Записки научных
семинаров ПОМИ
Том 523, 2023 г.

В. М. Поляков

ВЕКТОРНЫЕ РАССЛОЕНИЯ РАНГА 2 НА $\mathbb{P}^1_{\mathbb{Z}}$ И КВАДРАТИЧНЫЕ ФОРМЫ

§1. Основные обозначения

В работе мы будем придерживаться стандартных обозначений:

$$\mathbb{P}^1_{\mathrm{A}} = \mathrm{Proj}\ A[t_0, t_1], \qquad \deg\, t_0 = \deg\, t_1 = 1,$$

где A – нетерово кольцо. В обозначениях $\mathcal{O}_X$ и $\mathcal{O}_X(n)$ будем опускать $X = \mathbb{P}^1_{\mathrm{A}}$ и писать просто $\mathcal{O}$ и $\mathcal{O}(n)$. Как обычно, U_i – дополнение к нулям t_i, $U_{01} = U_0 \cap U_1$, $x = t_1/t_0$, $y = t_0/t_1$. Кроме того $\mathcal{O}(U_0) = A[x]$, $\mathcal{O}(U_1) = A[y]$, $\mathcal{O}(U_{01}) = A[x, y]$, при этом $xy = 1$.

§2. Введение

В данной работе мы будем изучать связь расслоений на $\mathbb{P}^1_{\mathbb{Z}}$ ранга 2 с тривиальным общим слоем и простыми подскоками с бинарными квадратичными формами. В первой части работы будет рассмотрено действие группы $\mathrm{SL}_2(\mathbb{Z})$ на классах изоморфизма векторных расслоений на $\mathbb{P}^1_{\mathbb{Z}}$ ранга 2 с тривиальным общим слоем и простыми подскоками. Для этого мы введем и изучим соответствующее действие на $\mathrm{Ext}^1(\mathcal{O}(2), \mathcal{O}(\text{-}2))$, что окажется более естественным. В работе [2] было доказано, что любое расслоение ранга 2 с тривиальным общим слоем и простыми подскоками реализуется как элемент $\mathrm{Ext}^1(\mathcal{O}(2), \mathcal{O}(\text{-}2))$. Расслоение, соответствующее элементу $\mathcal{E} \in \mathrm{Ext}^1(\mathcal{O}(2), \mathcal{O}(\text{-}2))$,

$$\mathcal{E} : 0 \longrightarrow \mathcal{O}(-2) \longrightarrow E \longrightarrow \mathcal{O}(2) \longrightarrow 0$$

мы будем, как правило, обозначать той же буквой. Будет доказано, что такие расслоения эквивариантны относительно действия $\mathrm{SL}_2(\mathbb{Z})$.

Во второй части работы будут изучаться оснащенные векторные расслоения, то есть расслоения с фиксированным изоморфизмом определителя и тривиального расслоения. Эта фиксация дает более тонкую классификацию и позволяет связать множество классов изоморфизма

Ключевые слова: векторное расслоение, арифметическая поверхность, проективная прямая, подскоки.

Работа выполнена при финансовой поддержке Минобрнауки РФ (грант на создание и развитие МЦМУ им. Леонарда Эйлера, соглашение No. 075-15-2022-289).

таких расслоений с фактором по 2-кручению группы классов, что является группой родов.

§3. Действие $\mathrm{SL}_2(\mathbb{Z})$ на расслоениях

3.1. Сопоставление элементу $\mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(-2))$ **формы.** Пусть $\mathcal{E}$ элемент $\mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(-2)) \simeq H^1(\mathcal{O}(-4)) \simeq \mathbb{Z}^3$, которому соответсвует расслоение E на $\mathbb{P}^1_{\mathbb{Z}}$ ранга 2 с тривиальным общим слоем и простыми подскоками. Далее мы будем фиксировать изоморфизм

$$\mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(-2)) \simeq \mathbb{Z}^3$$

и считать элементом $\mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(\text{-}2))$ тройку чисел. Можно проверить, что элементу $(a,b,c) \in \mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(\text{-}2))$ соответствует расслоение с фиксированной матрицей склейки

$$\sigma = \begin{pmatrix} y^2 & cy+b+ax \\ 0 & x^2 \end{pmatrix}.$$

Мы предполагаем, что полученное расслоение имеет простые подскоки, поэтому считаем, что $(a,b,c)=1$, а также $b^2-ac=\nu$, где ν – дискриминант расслоения E, в простых делителях которого лежат точки подскока ($H^1(E(-1)) \simeq \mathbb{Z}/\nu$).

Сопоставим элементу группы $\mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(\text{-}2))$ бинарную квадратичную форму с помощью следующей цепочки канонических морфизмов:

$$\begin{aligned}\mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(-2)) &\overset{\simeq}{\to} H^1(\mathcal{O}(-4)) \overset{\simeq}{\to} H^0(\mathcal{O}(2)) \\ &\overset{\simeq}{\to} S^2(V^*)^* \overset{\simeq}{\to} DP^2(V) \to S^2(V),\end{aligned}$$

V – некоторый свободный $\mathbb{Z}$-модуль ранга 2, причем $\mathbb{P}^1_{\mathbb{Z}}=\mathrm{Proj}(S(V^*))$, $S(V)$ – алгебра симметрических степеней, $DP(V)$ – алгебра разделенных степеней и последняя стрелка задается следующим образом: $v_0\otimes v_0 \to v_0^2$, $v_1\otimes v_1 \to v_1^2$, $v_0\otimes v_1 + v_1 \otimes v_0 \to 2v_0v_1$.

Тогда мы получаем, что образом элемента

$$(a,b,c) \in \mathbb{Z}^3 \simeq \mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(-2))$$

будет форма $av_0^2+2bv_0v_1+cv_1^2$ (с дискриминантом равным 4ν). Далее бинарную квадратичную форму $aX^2+bXY+cY^2$ будем обозначать $[a,b,c]$. Таким образом, стрелка $\mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(\text{-}2)) \to S^2(V)$ выглядит так:

$$(a,b,c) \mapsto [a,2b,c].$$

3.2. Действие $\mathrm{GL}_2(\mathbb{Z})$ на $\mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(\text{-}2))$. Заведем действие $\mathrm{GL}_2(\mathbb{Z})$ на $\mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(\text{-}2))$ следующим образом. Возьмем элемент $g\in\mathrm{GL}_2(\mathbb{Z})$ и рассмотрим его образ в $\mathrm{PGL}_2(\mathbb{Z})=\mathrm{Aut}(\mathbb{P}^1_{\mathbb{Z}})$, обозначим его той же буквой.

Вместо классического действия $\mathrm{PGL}_2(\mathbb{Z})$ на $\mathbb{P}^1_{\mathbb{Z}}$ рассмотрим следующее подкрученное действие: элемент $g\in\mathrm{PGL}_2(\mathbb{Z})$ переводит

$$\begin{pmatrix}t_0\\t_1\end{pmatrix}\quad \text{в}\quad Rg^{-1}R\begin{pmatrix}t_0\\t_1\end{pmatrix},\quad \text{где}\quad R=\begin{pmatrix}0&1\\1&0\end{pmatrix}.$$

Такая подкрутка делается для того, как мы дальше увидим, чтобы действие $\mathrm{SL}_2(\mathbb{Z})$ на $\mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(\text{-}2))$ индуцировало классическое действие на квадратичных формах.

Зафиксируем некоторый изоморфизм $\gamma(-1): g^*\,\mathcal{O}(-1)\xrightarrow{\simeq}\mathcal{O}(-1)$, который будет либо тождественным либо умножением на -1. Тогда индуцированные изоморфизмы на четных степенях тавтологического расслоения будут тождественными, так что от выбора изоморфизма ничего не будет зависеть. Возьмем элемент $\mathcal{E}\in\mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(\text{-}2))$,

$$\mathcal{E}: 0\longrightarrow\mathcal{O}(-2)\xrightarrow{\alpha}E\xrightarrow{\beta}\mathcal{O}(2)\longrightarrow 0$$

и рассмотрим следующую диаграмму:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{O}(-2) \arrow[r, "\alpha"] \arrow[d, "\gamma(-2)"] \arrow[dr, "\xi"] & E \arrow[r, "\beta"] & \mathcal{O}(2) \arrow[r] \arrow[d, "\gamma(2)"] & 0 \\
0 \arrow[r] & g^*\,\mathcal{O}(-2) \arrow[r, "g^*\alpha"] & g^*E \arrow[r, "g^*\beta"] \arrow[ur, "\chi"] & g^*\,\mathcal{O}(2) \arrow[r] & 0.
\end{tikzcd}$$

Здесь диагональные стрелки – это композиции соответствующих вертикальных и горизонтальных стрелок, а вертикальные стрелки – тождественные изоморфизмы. Тогда в качестве $g^*\mathcal{E}$ мы возьмем

$$g^*\mathcal{E}: 0\longrightarrow\mathcal{O}(-2)\xrightarrow{\xi}g^*E\xrightarrow{\chi}\mathcal{O}(2)\longrightarrow 0.$$

Далее будет видно, что для более полной аналогии с теорией бинарных квадратичных форм будет естественно рассматривать действие не всей группы $\mathrm{GL}_2(\mathbb{Z})$, а только ее подгруппы $\mathrm{SL}_2(\mathbb{Z})$, поэтому теперь мы будем рассматривать только эту группу.

Определение 1. *Будем называть два расширения*

$$\mathcal{E},\mathcal{F}\in\mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(\text{-}2))$$

эквивалентными и писать $\mathcal{E} \sim \mathcal{F}$*, если найдется* $g \in \mathrm{SL}_2(\mathbb{Z})$ *такой, что* $\mathcal{E} \simeq g^*\mathcal{F}$*.*

3.3. Вычисление действия $\mathrm{SL}_2(\mathbb{Z})$ **на** $\mathrm{Ext}^1(\mathcal{O}(2), \mathcal{O}(\text{-}2))$**.** Вычислим теперь куда переходит расширение $\mathcal{E} = (a, b, c) \in \mathrm{Ext}^1(\mathcal{O}(2), \mathcal{O}(\text{-}2))$ под действием

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Для этого вычислим действие образующих

$$S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{и} \quad T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{группы} \quad \mathrm{SL}_2(\mathbb{Z}).$$

3.3.1. *Действие* S*.* По определению подкрученного действия,

$$\begin{pmatrix} t_0 \\ t_1 \end{pmatrix} \quad \text{перейдет в} \quad RS^{-1}R \begin{pmatrix} t_0 \\ t_1 \end{pmatrix} = \begin{pmatrix} -t_1 \\ t_0 \end{pmatrix}.$$

Тогда пуллбек расслоения с матрицей склейки

$$\sigma = \begin{pmatrix} y^2 & cy + b + ax \\ 0 & x^2 \end{pmatrix},$$

которая связывает базисы на U_0 и U_1 будет иметь матрицу склейки

$$\sigma = \begin{pmatrix} x^2 & -ax + b - cy \\ 0 & y^2 \end{pmatrix},$$

связывающую базисы на U_1 и U_0. Тогда матрица склейки S^*E, связывающая базисы на U_0 и U_1, будет

$$\sigma = \begin{pmatrix} y^2 & ay - b + cx \\ 0 & x^2 \end{pmatrix}.$$

Таким образом,

$$S^*(a, b, c) = (c, -b, a).$$

3.3.2. *Действие* T*.* Под действием T, пара $\begin{pmatrix} t_0 \\ t_1 \end{pmatrix}$ перейдет в $\begin{pmatrix} t_0 \\ t_1 - t_0 \end{pmatrix}$.

Пусть снова $\mathcal{E} = (a, b, c) \in \mathrm{Ext}^1(\mathcal{O}(2), \mathcal{O}(\text{-}2))$ представлен расслоением E с матрицей склейки

$$\sigma = \begin{pmatrix} y^2 & cy + b + ax \\ 0 & x^2 \end{pmatrix}.$$

Тогда пуллбэк будет иметь матрицу склейки

$$\sigma' = \begin{pmatrix} {y'}^2 & cy' + b + ax' \\ 0 & {x'}^2 \end{pmatrix}, \quad x' = \frac{t_1 - t_0}{t_0}, \quad y' = \frac{t_0}{t_1 - t_0},$$

которая связывает базисы расслоения E на $T^{-1}(U_0) = U_0$ и $T^{-1}(U_1) = \{$дополнение к нулям $t_1 - t_0\}$. Предположим, что T^*E имеет матрицу склейки

$$\tau = \begin{pmatrix} y^2 & fy + e + dx \\ 0 & x^2 \end{pmatrix}$$

для базисов на U_0 и U_1. Чтобы найти f, e, d достаточно расписать матрицу склейки между базисами U_1 и $T^{-1}(U_1)$, образованную композицией $\tau^{-1}\sigma'$ и потребовать, чтобы в знаменателях ее элементов были только t_1 и $t_1 - t_0$. Расписав это условие мы получаем однозначно определенные d, e, f. В конечном итоге получаем

$$T^*(a, b, c) = (a, a + b, a + 2b + c).$$

3.3.3. *Действие произвольной матрицы* $g \in \mathrm{SL}_2(\mathbb{Z})$. Зная как действуют образующие $\mathrm{SL}_2(\mathbb{Z})$, несложно по индукции (по длине слова состоящего из букв T и S) вывести, как выглядит действие произвольного элемента. Пусть

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}), \quad (a, b, c) \in \mathrm{Ext}^1(\mathcal{O}(2), \mathcal{O}(\text{-}2)),$$

тогда $g^*(a, b, c)$ равно

$$(a\alpha^2 + 2b\alpha\gamma + c\gamma^2,\ a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta,\ a\beta^2 + 2b\beta\delta + c\delta^2).$$

Видно, что наше действие $\mathrm{SL}_2(\mathbb{Z})$ на $\mathrm{Ext}^1(\mathcal{O}(2), \mathcal{O}(\text{-}2))$ согласованно с действием $\mathrm{SL}_2(\mathbb{Z})$ на квадратичных формах (напомним, что отображение $\mathrm{Ext}^1(\mathcal{O}(2), \mathcal{O}(\text{-}2)) \to S^2(V)$ устроено так: $(a, b, c) \mapsto [a, 2b, c]$). Таким образом, следующая диаграмма коммутативна:

$$\begin{tikzcd} (a, b, c) \arrow[r] \arrow[d] & {[a, 2b, c]} \arrow[d] \\ g^*(a, b, c) \arrow[r] & g \circ [a, 2b, c]\,. \end{tikzcd}$$

Теорема 1. *Расслоения ранга 2 с тривиальным общим слоем и простыми подскоками эквивариантны относительно действия* $\mathrm{SL}_2(\mathbb{Z})$, *то есть* $g^*E \simeq E$ *для любого* $g \in \mathrm{SL}_2(\mathbb{Z})$.

Доказательство. Пусть $E = V(\nu, \varepsilon)$ – расслоение ранга 2 с тривиальным общим слоем и простыми подскоками, тогда его можно задать с помощью матрицы склейки

$$\sigma = \begin{pmatrix} y^2 & cy + b + ax \\ 0 & x^2 \end{pmatrix},$$

где $c \equiv \varepsilon\lambda^2 \pmod{\nu}$. Пусть

$$g = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

тогда коэффициент при y в матрице склейки расслоения g^*E будет $a\beta^2 + 2b\beta\delta + c\delta^2 \equiv b^2\beta^2/c + 2b\beta\delta + c\delta^2 \equiv c(\delta + b\beta/c)^2 \pmod{\nu}$. Таким образом, $g^*V(\nu, \varepsilon) \simeq V(\nu, c\lambda_1^2) \simeq V(\nu, \varepsilon)$. □

§4. Оснащенные расслоения

Далее мы будем изучать расслоения на $\mathbb{P}^1_{\mathbb{Z}}$ ранга 2 с тривиальным общим слоем и простыми подскоками с фиксированными изоморфизмами $t_E : \det(E) \longrightarrow \mathcal{O}$.

Определение 2. *Мы будем называть пару (E, t_E) оснащенным расслоением. В дальнейшем мы будем опускать t_E в этом обозначении и просто писать E.*

Определение 3. *Будем говорить, что два оснащенных расслоения E и F строго изоморфны, если существует изоморфизм расслоений $f\colon E \xrightarrow{\simeq} F$ и этот изоморфизм индуцирует тождественный морфизм из $\mathcal{O}$ в $\mathcal{O}$, то есть $t_E^{-1}\det(f)t_F = id_{\mathcal{O}}$.*

Замечание 1. Технически и морально изучение оснащенных расслоений отличается от изучения обычных расслоений только тем, что во всех определениях и вычислениях группы GL заменяются на SL.

По аналогии с классификацией обычных расслоений доказывается следующая теорема классификации оснащенных расслоений. Классификация практически совпадает с обычной, только теперь необходимо учитывать знаки (в общем случае – единицы кольца), для этого вводится отдельный параметр, который принимает значения ± 1.

Пусть $\nu, \varepsilon \in \mathbb{Z}$, $u = \pm 1$. Обозначим $V(\nu, \varepsilon, u)$ расслоение, которое является коядром стрелки

$$\varphi = \begin{pmatrix} ut_1 & 0 \\ \varepsilon t_0 & t_1 \\ \nu t_0 & 0 \\ 0 & t_0 \end{pmatrix}$$

в следующей короткой точной последовательности

$$0 \longrightarrow \mathcal{O}(-2)^2 \xrightarrow{\varphi} \mathcal{O}(-1)^4 \longrightarrow V(\nu, \varepsilon, u) \longrightarrow 0.$$

Теорема 2. (i) *Любое оснащенное векторное расслоение на* $\mathbb{P}^1_{\mathbb{Z}}$ *ранга 2 с тривиальным общим слоем и простыми подскоками с точностью до строгого изоморфизма имеет вид* $V(\nu, \varepsilon, u)$, *где* $\nu, \varepsilon \in \mathbb{Z}$, $u = \pm 1$, $\nu > 0$ *и* $(\nu, \varepsilon) = 1$.

(ii) *Пусть два оснащенных расслоения* $V_1 = V(\nu, \varepsilon, u_1)$ *и* $V_2 = V(\mu, \xi, u_2)$ *ранга 2 с тривиальным общим слоем и простыми подскоками на* $\mathbb{P}^1_{\mathbb{Z}}$ *задаются матрицами*

$$\varphi = \begin{pmatrix} u_1 t_1 & 0 \\ \varepsilon t_0 & t_1 \\ \nu t_0 & 0 \\ 0 & t_0 \end{pmatrix} \quad \text{и} \quad \psi = \begin{pmatrix} u_2 t_1 & 0 \\ \xi t_0 & t_1 \\ \mu t_0 & 0 \\ 0 & t_0 \end{pmatrix}$$

соответственно, тогда они строго изоморфны если и только если $\nu = \mu$, $u_1 = u_2$ *и* $\exists \lambda \in \mathbb{Z}\colon \xi \equiv \lambda^2 \varepsilon \pmod{\nu}$.

Доказательство. Мы не будем приводить доказательство этой теоремы, поскольку оно практически полностью совпадает с доказательством аналогичной теоремы для неоснащенных расслоений, за исключением того, что на каждом шаге приходится следить за знаком. □

Определение 4. *Обозначим множество классов строгого изоморфизма оснащенных векторных расслоений на* $\mathbb{P}^1_{\mathbb{Z}}$ *ранга 2 с тривиальным общим слоем и простыми подскоками дискриминанта* ν *как* $Cl_{vect}(\nu)$ *и зададим на этом множестве умножение следующим образом*

$$V(\nu, \varepsilon, u) \cdot V(\nu, \xi, v) = V(\nu, \varepsilon\xi, uv).$$

Тривиально проверяется, что данная операция задает структуру группы на $Cl_{vect}(\nu)$ *с единицей* $V(\nu, 1, 1)$.

Замечание 2. Из пункта (ii) предыдущей теоремы следует, что
$$Cl_{vect}(\nu) \simeq (\mathbb{Z}/n)^{\times}/((\mathbb{Z}/n)^{\times})^2.$$

Будем обозначать $Cl(n)$ группу классов бинарных квадратичных форм с целыми коэффициентами дискриминанта n.

4.1. Существование 2-фильтрации с квадратичной формой отрицательного дискриминанта.

Теорема 3. *Пусть даны* $\nu \in \mathbb{Z}$, $\varepsilon \in (\mathbb{Z}/\nu)^{\times}/((\mathbb{Z}/\nu)^{\times})^2$ *такие, что* $\nu \equiv 1 \pmod 4$, $\nu > 0$. *Тогда существуют такие* $a, b, c \in \mathbb{Z}$, *что* $b^2 - ac = -\nu$ *и* a *является представителем класса* ε.

Доказательство. Пусть $\nu = p_1^{k_1} \dots p_n^{k_n}$ – каноническое разложение. Предположим, что a нечетное простое число и будем искать все сравнения, которым удовлетворяет a, после чего воспользуемся теоремой Дирихле о простых числах в арифметической прогрессии и установим существование такого a. Пусть $p_1, \dots, p_s$ – простые числа, входящие в разложение ν в нечетных степенях, тогда
$$\begin{aligned}\left(\frac{-\nu}{a}\right) &= \left(\frac{-1}{a}\right)\left(\frac{\nu}{a}\right) = (-1)^{\frac{a-1}{2}}\left(\frac{p_1}{a}\right)\dots\left(\frac{p_s}{a}\right)\\ &= (-1)^{\frac{a-1}{2}}(-1)^{\frac{a-1}{2}(\frac{p_1-1}{2}+\dots+\frac{p_s-1}{2})}\left(\frac{a}{p_1}\right)\dots\left(\frac{a}{p_s}\right)\end{aligned}$$
Поскольку $\nu \equiv 1 \pmod 4$, среди $p_1, \dots, p_s$ четное число простых, сравнимых с 3 по модулю 4, поэтому второй множитель равен 1. Также, поскольку $\overline{a} = \varepsilon$ в $(\mathbb{Z}/\nu)^{\times}/((\mathbb{Z}/\nu)^{\times})^2$, последние s множителей зафиксированы. Поэтому, потребовав сравнение $a \equiv 1 \pmod 4$ либо $a \equiv 3 \pmod 4$, с помощью первого множителя мы можем добиться того, чтобы весь символ Лежандра равнялся 1. Таким образом, имеем систему сравнений. Осталось воспользоваться теоремой Дирихле о простых числах и найти требуемое a. □

Эта теорема и вычисления (4.2.5) из [2] говорят о том, что расслоение с простыми подскоками и тривиальным общим слоем $E = V(\nu, \varepsilon)$, где $\nu > 0$, можно задать матрицей склейки
$$\sigma = \begin{pmatrix} y^2 & ay + b + cx \\ 0 & x^2 \end{pmatrix},$$
где a представляет класс ε, и $b^2 - ac = -\nu$, то есть соответствующая квадратичная форма $[c, 2b, a]$ имеет отрицательный дискриминант -4ν.

4.2. $\alpha-$инвариант квадратичной формы. Далее нам потребуется отображение, которое сопоставляет квадратичной форме отрицательного дискриминанта $-4n$ ее первый коэффициент по модулю n с точностью до квадратов, будем называть его $\alpha-$инвариантом.

Более точно, определим отображение

$$\alpha : Cl(-4n) \to (\mathbb{Z}/n)^{\times}/((\mathbb{Z}/n)^{\times})^2$$

следующим образом: для заданного класса форм $\overline{f}$ берем такого его представителя $[a, 2b, c]$, чтобы $(a, n) = 1$ и сопоставляем этому классу a $(\mathrm{mod}\ n)$ с точностью до умножения на взаимно простые с n квадраты. Такой представитель всегда найдется, см. лемму 2.25 в [3].

Определение 5. *Будем называть представителя класса форм допустимым, если его первый коэффициент – a взаимно прост с n.*

Далее мы также будем пользоваться отображением, сопоставляющим конкретной форме ее первый коэффициент с точностью до квадратов по модулю n, и будем обозначать это отображение α'.

Предложение 1. *Отображение α не зависит от выбора допустимого представителя класса квадратичных форм и является гомоморфизмом групп.*

Доказательство. Сначала докажем независимость от выбора допустимого представителя. Любой другой допустимый представитель класса получается из фиксированного $[a{,}2b{,}c]$ действием группы $\mathrm{SL}_2(\mathbb{Z})$ (обратное, конечно, не верно, а именно, что при действии этой группы мы будем получать только допустимые представители), поэтому достаточно проверить независимость, подействовав на $[a, 2b, c]$ подходящим элементом

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Имеем,

$$\begin{aligned} \alpha'(S * [a, 2b, c]) &= \alpha'\big([a\alpha^2 + 2b\alpha\gamma + c\gamma^2, *, *]\big) \\ &\equiv a\alpha^2 + 2b\alpha\gamma + c\gamma^2 \equiv a\alpha^2 + 2\alpha\gamma b + a^{-1}b^2\gamma^2 \\ &\equiv a\Big(\alpha^2 + 2\frac{b}{a}\alpha\gamma + \Big(\frac{b}{a}\Big)^2\gamma^2\Big) \equiv a\Big(\alpha + \frac{b}{a}\gamma\Big)^2 \ (\mathrm{mod}\ n). \end{aligned}$$

Таким образом, отображение α' действует одинаково на допустимых формах из одного класса, поэтому отображение α определено корректно.

Для доказательства того, что α гомоморфизм возьмем два класса $\overline{f}$ и $\overline{g}$ квадратичных форм дискриминанта $-4n$ и выберем в них по допустимому представителю $[a_1, 2b_1, c_1]$ и $[a_2, 2b_2, c_2]$, соответственно. Тогда, по определению композиции бинарных квадратичных форм,

$$[a_1, 2b_1, c_1] \circ [a_2, 2b_2, c_2] = [\frac{a_1 a_2}{d^2}, *, *],$$

где $d = \gcd\Big(a_1, a_2, \dfrac{b_1 + b_2}{2}\Big)$ взаимно прост с n, поэтому $\alpha(\overline{f} \circ \overline{g}) = \alpha(\overline{f})\,\alpha(\overline{g})$. □

Замечание 3. Гомоморфизм α будет иметь более естественный вид, если мы от бинарных квадратичных форм дискриминанта D известным образом перейдем к идеалам кольца $\mathcal{O}_K$, где $K = \mathbb{Q}(\sqrt{D})$. Тогда этот гомоморфизм будет просто нормой соответствующего идеала взятой по модулю $D/4$.

4.3. Вспомогательные результаты.

Теорема 4. *Пусть* $n \equiv 1 \pmod 4$, $n > 0$ *и* $\overline{f} \in Cl(-4n)$. *Тогда* $\overline{f}$ *принадлежит к главному роду тогда и только тогда, когда* $\overline{f}$ *представляет квадраты и только квадраты в* $(\mathbb{Z}/n)^{\times}$.

Доказательство. Если класс $\overline{f}$ принадлежит к главному роду, то он представляет в $(\mathbb{Z}/4n)^{\times}$ те же элементы, что и класс формы $[1, 0, n]$, а эта форма представляет все квадраты в $(\mathbb{Z}/n)^{\times}$ и ничего кроме них (необходимую информацию по теории родов можно найти в [3], глава 1, §3).

Обратно, предположим, что $\overline{f}$ представляет квадраты и только квадраты $(\mathbb{Z}/n)^{\times}$. Из китайской теоремы об остатках имеем изоморфизм $(\mathbb{Z}/4n)^{\times} \simeq (\mathbb{Z}/4)^{\times} \times (\mathbb{Z}/n)^{\times}$. Поскольку $n \equiv 1 \pmod 4$, форма $[1, 0, n]$ представляет элементы $(1, t^2)$, $t \in (\mathbb{Z}/n)^{\times}$. Предположим, что класс $\overline{f}$ представил элемент $a \equiv 3 \pmod 4$. Рассмотрим символ Якоби и напишем следующую цепочку равенств:

$$\left(\frac{-n}{a}\right) = (-1)^{\frac{a-1}{2}} \left(\frac{n}{a}\right) = -\left(\frac{a}{n}\right)(-1)^{\frac{(a-1)(n-1)}{4}} = -1.$$

Откуда следует, что $-n$ не является квадратом по модулю a, что противоречит тому, что $b^2 - ac = -n$. Поэтому класс $\overline{f}$ представляет все элементы вида $(1, t^2)$ в $(\mathbb{Z}/4)^{\times} \times (\mathbb{Z}/n)^{\times}$ и притом только их. Таким образом, $\overline{f}$ принадлежит к главному роду. □

Лемма 1. *Пусть $\nu > 0$, тогда, если в классе форм дискриминанта -4ν существует форма, которая представляет квадрат в $(\mathbb{Z}/\nu)^\times$, то данный класс представляет в $(\mathbb{Z}/\nu)^\times$ все квадраты.*

Доказательство. Пусть имеется форма $[a, 2b, c]$, где $(a,\nu) = 1$, откуда $(a, b) = 1$. Как мы уже видели, под действием

$$S = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$$

первый коэффициент квадратичной формы a переходит в $aa^2(a\alpha+b\gamma)^2 \pmod{\nu}$, поэтому достаточно доказать, что для любого $t \in (\mathbb{Z}/\nu)^\times$ разрешимо сравнение $a\alpha + b\gamma \equiv t \pmod{\nu}$, где $(\alpha, \gamma) = 1$. По взаимной простоте a и b найдем $\overline{a}$ и $\overline{b}$ такие, что $a\overline{a} + b\overline{b} = 1$. Тогда

$$a(\overline{a}t + k\nu) + b(\overline{b}t + m\nu) = t \pmod{\nu}.$$

Осталось, воспользовавшись теоремой Дирихле о простых числах в арифметической прогресии, подобрать k и m так, чтобы $\overline{a}t + k\nu$ и $\overline{b}t + m\nu$ были взаимно простыми числами.

Итак, пусть имеем $(\overline{a}, \overline{b}) = 1$, $(\overline{a}, \nu) = u_1$, $(\overline{b}, \nu) = u_2$, $(u_1, u_2) = 1$, $(t, \nu) = 1$. Пусть $t\overline{a}/u_1 + k\nu/u_1 = p_1$ и $t\overline{b}/u_2 + m\nu/u_2 = p_2$ различные простые числа, полученные с помощью теоремы Дирихле (теорема применима, поскольку $(t\overline{a}/u_1, \nu/u_1) = 1$ и $(t\overline{b}/u_2, \nu/u_2) = 1$), не участвующие в разложении u_1 и u_2. Тогда $p_1u_1 = \overline{a}t + k\nu$ и $p_2u_2 = \overline{b}t + m\nu$ искомые взаимно простые числа. □

4.4. Связь между квадратичными формами и расслоениями.

Теорема 5. *Пусть $\nu \in \mathbb{Z}$, $\nu > 0$, $\nu \equiv 1 \pmod 4$. Тогда имеется следующий естественный изоморфизм групп*

$$Cl_{vect}(\nu) \simeq Cl(-4\nu)/[2]Cl(-4\nu) \times \mathbb{Z}/2.$$

Доказательство. Рассмотрим гомоморфизм

$$\alpha : Cl(-4\nu) \to (\mathbb{Z}/\nu)^\times/((\mathbb{Z}/\nu)^\times)^2 \to 0.$$

Он является сюръекцией, поскольку по теореме 3 для заданного

$$\varepsilon \in (\mathbb{Z}/\nu)^\times/((\mathbb{Z}/\nu)^\times)^2$$

найдутся a, b, c такие, что $b^2 - ac = -\nu$, $\overline{a} = \varepsilon$ в $(\mathbb{Z}/\nu)^\times/((\mathbb{Z}/\nu)^\times)^2$ и в качестве требуемого представителя класса форм достаточно взять $[a, 2b, c]$. Он автоматически окажется допустимым, поскольку в качестве a мы выбирали простое число.

Ядро этого гомоморфизма состоит из классов форм, у которых существует представитель, первый коэффициент которого является квадратом в $(\mathbb{Z}/\nu)^\times$. По лемме 1 каждый такой класс представляет все квадраты в $(\mathbb{Z}/\nu)^\times$. Тогда, по теореме 4 это равносильно тому, что классы этих форм принадлежат к главному роду, то есть являются элементами $[2]Cl(-4\nu)$. Таким образом, $\ker\alpha = [2]Cl(-4\nu)$. Отсюда имеем следующий изоморфизм

$$Cl(-4\nu)/[2]Cl(-4\nu) \simeq (\mathbb{Z}/\nu)^\times/((\mathbb{Z}/\nu)^\times)^2,$$

откуда напрямую следует наше утверждение. Таким образом, изоморфизм

$$Cl_{vect}(\nu) \xrightarrow{\simeq} Cl(-4\nu)/[2]Cl(-4\nu) \times \mathbb{Z}/2$$

устроен так: классу оснащенного расслоения $V(\nu,\varepsilon,u)$ мы сопоставляем класс форм $[a,2b,c]$ и знак $u \in \mathbb{Z}/2$, где a представляет $\varepsilon \in (\mathbb{Z}/\nu)^\times/((\mathbb{Z}/\nu)^\times)^2$ и $4b^2 - 4ac = -4\nu$. Также, ранее фактически было проверено, что это действительно гомоморфизм групп. □

Пусть p нечетное просто число. Тогда, поскольку $\mathrm{SL}_2(\mathbb{Z})$ плотно в $\mathrm{SL}_2(\mathbb{Z}_p)$, действие последней группы вычисляется по тем же формулам и соответствует действию на бинарных квадратичных формах с коэффициентами из $\mathbb{Z}_p$. Для этого случая аналогично доказывается теорема 1. Также абсолютно аналогично определяются оснащенные расслоения и строгие изоморфизмы и доказывается соответствующая теорема классификации, которая отличается от теоремы для случая кольца $\mathbb{Z}$ только тем, что u теперь равняется не только ± 1, а пробегает всю группу единиц $\mathbb{Z}_p^\times$.

Теорема 6. *Пусть p нечетное простое, и пусть есть два расширения $\mathcal{E} = (a,b,c)$, $\mathcal{F} = (d,e,f) \in \mathrm{Ext}^1(\mathcal{O}(2),\mathcal{O}(\text{-}2))$ с равными дискриминантами $\nu = b^2 - ac = e^2 - df$. Тогда $\mathcal{E}|_{\mathbb{Z}_p} \sim \mathcal{F}|_{\mathbb{Z}_p}$ тогда и только тогда, когда $E|_{\mathbb{Z}_p}$ строго изоморфно $F|_{\mathbb{Z}_p}$.*

Доказательство. Если два расширения эквивалентны, то соответствующие расслоения изоморфны по теореме 1 и более того, легко проверяется, что они строго изоморфны (все рассуждения над $\mathbb{Z}$ дословно переносятся на случай расслоений над $\mathbb{Z}_p$).

Предположим теперь, что расслоения

$$E|_{\mathbb{Z}_p} = V(\nu,\alpha_1)|_{\mathbb{Z}_p} \quad \text{и} \quad F|_{\mathbb{Z}_p} = V(\nu,\alpha_2)|_{\mathbb{Z}_p}$$

строго изоморфны и p делит ν. Тогда $\left(\frac{\alpha_1}{p}\right) = \left(\frac{\alpha_2}{p}\right)$, следовательно

$$\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right).$$

Перейдем от элементов $\mathrm{Ext}^1(\mathcal{O}(2), \mathcal{O}(\text{-}2))$, $\mathcal{E}$ и $\mathcal{F}$ к квадратичным формам $[a, 2b, c]$ и $[d, 2e, f]$ соответственно. Легко проверить, что они эквивалентны $[a, 0, -\nu/a]$ и $[d, 0, -\nu/d]$ соответственно, из теории целых квадратичных форм над $\mathbb{Z}_p$ следует, что они эквивалентны тогда и только тогда, когда

$$\left(\frac{a}{p}\right) = \left(\frac{d}{p}\right)$$

(более подробно см. [4, глава 4]). Тогда матрицы из $\mathrm{SL}_2(\mathbb{Z}_p)$, осуществляющие эту эквивалентность, дадут нам эквивалентность расширений $\mathcal{E}$ и $\mathcal{F}$.

Если p не делит ν, то теорема верна, поскольку соответствующие квадратичные формы $[a, 2b, c]$ и $[d, 2e, f]$ имеют одинаковый дискриминант, который в свою очередь является единицей $\mathbb{Z}_p$, поэтому они эквивалентны. $\square$

Список литературы

1. A. L. Smirnov, *On filtrations of vector bundles over* $\mathbb{P}^1_{\mathbb{Z}}$. — Arithmetic and Geometry, London Math. Soc. Lect. Note Series **420** (2015), 436–457.
2. А. Л. Смирнов, *Векторные расслоения на* $\mathbb{P}^1_{\mathbb{Z}}$ *с простыми подскоками.* — Зап. научн. семин. ПОМИ **452** (2016), 202–217.
3. D. A. Cox, *Primes of the Form* x^2+ny^2*: Fermat, Class Field Theory, and Complex Multiplication*, Monographs and textbooks in pure and applied mathematics, Wiley, 1989.
4. B. W. Jones, *The Arithmetic Theory of Quadratic Forms*, Mathem. Association of America, vol. 10, 1950.

Polyakov V. M. Rank 2 vector bundles on $\mathbb{P}^1_{\mathbb{Z}}$ and quadratic forms.

We study the action of the group $\mathrm{SL}_2(\mathbb{Z})$ on $\mathrm{Ext}^1(\mathcal{O}(2), \mathcal{O}(-2))$ and on isomorphism classes of vector bundles on $\mathbb{P}^1_{\mathbb{Z}}$ of rank 2 with a trivial generic fiber and simple jumps. It is proved that such bundles are equivariant under the action of this group. The concept of a rigged bundle is introduced and studied. It is shown that the group of isomorphism classes of rigged bundles of rank 2 with a trivial generic fiber and simple jumps is isomorphic to

the 2-torsion quotient of the class group of binary quadratic forms of the corresponding discriminant up to a $\mathbb{Z}/2$ factor.

С.-Петербургское
отделение Математического
института им. В. А. Стеклова РАН, Фонтанка 27,
191023 Санкт-Петербург, Россия
E-mail: polyakov@pdmi.ras.ru

Поступило 25 октября 2023 г.