha\}$, что и блок C^r .

Шаг 1. Из сравнения для V получаем сравнение

$$UC^r V \equiv (\dots |UC_1 x_1| 0 \dots 0) \pmod{p},$$

доказывающее, что орбита $\langle C_1 \rangle$ из матриц $UC_1 x_1 / \text{mod } p$, где $U \in \text{GL}(\mathbb{Z}_p)$, $x_1 \in O(G_{p^{\alpha_1}})$, есть инвариант, а поэтому и $\text{rang } r_p(C_1) = r_{\alpha_1}$ – тоже инвариант. Выберем матрицу $U = \begin{pmatrix} U_1 & U_2 \\ U_3 & U_4 \end{pmatrix}$ с условием $UC_1 x_1 \equiv \begin{pmatrix} 0 \\ * \end{pmatrix} \pmod{p}$, где ненулевой блок имеет высоту r_{α_1} . Отсюда и из сравнения

$$UC_1 x_1 \equiv \begin{pmatrix} U_2 C_{\alpha_1} x_1 \\ U_4 C_{\alpha_1} x_1 \end{pmatrix} (p)$$

выводим $U_2 C_{\alpha_1} x_1 \equiv 0 \pmod{p}$, а ввиду условий $|x_1| \not\equiv 0(p)$, $r_p(C_{\alpha_1}) = r_{\alpha_1}$ заключаем, что $U_2 \equiv 0(p)$, $|U_1|, |U_4| \not\equiv 0(p)$. Отображение $C_{\alpha_1} \mapsto U_4 C_{\alpha_1} x_1$ показывает, что орбита $\langle C^r \rangle$ однозначно определяет орбиту $\langle C_{\alpha_1} \rangle$ из матриц, стоящих слева, а тогда в силу п. 2.7 $r_{\alpha_1}^\varepsilon, r_{\alpha_1}^0, \varepsilon = \varepsilon_{\alpha_1}$ будут инвариантами.

ШАГ 2. Имеем

$$\begin{aligned}
 UC^rV &\equiv \begin{pmatrix} U_1 & 0 \\ U_3 & U_4 \end{pmatrix} \left(\begin{array}{c|c|c|c} \cdots & & & \\ \hline & C_2 & \cdots & 0 \\ \hline 0 & 0 & & C_{\alpha_1} \end{array} \right) \\
 &\quad \times \begin{pmatrix} \ddots & & & 0 \\ & x_2 & & \\ & & \ddots & \\ & & & x_1 \\ * & & & \ddots \end{pmatrix} \\
 &\equiv \left(\begin{array}{c|c|c|c} & U_1C_2x_2 & \cdots & 0 \\ \hline & * & * & U_4C_{\alpha_1}x_1 \end{array} \right) \pmod{p}.
 \end{aligned}$$

Тогда ввиду сравнения (2.3) α_2 – инвариант, орбита $\langle C_2 \rangle$ и затем $\langle C_{\alpha_2} \rangle$ – инварианты, а согласно п. 2.7 будут инвариантами $r_{\alpha_2}^\varepsilon, r_{\alpha_2}^0$, $\varepsilon = \varepsilon_{\alpha_2}$.

По индукции получаем

ПРЕДЛОЖЕНИЕ 4.1. *Совокупность $\{r_\alpha\} = \{r_\alpha^\varepsilon, r_\alpha^0, \varepsilon = \varepsilon_\alpha : \alpha \geq 1\}$ п. 2.8 образует полную систему инвариантов орбит $\{C\}$ п. 2.2 решений матричного сравнения $E[C] \equiv -G \pmod{p}$, ограниченную лишь неравенствами*

$$-G_0 \oplus J(r) \leq E, \quad 1_\alpha^\varepsilon \oplus J_\alpha \leq G_{p^\alpha}, \quad \alpha \geq 1. \quad (4.1)$$

Здесь неравенство форм $X \leq Y$ означает, что $Y \sim X \oplus Z$ для некоторой формы Z , т.е. это – неравенство классов $\{X\} \leq \{Y\}$.

§ 5. Расширения форм

Переходим к расширениям $Q_G^A(C)$, полученным сплением квадратичных форм A и G матрицами C . Класс расширения $\{Q_G^A(C)\}$ не зависит от выбора представителя C из орбиты $\{C\}$. Удобно брать канонические матрицы C (2.7) и использовать инварианты $\{r_\alpha\}$ для описания классов расширений.

5.1. Пусть C – сцепляющая матрица (2.7) для квадратичной формы $E = aA^{-1}$ и формы G с разложением (2.8). Так как $E[C] = \begin{pmatrix} -G_0 & 0 \\ 0 & 0 \end{pmatrix}$, то форма Q' п. 1.3 принимает вид

$$Q' = \frac{1}{a}(E[C] + G) = \begin{pmatrix} 0 & 0 \\ 0 & \frac{1}{a}G_{>0} \end{pmatrix},$$

а расширение $Q_G^A(C)$ (1.4) распадается в ортогональную сумму

$$Q_G^A(C) = Q(r_0^{\varepsilon_0}) \oplus ae^{-1} \oplus Q(r_{>0}) \quad (5.1)$$

форм

$$Q(r_0^{\varepsilon_0}) = \begin{pmatrix} -aG_0^{-1} & 1 \\ 1 & 0 \end{pmatrix}, \quad Q(r_{>0}) = \left(\begin{array}{c|c} aJ(r) & C^r \\ \hline {}^t C^r & 0 \end{array} \middle| \begin{array}{c} C^r \\ 0 \\ \hline \frac{1}{a}G_{>0} \end{array} \right),$$

где $r = r_{>0}$. Если начальный блок G_0 размера $r_0 = k_0$ и знака ε_0 привести к диагональному виду

$$G_0 = 1_{r_0}^{\varepsilon_0} = \bigoplus_{1 \leq j \leq r_0} 1^{\varepsilon_j},$$

где $\prod_j \varepsilon_j = \varepsilon_0$ и 1^{ε_j} – произвольные единицы кольца $\mathbb{Z}_p$ со знаками ε_j , то

$$Q(r_0^{\varepsilon_0}) = \bigoplus_{1 \leq j \leq r_0} Q(1_0^{\varepsilon_j})$$

и слагаемые $Q(1_0^{\varepsilon_j})$ – бинарные формы вида

$$Q(1_0^{\varepsilon}) = \begin{pmatrix} -a \cdot 1^{\varepsilon} & 1 \\ 1 & 0 \end{pmatrix} \sim J(1). \quad (5.2)$$

Следовательно, $Q(r_0^{\varepsilon_0}) \sim J(r_0)$. Конечно, это можно было доказать и непосредственно, вычисляя определитель $|Q(r_0^{\varepsilon_0})|$, но для нас важно было отметить разложение формы $Q(r_0^{\varepsilon_0})$ в сумму бинарных форм (5.2).

5.2. Для вычисления инвариантов формы $Q(r_{>0})$ воспользуемся видом матрицы C^r (2.4) и разложениями (2.8) формы $G_{>0} = \bigoplus_{\alpha > 0} G_{\alpha}$. Прежде всего заметим, что форма $Q(r_{>0})$ разлагается в ортогональную сумму:

$$Q(r_{>0}) = Q_1(r_{>0}) \bigoplus_{\substack{\alpha > 0 \\ \alpha \neq \alpha_i}} \frac{1}{a} G_{\alpha},$$

при этом форма $Q_1(r_{>0})$ в свою очередь разлагается в сумму:

$$Q_1(r_{>0}) = \bigoplus_{\alpha_i} Q(r_{\alpha_i}), \quad Q(r_{\alpha}) = Q_1(r_{\alpha}^{\varepsilon}) \oplus Q(r_{\alpha}^0) \oplus \frac{p^{\alpha}}{a} g_{\alpha},$$

форм

$$Q(r_{\alpha}^{\varepsilon}) = \left(\begin{array}{c|c} aJ(r_{\alpha}^{\varepsilon}) & 1 \\ \hline 1 & 0 \end{array} \middle| \begin{array}{c} 0 \\ \hline \frac{p^{\alpha}}{a} \cdot 1^{\varepsilon} \end{array} \right), \quad Q(r_{\alpha}^0) = \left(\begin{array}{c|c} aJ(r_{\alpha}^0) & 1 & 0 \\ \hline 1 & 0 & 0 \\ \hline 0 & 0 & \frac{p^{\alpha}}{a} J(r_{\alpha}^0) \end{array} \right),$$

где $J(r_{\alpha}^{\varepsilon})$ и $J(r_{\alpha}^0)$ – гиперболические формы размеров $2r_{\alpha}^{\varepsilon}$ и $2r_{\alpha}^0$ соответственно, $1^{\varepsilon} = 1(r_{\alpha}^{\varepsilon})$ – форма размера r_{α}^{ε} и знака $\varepsilon = \varepsilon_{\alpha}$. Формы $Q(r_{\alpha}^{\varepsilon})$ и $Q(r_{\alpha}^0)$ допускают дальнейшие разложения:

$$Q(r_{\alpha}^{\varepsilon}) = \bigoplus_{1 \leq j \leq r_{\alpha}^{\varepsilon}} Q(1_{\alpha}^{\varepsilon_j}),$$

$Q(r_{\alpha}^0) = Q(1_{\alpha}^0) \oplus \dots \oplus Q(1_{\alpha}^0)$ – сумма из r_{α}^0 одинаковых форм $Q(1_{\alpha}^0)$. Слагаемые в этих разложениях – тернарные и кватернарные формы вида

$$Q(1_{\alpha}^{\varepsilon}) = \left(\begin{array}{c|c} aJ(1) & 1 \\ \hline 1 & 0 \end{array} \middle| \begin{array}{c} 0 \\ \hline \frac{p^{\alpha}}{a} \cdot 1^{\varepsilon} \end{array} \right), \quad Q(1_{\alpha}^0) = \left(\begin{array}{c|c} aJ(1) & 1 & 0 \\ \hline 1 & 0 & 0 \\ \hline 0 & 0 & \frac{p^{\alpha}}{a} J(1) \end{array} \right). \quad (5.3)$$

Знаки ε_j должны удовлетворять условию $\prod_j \varepsilon_j = \varepsilon$.

5.3. Вычислим инварианты форм $Q(1_\alpha^\varepsilon)$ и $Q(1_\alpha^0)$ с помощью следующего матричного аналога приведения квадратичных форм к диагональному виду над локальными кольцами $\mathbb{Z}_p$, $p \neq 2$ (ср. [4, с. 465]).

Пусть целая квадратичная форма Q разбита на блоки:

$$Q = \begin{pmatrix} A & C & C_1 \\ {}^tC & Q_1 & C_2 \\ {}^tC_1 & {}^tC_2 & Q_2 \end{pmatrix},$$

и квадратный блок Q_1 имеет определитель $|Q_1| \not\equiv 0(p)$. В качестве приводящей матрицы M возьмем целую матрицу

$$M = \begin{pmatrix} 1 & 0 & 0 \\ -Q_1^{-1} \cdot {}^tC & 1 & -Q_1^{-1} \cdot C_2 \\ 0 & 0 & 1 \end{pmatrix}$$

с определителем $|M| = 1$. Тогда исходная форма Q эквивалентна над кольцом $\mathbb{Z}_p$ распадающейся в ортогональную сумму форме $Q[M] = {}^tM Q M$. После перемножения матриц получаем

$$Q \sim Q_1 \oplus \begin{pmatrix} \tilde{A} & \tilde{C}_1 \\ {}^t\tilde{C}_1 & \tilde{Q} \end{pmatrix}, \quad (5.4)$$

и блоки $\tilde{A}$, $\tilde{C}_1$, $\tilde{Q}$ вычисляются по формулам

$$\tilde{A} = A - Q_1^{-1}[{}^tC], \quad \tilde{C}_1 = C_1 - C Q_1^{-1} C_2, \quad \tilde{Q} = Q_2 - Q_1^{-1}[C_2].$$

5.4. Поменяем местами вторые и третьи строки и столбцы у формы $Q(1_\alpha^\varepsilon)$. Имеем

$$Q(1_\alpha^\varepsilon) \sim \left(\begin{array}{cc|c} 0 & 1 & a \\ 1 & \frac{p^\alpha}{a} \cdot 1^\varepsilon & 0 \\ a & 0 & 0 \end{array} \right) = \begin{pmatrix} Q_1 & C_2 \\ {}^tC_2 & Q_2 \end{pmatrix}, \quad Q_1 \sim J(1).$$

По формуле (5.4) $Q(1_\alpha^\varepsilon) \sim Q_1 \oplus -Q_1^{-1}[C_2]$, что для тернарных форм дает требуемое разложение

$$Q(1_\alpha^\varepsilon) \sim J(1) \oplus ap^\alpha \cdot 1^\varepsilon, \quad \alpha \geq 1, \quad (5.5)$$

где 1^ε – любая единица кольца $\mathbb{Z}_p$ с условием $(\frac{1^\varepsilon}{p}) = \varepsilon$.

В форме $Q(1_\alpha^0)$ также поменяем местами вторые и третьи строки и столбцы:

$$Q(1_\alpha^0) \sim \left(\begin{array}{cc|cc} & & a & 0 \\ J(1) & & 0 & p^\alpha/a \\ a & 0 & 0 & 0 \\ 0 & p^\alpha/a & 0 & 0 \end{array} \right) = \begin{pmatrix} Q_1 & C_2 \\ {}^tC_2 & Q_2 \end{pmatrix}.$$

Применяя формулу (5.4), находим для этих кватернарных форм инварианты

$$Q(1_\alpha^0) \sim J(1) \oplus p^\alpha J(1), \quad \alpha \geq 1. \quad (5.6)$$

5.5. Вычисления пп. 5.1–5.4 позволяют явно записать расширения $Q_G^A(C)$ для сцепляющих матриц C из орбиты $\{C\}$ в терминах ее параметров $\{r_\alpha\}$. Введем дополнительные обозначения.

Возвращаемся к квадратичным формам A общего вида $A = A_0 \oplus A_1$ (см. п. 2.1) с блоком $A_1 = pA_p = aE^{-1}$. Из формулы (2.8) следует

$$A = -aG_0^{-1} \oplus aJ(r_{>0}) \oplus A_0 \oplus ae^{-1}, \quad G_0^{-1} = 1(r_0^{\varepsilon_0}).$$

Расширим систему параметров $\{r_\alpha\}$, добавив к ней r_0, ε_0 , и тогда можем записать

$$A = A(\{r_\alpha\}) \oplus A_0 \oplus ae^{-1}, \quad A(\{r_\alpha\}) = -a \cdot 1(r_0^{\varepsilon_0}) \oplus aJ(r_{>0}). \quad (5.7)$$

Чтобы аналогично записать расширения $Q_G^A(C)$, введем следующие обозначения:

$$\begin{aligned} Q(\{r_\alpha\}) &= J(r_0) \bigoplus_{\alpha_i > 0} (J(r_{\alpha_i}) \oplus ap^{\alpha_i} \cdot 1(r_{\alpha_i}^{\varepsilon_i}) \oplus p^i J(r_{\alpha_i}^0)), \\ Q^A(\{r_\alpha\}) &= Q(\{r_\alpha\}) \oplus A_0 \oplus ae^{-1} = Q(\{r_\alpha\}) \oplus (A \ominus A(\{r_\alpha\})), \\ Q_G^A(\{r_\alpha\}) &= Q^A(\{r_\alpha\}) \bigoplus_{\alpha_i > 0} \frac{p^{\alpha_i}}{a} g_{\alpha_i} \bigoplus_{\substack{\alpha > 0 \\ \alpha \neq \alpha_i}} \frac{1}{a} G_\alpha. \end{aligned} \quad (5.8)$$

Связи форм A и G с параметрами $\{r_\alpha\}$ симметричны: так, согласно формулам (2.8)

$$G = G(\{r_\alpha\}) \bigoplus_{\alpha_i > 0} p^{\alpha_i} g_{\alpha_i} \bigoplus_{\substack{\alpha > 0 \\ \alpha \neq \alpha_i}} G_\alpha, \quad (5.9)$$

где

$$G(\{r_\alpha\}) = 1(r_0^{\varepsilon_0}) \oplus p^{\alpha_i} (1(r_{\alpha_i}^{\varepsilon_i}) \oplus J(r_{\alpha_i}^0)).$$

Отсюда следует, что форма

$$\begin{aligned} Q_G^A(\{r_\alpha\}) &= Q^A(\{r_\alpha\}) \oplus \frac{1}{a} (G \ominus G(\{r_\alpha\})) \\ &= Q(\{r_\alpha\}) \oplus (A \ominus A(\{r_\alpha\})) \oplus \frac{1}{a} (G \ominus G(\{r_\alpha\})) \end{aligned} \quad (5.10)$$

выражается через исходные формы A, G и параметры $\{r_\alpha\}$. Причем формула (5.10) также определяет область (4.1) допустимых значений параметров $\{r_\alpha\}$: разности форм из (5.10) существуют тогда и только тогда, когда выполнены неравенства (4.1).

Ясно, что отображение

$$C / \text{mod } A_1 \xrightarrow{\sim} C' = \begin{pmatrix} 0 \\ C \end{pmatrix} / \text{mod } A \quad (5.11)$$

задает биекцию между классами решений сравнений $E[C] \equiv -G \pmod{p}$ и

$$aA^{-1}[C'] \equiv -G \pmod{p},$$

и при этом согласно п. 2.1 расширения для C и C' связаны соотношением

$$Q_G^A(C') = A_0 \oplus Q_G^{A_1}(C).$$

ЛЕММА 5.1. Если C – решение сравнения $E[C] \equiv -G \pmod{p}$ и его орбита $\{C\}$ согласно предложению 4.1 имеет инварианты $\{r_\alpha\}$, то расширение $Q_G^A(C')$ эквивалентно форме $Q_G^A(\{r_\alpha\})$ (5.10).

ДОКАЗАТЕЛЬСТВО вытекает из (5.10) и формул пп. 5.1–5.4.

5.6. Теперь у нас есть все необходимое, чтобы сформулировать основной результат об орбитах $\{b\}$ (1.14) целых примитивных представлений $b : Q[b] = A$ формы $A = A_0 \oplus A_1$ формой Q . Множество всех примитивных представлений $\text{pb}_{Q,A}$ разбивается на классы $\text{pb}_{Q,A}(\{G\})$ относительно отображения $[Q, A] : b \mapsto \{G\}$ п. 1.4. Зададим биекцию $\{b\} \xrightarrow{\sim} \{r_\alpha\}$ коммутативной диаграммой

$$\begin{array}{ccc} \text{pb}_{Q,A}(\{G\}) \supset \{b\} & \xrightarrow{\sim} & \{C\} \subset C_G^A(Q) \\ & \searrow & \swarrow \\ & \{r_\alpha\} & \end{array}$$

где горизонтальная стрелка есть композиция отображений (1.15) и (5.11), правая стрелка определена в предложении 4.1. Параметры $\{r_\alpha\}$ удовлетворяют условию $Q_G^A(\{r_\alpha\}) = Q$ (здесь и далее равенство квадратичных форм означает равенство их классов), эквивалентному в силу (5.10) и леммы 5.1 условиям

$$\begin{aligned} G_{>0} &= G_{>0}(\{r_\alpha\}) \oplus a\{Q \ominus [Q(\{r_\alpha\}) \oplus (A \ominus A(\{r_\alpha\}))]\}, \\ G_0 &= 1(r_0^{\varepsilon_0}), \end{aligned} \quad (5.12)$$

определяющим однозначно класс $\{G\}$. Отсюда вытекает основная

ТЕОРЕМА 5.1. Пусть $A = A_0 \oplus pA_p$ и Q – невырожденные целые над кольцом $\mathbb{Z}_p$, $p \neq 2$, формы размерностей m и n , и пусть $1 \leq m < n$. Тогда справедливы следующие утверждения:

1) множество целых примитивных представлений $\text{pb}_{Q,A}(\{G\})$ непустое тогда и только тогда, когда система равенств (5.12) имеет решения $\{r_\alpha\}$, т.е. все классы $\{G\}$ с непустым множеством $\text{pb}_{Q,A}(\{G\})$, и только такие классы определяются равенствами (5.12);

2) с помощью диаграммы орбиты $\{b\}$ (1.14) представлений b из множества $\text{pb}_{Q,A}(\{G\})$ параметризуются решениями $\{r_\alpha\}$ системы равенств (5.12);

3) число орбит $\{b\}$ (1.14) целых примитивных представлений $b : Q[b] = A$ равно числу решений $\{r_\alpha\}$ неравенства (см. п. 4.2)

$$Q^A(\{r_\alpha\}) = Q(\{r_\alpha\}) \oplus (A \ominus A(\{r_\alpha\})) \leq Q. \quad (5.13)$$

§ 6. Разложение вложений решеток

Перейдем на более инвариантный бескоординатный язык решеток и получим геометрическое описание представлений форм формой.

6.1. Решеткой L над кольцом $\mathbb{Z}_p$ называется свободный $\mathbb{Z}_p$ -модуль конечного ранга с невырожденной симметрической билинейной формой $(\cdot, \cdot)_L$, принимающей целые значения, т.е. значения из $\mathbb{Z}_p$. Если в L выбрать базис и записать его в виде строки $e = (e_1, \dots, e_n)$, то $Q = {}^t e \cdot e = ((e_i, e_j))$ – целая невырожденная матрица Грама решетки L или матрица квадратичной формы в базисе e . Если же $e' = eU$ – другой базис L , то U – целая матрица с определителем из группы единиц $\mathbb{Z}_p$, и матрица Грама $Q' = {}^t e' \cdot e' = Q[U]$ эквивалентна Q . Отождествляя изоморфные решетки, получаем биекцию $L \xrightarrow{\sim} \{Q\}$.

6.2. Вложение $i: M \hookrightarrow L$ решетки M размерности $1 \leq m \leq n$ в L – это вложение $\mathbb{Z}_p$ -модуля M в L с условием $(x', y')_M = (i(x'), i(y'))_L$. Пусть e' – некоторый базис решетки M и $A = {}^t e' \cdot e'$ – его матрица Грама. Тогда $i e' = e \cdot b$, b – целая однозначно определяемая $(n \times m)$ -матрица, и в силу сохранения билинейной формы имеем $Q[b] = A$. Будем записывать $b: A \hookrightarrow Q$ и говорить, что квадратичная форма A вложена в форму Q . Обратно, любое вложение b формы A в Q задает вложение $i: i e' = e \cdot b$ решетки M в L . Таким образом, вложениям решеток отвечают вложения квадратичных форм для выбранных в решетках базисов. В зависимости от ситуации удобно использовать то решетки, то квадратичные формы. Так, например, следующие свойства вложений естественно формулируются для решеток.

6.3. Определение примитивных вложений форм было дано в п. 1.2. Для решеток *примитивность* вложения $i: M \hookrightarrow L$ будет означать, что $L/i(M)$ – свободный $\mathbb{Z}_p$ -модуль. Далее, вложение i *разложимо*, $i = i_1 \oplus i_2$, если существуют разложения решеток в ортогональные суммы $M = M_1 \oplus M_2$, $\dim M_j \geq 1$ для $j = 1, 2$, $L = L_1 \oplus L_2$, для которых ограничения $i_j = i|_{M_j}$ определяют вложения $i_j: M_j \hookrightarrow L_j$, $j = 1, 2$. Если из включения $iM \subset L_1$ в любую подрешетку L_1 из разложения $L = L_1 \oplus L_2$ следует $L_1 = L$, то i называется *минимальным вложением размерности* $\dim L$.

Перенесем на решетки понятие орбиты $\{b\}$ (1.14) вложений форм. Для любых $\gamma \in \text{Aut } L$ и $U \in \text{Aut } M$ из групп автоморфизмов (изометрий) решеток L и M отображение $i_1 = \gamma \cdot i \cdot U$ – снова вложение M в L . Множество эквивалентных вложений $i_1 \sim i$ образуют орбиту $\{i\}$ вложения i . Если вложение i обладает одним из перечисленных свойств, то им обладают все вложения орбиты $\{i\}$.

6.4. Пусть форма $A = A_0 \oplus pA_p$, $p \neq 2$, имеет такой же вид, как в теореме 5.1. Решетки M с такими формами A называются *p-элементарными*. Для них максимальный порядок элементов факторгруппы $M^*/M \simeq M/AM$, где M^* – двойственная решетка, равен p . Примитивные вложения форм $b: A \hookrightarrow Q$ описываются теоремой 5.1, дающей способ вычисления числа орбит $\{b\}$ таких вложений. Теперь, объединяя разложения форм из пп. 5.1, 5.2 и теорему 5.1, можем дать геометрическое описание вложений соответствующих решеток.

ТЕОРЕМА 6.1. 1) Орбиты $\{i\}$ примитивных вложений $i: M \hookrightarrow L$ параметризуются инвариантами $\{r_\alpha\}$, удовлетворяющими неравенству (5.13).

2) В каждой орбите $\{i\}$ есть вложение $A \hookrightarrow Q_G^A(\{r_\alpha\})$, разлагающееся на минимальное вложение $A \hookrightarrow Q^A(\{r_\alpha\})$ и его ортогональное дополнение,

$$Q_G^A(\{r_\alpha\}) = Q^A(\{r_\alpha\}) \oplus \frac{1}{a}(G \ominus G(\{r_\alpha\})). \quad (6.1)$$

3) При разложении формы $A = A_0 \oplus ae^{-1} \oplus A(\{r_\alpha\})$ минимальное вложение разлагается на вложения

$$A_0 \oplus ae^{-1} \hookrightarrow A_0 \oplus ae^{-1} = A \ominus A(\{r_\alpha\}), \quad (6.2)$$

$$A(\{r_\alpha\}) \hookrightarrow Q(\{r_\alpha\}) = Q(r_0^{\varepsilon_0}) \bigoplus_{\alpha_i > 0} Q(r_{\alpha_i}^{\varepsilon_i}) \bigoplus_{\alpha_i > 0} Q(r_{\alpha_i}^0) \quad (6.3)$$

– суммы одномерных и многомерных минимальных неразложимых вложений следующего вида:

$$1^\varepsilon \hookrightarrow 1^\varepsilon, \quad a \cdot 1^\varepsilon \hookrightarrow a \cdot 1^\varepsilon, \quad A(1_0^\varepsilon) = -a \cdot 1^\varepsilon \hookrightarrow Q(1_0^\varepsilon) = \begin{pmatrix} -a \cdot 1^\varepsilon & 1 \\ 1 & 0 \end{pmatrix} \quad (6.4)$$

– вложения id и 1_0^ε одномерных форм $A = 1^\varepsilon$ и $a \cdot 1^\varepsilon$;

$$A(1_\alpha^\varepsilon) = aJ(1) \hookrightarrow Q(1_\alpha^\varepsilon) = \left(\begin{array}{cc|c} aJ(1) & & 1 \\ & & 0 \\ \hline 1 & 0 & \frac{p^\alpha}{a} \cdot 1^\varepsilon \end{array} \right), \quad (6.5)$$

$$A(1_\alpha^0) = aJ(1) \hookrightarrow Q(1_\alpha^0) = \left(\begin{array}{cc|cc} aJ(1) & & 1 & 0 \\ & & 0 & 0 \\ \hline 1 & 0 & \frac{p^\alpha}{a} J(1) & \end{array} \right) \quad (6.6)$$

– вложения 1_α^ε и 1_α^0 , $\alpha \geq 1$, двумерных решеток $A = aJ(1) = \begin{pmatrix} 0 & a \\ a & 0 \end{pmatrix}$.

4) Все разложения однозначны с точностью до выбора знаков при приведении квадратичных форм к диагональному виду.

ЗАМЕЧАНИЕ 1. Нетрудно подсчитать размерность минимального вложения $\dim Q^A(\{r_\alpha\}) = m + r + r_{>0}^0$, где r – сумма всех размерностей $r_{\alpha_i}^*$, а $r_{>0}^0$ – сумма размерностей $r_{\alpha_i}^0$ для $\alpha_i > 0$. Таким образом, размерность минимальных вложений $\leq 2m$, и равенство достигается только для гиперболических форм $A = aJ(m/2)$ четной размерности m .

ЗАМЕЧАНИЕ 2. Теорема 6.1 утверждает, что любое вложение p -элементарной решетки распадается в ортогональную сумму минимальных неразложимых вложений размерностей 1, 2, 3, 4 ее подрешеток размерностей 1 и 2.

6.5. Минимальные вложения $b: A \hookrightarrow Q$ задаются формами $Q^A(\{r_\alpha\})$ (5.8). Если не интересоваться структурой вложений форм, а, скажем, количеством орбит $\{b\}$, то по теореме 5.1 нужно знать только классы $\{Q^A(\{r_\alpha\})\}$ и их веса, равные числу инвариантов $\{r_\alpha\}$ для данного класса. Для форм A малых определителей из неравенства (5.13) вытекает

ПРЕДЛОЖЕНИЕ 6.1. Пусть форма $A = A_0 \oplus pA_p$ имеет блок A_p размерности $m_p \leq 3$. Тогда орбит $\{b\}$ примитивных представлений $b: Q[b] = A$ столько же, сколько форм $Q^{A_p} \leq Q \ominus A_0$, где формы Q^{A_p} имеют следующий вид: для $m_p = 1$

$$pA_p, \quad J = J(1); \quad (6.7)$$

для $m_p = 2$

$$\begin{aligned} pA_p, \quad J \oplus p1^\pm, \quad J \oplus p^\alpha 1^\pm \quad \text{при } \alpha \geq 2, \quad A_p \sim J, \\ 1_4, \quad J \oplus p^\alpha J \quad \text{при } \alpha \geq 1, \quad A_p \sim J; \end{aligned} \quad (6.8)$$

для $m_p = 3$

$$\begin{aligned} pA_p, \quad J \oplus p1_2^\pm, \quad J \oplus p(A_p \ominus J) \oplus p^\alpha 1^\pm \quad \text{при } \alpha \geq 2, \\ 1_4 \oplus p1^\pm, \quad J \oplus pA_p, \quad J \oplus p(A_p \ominus J) \oplus p^\alpha J, \quad 1_4 \oplus p^\alpha 1^\pm \quad \text{при } \alpha \geq 2, \\ J(3), \quad 1_4 \oplus p^\alpha J \quad \text{при } \alpha \geq 1. \end{aligned} \quad (6.9)$$

Посмотрим применение этих форм на конкретных примерах.

ПРИМЕР 1. Найдем решения $x, y \in \mathbb{Z}_p^4$, $p \neq 2$, системы диофантовых уравнений

$$(x, x) = 1, \quad (y, y) = p, \quad (x, y) = 0, \quad (6.10)$$

где $(x, y) = x_1y_1 + x_2y_2 + p(x_3y_3 + x_4y_4)$.

Имеем $A = 1 \oplus p \cdot 1$, $m_p = 1$, $Q = 1_2 \oplus p \cdot 1_2$. Согласно (6.7) имеется только одна форма $p \cdot 1 \leq 1 \oplus p \cdot 1_2$, и поэтому решения системы образуют одну орбиту. Так как $x = (1, 0, 0, 0)$, $y = (0, 0, 1, 0)$ – решение, то остальные получаются из примитивного решения $b = ({}^t x, {}^t y)$ целыми ортогональными преобразованиями из $O(A)$ и $O(Q)$, которые можно получить с помощью предложения 3.1.

ПРИМЕР 2. Форма $A = p \cdot 1_3$ примитивно вкладывается в четырехмерную форму $Q = Q_0 \oplus pQ_p$. Выясним, для каких Q это возможно. В данном случае $m_p = 3$ и форма Q должна быть по (6.9) больше хотя бы одной из форм $p \cdot 1_3$ или $J \oplus p \cdot 1_2^\pm$. Таким образом, для Q имеются шесть вариантов: $J \oplus p \cdot 1_2^\pm$, $1^\pm \oplus p \cdot 1_3$, $p \cdot 1_4^\pm$.

§ 7. Локальные множители

Теорема 5.1 позволяет найти число решений сравнения $E[C] \equiv -G \pmod{p}$, для которых расширенная форма $Q_G^A(C)$ эквивалентна p -элементарной форме Q . Это число $c(A; Q, G) = c_p(A; Q, G)$ является локальным множителем в формуле (12) для числа представлений над кольцом целых чисел $\mathbb{Z}$ квадратичных форм родом положительно определенных форм.

7.1. Пусть снова $A = A_0 \oplus A_1$ с блоком $A_1 = pA_p$ размерности m_1 , а форма Q также p -элементарная с разложением $Q = Q_0 \oplus Q_1$ и $Q_1 = pQ_p$, $|Q_p| \not\equiv 0(p)$. Ввиду (5.12) форма

$$G = 1(r_0^{\varepsilon_0}) \oplus G_{>0}(\{r_\alpha\}) \oplus (Q \ominus Q^A(\{r_\alpha\})) \quad (7.1)$$

существует, только если инварианты имеют вид $\{r_\alpha\} = \{r_0^{\varepsilon_0}, r_1^0\}$. Для тех $\{r_\alpha\}$, для которых форма G существует, ее класс $\{G\}$ зависит только от параметров $r_0^{\varepsilon_0}$. Найдем число $c(A; Q, G)$ сплетающих матриц C из множества п. 1.6 $C_G^A(Q)$. Используя формулу п. 2.1 $c(A; Q, G) = c(A_1; Q \ominus A_0, G)$, приходим к следующему разбиению:

$$c(A; Q, G) = \sum_{r_1} c(\{r_\alpha\}), \quad (7.2)$$

где $r_1 = r_1^0$ пробегает все значения из уравнения (7.1), $c(\{r_\alpha\})$ – число элементов орбиты $\{C\}$ с инвариантами $\{r_\alpha\}$. Согласно (2.8) и (5.7) можем считать

$$E = aA_1^{-1} = -G_0 \oplus J(r_1) \oplus e, \quad e = \{a\}A_p \ominus (-1(r_0^{\varepsilon_0})) \ominus J(r_1). \quad (7.3)$$

Далее, из (7.1) вытекает $G = G_0 \oplus G_1 \oplus G_2$ с блоком $G_1 = pG_p$ размерности k_1 и (см. (2.8))

$$G_p = J(r_1) \oplus g_1, \quad g_1 = \{a\}(Q_0 \ominus A_0 \ominus J(r)), \quad (7.4)$$

где $r = r_0 + r_1$. По (2.7) в орбите $\{C\}$ можем взять матрицу $C = C_{\text{fix}}$ вида

$$C = \left(\begin{array}{c|cc|cc} 1_{r_0} & & & & & \\ \hline & 1_{r_1} & 0 & 0 & & \\ & 0 & 0 & 0 & & \\ \hline & & & & & \end{array} \right).$$

Из доказательства пп. 2.4–2.7 следует, что элементы орбиты $\{C\}$ имеют вид $UCV \pmod{p}$, где $U \in O(E)$, $V \in O(G)$ и

$$U = \begin{pmatrix} \alpha & a & b & c \\ a_1 & A & B & E \\ b_1 & C & D & G \\ c_1 & E_1 & G_1 & F \end{pmatrix}, \quad V = \begin{pmatrix} 1 & 0 & 0 \\ 0 & V_1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad V_1 = \begin{pmatrix} A' & B' & E' \\ C' & D' & G' \\ E'_1 & G'_1 & F' \end{pmatrix} \in O(G_p),$$

с разбиениями на блоки из (7.3) и (7.4). Отсюда заключаем, что

$$c(\{r_\alpha\}) = o(A_p)o(G_p)/\text{stab}(\{r_\alpha\}). \quad (7.5)$$

Здесь $o(\cdot)$ обозначает *порядок ортогональной группы* $O(\cdot/p)$ над полем $\mathbb{F}_p$, а $\text{stab}(\{r_\alpha\})$ – *стабилизатор* матрицы $C \pmod{p}$.

7.2. Найдем порядок стабилизатора. Из условия $UCV \equiv C \pmod{p}$ прямыми вычислениями выводим сравнения

$$U \equiv \begin{pmatrix} 1 & 0 & b & c \\ 0 & A & B & E \\ 0 & 0 & D & G \\ 0 & 0 & G_1 & F \end{pmatrix}, \quad V_1 \equiv \begin{pmatrix} A' & 0 & 0 \\ C' & D' & G' \\ E'_1 & G'_1 & F' \end{pmatrix}, \quad AA' \equiv 1 \pmod{p}. \quad (7.6)$$

По лемме 3.3 отображение $O(E) \xrightarrow{\text{mod } p} O(E/p)$ эпиморфно. Все рассуждения проводятся по $\text{mod } p$, и поэтому можем считать U из группы $O(E/p)$, т.е. $E[U] \equiv E \pmod{p}$. Это сравнение равносильно тому, что

$$U \equiv \begin{pmatrix} 1 & 0 \\ 0 & U_1 \end{pmatrix} \text{ с блоком } U_1 = \begin{pmatrix} A & B & E \\ 0 & D & G \\ 0 & G_1 & F \end{pmatrix} \in O\left(\begin{pmatrix} J(r_1) & 0 \\ 0 & e \end{pmatrix}/p\right).$$

Последнее включение равносильно условиям $G \equiv 0(p)$ и

$$\begin{aligned} {}^t A D &\equiv 1, & ({}^t B D)^s + e[G_1] &\equiv 0 \pmod{p}, \\ {}^t D E + {}^t G_1 e F &\equiv 0, & e[F] &\equiv e \pmod{p}, \end{aligned} \quad (7.7)$$

где использовано обозначение $M^s = M + {}^t M$ для симметризации квадратной матрицы M . В сравнениях (7.7) матрицы A с определителем $|A| \not\equiv 0(p)$, блоки G_1 и $F \in O(e/p)$ можно брать любыми по $\text{mod } p$. Этим выбором матрицы D и E определяются однозначно.

Осталось найти решения B сравнения $({}^t B D)^s \equiv -e[G_1] \pmod{p}$. Разложим произведение ${}^t B D = S + S_-$ в сумму симметрической матрицы $S = {}^t S$ и кососимметрической матрицы $S_- = -{}^t S_-$, где слагаемые $S = \frac{1}{2}({}^t B D)^s$ и $S_- = \frac{1}{2}({}^t B D - {}^t D B)$ определены однозначно. Поэтому исходное сравнение равносильно $2S \equiv -e[G_1](p)$. По условию $p \neq 2$, и, следовательно, $S \equiv -\frac{1}{2}e[G_1](p)$ однозначно определяется матрицей G_1 , а кососимметрическая матрица S_- может быть любой. Так как по (7.7) матрица D обратима, то получаем требуемые решения $B \equiv {}^t D^{-1}(S - S_-) \pmod{p}$.

Из предыдущих рассуждений для блока U_1 , а следовательно, и для U получаем параметризацию матрицами A, G_1, S_- и F , удовлетворяющими условиям

$$\begin{aligned} A &\in \text{GL}_{r_1}(\mathbb{F}_p), & G_1 &\in M_{m_1-(r_0+2r_1), r_1}(\mathbb{F}_p), \\ S_- &\equiv -{}^t S_- \in M_{r_1}(\mathbb{F}_p), & F &\in O(e/p). \end{aligned} \quad (7.8)$$

Перейдем теперь к матрицам V_1 (7.6) из $O(G_p)$. Снова получаем $V_1 \in O(G_p/p)$. Сравнение $G_p[V_1] \equiv G_p \pmod{p}$ равносильно сравнению $G_p^{-1}[{}^t V_1] \equiv G_p^{-1} \pmod{p}$, а транспонированная матрица уже аналогична матрице U_1 . Отсюда сразу получаем для V_1 параметризацию матрицами A', G', S'_- и F' , удовлетворяющими условиям

$$\begin{aligned} A' &\in \text{GL}_{r_1}(\mathbb{F}_p), & G' &\in M_{r_1, k_1-2r_1}(\mathbb{F}_p), \\ S'_- &\equiv -{}^t S'_- \in M_{r_1}(\mathbb{F}_p), & F' &\in O(g_1/p). \end{aligned} \quad (7.9)$$

Согласно (7.6) матрицы U и V_1 связаны одним условием $AA' \equiv 1(p)$. Поэтому из (7.8) и (7.9) получаем формулу

$$\text{stab}(\{r_\alpha\}) = \text{gl}(r_1)p^{(m_1-(r_0+2r_1))r_1}p^{\langle r_1 \rangle}o(e)p^{(k_1-2r_1)r_1}p^{\langle r_1 \rangle}o(g_1), \quad (7.10)$$

где $\text{gl}(r)$ – порядок полной линейной группы $\text{GL}_r(\mathbb{F}_p)$ невырожденных матриц размера r над полем $\mathbb{F}_p$, $\langle r \rangle = r(r-1)/2$.

7.3. Группа $\text{GL}_r(\mathbb{F}_p)$ действует транзитивно на проколоте пространстве $V = \mathbb{F}_p^r \setminus \{0\}$. Следовательно, $p^r - 1 = \text{gl}(r)/\text{stab}(v)$, где $\text{stab}(v)$ – стабилизатор, скажем, вектора $v = (1, 0, \dots, 0)$. Далее рассуждаем, как при доказательстве (7.8), и по индукции получаем формулу

$$\text{gl}(r) = p^{r^2}(1-p^{-1}) \cdots (1-p^{-r}). \quad (7.11)$$

Что же касается ортогональных групп над конечными полями $\mathbb{F}_p$, $p \neq 2$, то можно повторить тот же прием. Приведем в удобном для нас виде формулу из [2, с. 79]:

$$o(1(r^\varepsilon)) = p^{\langle r \rangle} M(r^\varepsilon)^{-1}, \quad (7.12)$$

где

$$M(r^\varepsilon)^{-1} = \begin{cases} 2(1-p^{-2}) \cdots (1-p^{-2r'}) & \text{для } r = 2r' + 1, \\ 2(1-p^{-2}) \cdots (1-p^{-2(r'-1)})(1-\varepsilon'p^{-r'}) & \text{для } r = 2r' \end{cases}$$

и знак ε' определен формулой $\varepsilon' = \varepsilon \left(\frac{(-1)^{r'}}{p} \right)$.

7.4. Из формул (7.2) и (7.10) вытекает

ТЕОРЕМА 7.1. Пусть форма $A = A_0 \oplus A_1$ с блоком $A_1 = pA_p$ размерности m_1 , $Q = Q_0 \oplus Q_1$ с блоком $Q_1 = pQ_p$, $p \neq 2$, и пусть $c(A; Q, G)$ – число сцепляющих матриц из множества $C_G^A(Q)$ п. 1.6. Тогда неравенство $c(A; Q, G) > 0$ равносильно существованию формы G (7.1). Если G существует, то имеет место следующая формула:

$$c(A; Q, G) = o(A_p)o(G_p) \sum_{r_1} \text{stab}(\{r_\alpha\})^{-1}, \quad (7.13)$$

при этом $\{r_\alpha\} = \{r_0^{\varepsilon_0}, r_1^0\}$ и $r_1 = r_1^0 \geq 0$ пробегает все значения, удовлетворяющие равенству (7.1), G_p – форма (7.3) размерности k_1 и

$$\text{stab}(\{r_\alpha\}) = p^{r_1(m_1+k_1-r_0-3r_1-1)} \text{gl}(r_1)o(e)o(g_1), \quad (7.14)$$

где e и g_1 – соответственно формы из разложений (7.3) и (7.4).

Формула (7.13) сильно упрощается для частного случая формы $Q = Q_0$ с делителем $|Q_0| \not\equiv 0(p)$. Так, из формулы (7.1) находим

$$G_2 = a\{pQ_p \oplus [pJ(r_1) \oplus (pA_p \oplus (-a)1(r_0^{\varepsilon_0}) \oplus J(r_1))]\}.$$

По условию блок Q_p нулевой и, значит, вся форма в квадратных скобках также нулевая. Отсюда заключаем, что $r_1 = 0$ и $pA_p = (-a)1(r_0^{\varepsilon_0})$. Поэтому форма e из разложения (7.3) нулевая. В силу (7.4) записываем $G_p = g_1$, и по (7.14) $\text{stab}(\{r_\alpha\}) = o(g_1) = o(G_p)$. В нашем случае равенство (7.1) однозначно определяет форму

$$G = \{-a\}A_p \oplus a(Q_0 \ominus A_0 \ominus J(m_1)),$$

условие существования которой принимает вид $A_0 \oplus J(m_1) \leq Q_0$, и по формуле (7.13)

$$c(A; Q, G) = o(A_p), \quad Q = Q_0. \quad (7.15)$$

Другим способом формула (7.15) доказана в [2].

Список литературы

1. Артин Э. Геометрическая алгебра. М.: Наука, 1969.
2. Журавлёв В. Г. Представление формы родом квадратичных форм // Алгебра и анализ. 1996. Т. 8. № 1. С. 21–112.
3. Касселс Дж. Рациональные квадратичные формы. М.: Мир, 1982.
4. Конвей Дж., Слоэн Н. Упаковки шаров, решетки и группы. М.: Мир, 1990.
5. Никулин В. В. Целочисленные симметрические билинейные формы и некоторые их геометрические приложения // Изв. АН СССР. Сер. матем. 1979. Т. 43. № 1. С. 111–177.
6. Siegel C. L. Über die analytische Theorie der quadratischen Formen // Ann. of Math. 1935. В. 36. № 2. S. 527–606.
7. Журавлёв В. Г. Орбиты представлений чисел локальными квадратичными формами // Тр. МИРАН. 1997. Т. 218. С. 151–164.

Поступило в редакцию
20.VII.1997