Записки научных
семинаров ПОМИ
Том 330, 2006 г.

М. А. Всемирнов

ЯВЛЯЕТСЯ ЛИ ГРУППА $\mathrm{SL}(6,\mathbb{Z})$ $(2,3)$-ПОРОЖДЕННОЙ?

1. Введение

Группа называется $(2,3)$-*порожденной,* если она порождается инволюцией и элементом порядка три. Таким образом, $(2,3)$-порожденные группы являются гомоморфными образами группы $\mathrm{PSL}(2,\mathbb{Z}) \simeq (\mathbb{Z}/2\mathbb{Z}) * (\mathbb{Z}/3\mathbb{Z})$.

Имеется обширная литература, посвященная $(2,3)$-порожденным группам. Читатель может найти дополнительную информацию в обзорах [1, 2]; см. также приведенный в них список литературы. Особое внимание уделялось проблеме, будут ли $(2,3)$-порожденными классические матричные группы над различными кольцами; см., например, [3, 4] для $\mathrm{SL}(n,q)$, [10] для $\mathrm{SL}(n,\mathbb{Z})$, $\mathrm{GL}(n,\mathbb{Z})$, а также [12, 13].

П. Санкини и М. К. Тамбурини [10] доказали, что группы $\mathrm{SL}(n,\mathbb{Z})$ при $n \geqslant 13$ и $\mathrm{GL}(n,\mathbb{Z})$ при $n \geqslant 19$ будут $(2,3)$-порожденными. С другой стороны, хорошо известно, что группы $\mathrm{SL}(n,\mathbb{Z})$, $\mathrm{GL}(n,\mathbb{Z})$ при $n = 2, 4$ не являются $(2,3)$-порожденными. В случае $n = 4$ это утверждение следует, например, из давнего результата Г. А. Миллера [8], утверждающего, что группа $\mathrm{GL}(4,2) \simeq \mathrm{SL}(4,2) \simeq \mathrm{Alt}(8)$ не $(2,3)$-порождена. Недавно М.К. Тамбурини и П. Цукка [14] показали, что группы $\mathrm{SL}(3,\mathbb{Z})$, $\mathrm{GL}(3,\mathbb{Z})$ не являются $(2,3)$-порожденными. Этот же результат был независимо переоткрыт в [9].

В статье [7] А. Лузгарев и И. Певзнер обратились к вопросу, будет ли $(2,3)$-порожденной группа $\mathrm{GL}(5,\mathbb{Z})$. Хотя они и не дали окончательный ответ, им удалось свести задачу к анализу конечного числа случаев.

Целью настоящей статьи является анализ следующей размерности, а именно $n = 6$. В отличие от случая $n = 4$, здесь не

При поддержке приграммы фундаментальных исследований РАН "Современные проблемы теоретической математики" и Федерального агентства по науке и инновациям (гос. контракт №02.442.11.7291).

имеется тривиальных препятствий для $(2,3)$-порожденности, поскольку группы $\mathrm{SL}(6,p)$ являются $(2,3)$-порожденными для всех простых p (см. [3]).

Ясно, что ответ на вопрос, порождает ли данная пара матриц группу $\mathrm{SL}(6,\mathbb{Z})$, зависит лишь от класса $\mathrm{GL}(6,\mathbb{Z})$-сопряженности данной пары. Поэтому в дальнейшем нас будут интересовать пары матриц с точностью до одновременного $\mathrm{GL}(6,\mathbb{Z})$-сопряжения. Основным результатом данной работы является следующая редукционная теорема. (Здесь и далее I_n обозначает квадратную единичную матрицу размера n.)

Теорема 1. *Пусть $\tilde{X}, \tilde{Y} \in \mathrm{SL}(6,\mathbb{Z})$ и $\tilde{X}^2 = \tilde{Y}^3 = I_6$. Предположим также, что пара $\tilde{X}, \tilde{Y}$ не сопряжена в $\mathrm{GL}(6,\mathbb{Z})$ ни с одной из пар $\pm X$, Y вида*

$$X = \begin{pmatrix} 0 & I_2 & B \\ I_2 & 0 & -B \\ 0 & 0 & I_2 \end{pmatrix}, \qquad Y = \begin{pmatrix} I_2 & 0 & A \\ 0 & 0 & -I_2 \\ 0 & I_2 & -I_2 \end{pmatrix}, \tag{1}$$

где

$$A = \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix}, \qquad B = \begin{pmatrix} b_1 & b_2 \\ b_3 & b_4 \end{pmatrix}, \tag{2}$$

а $(b_1, b_2, b_3, b_4, a_1, a_2, a_3, a_4)$ – один из следующих наборов:

$$(0,0,0,1,3,1,1,-3), \qquad (1,-1,-1,-4,-3,1,1,3), \tag{3}$$
$$(1,0,0,2,-3,1,1,3), \qquad (-6,-1,-1,1,3,1,1,-3), \tag{4}$$
$$(0,0,0,1,3,1,-1,-3), \qquad (1,-1,1,-4,-3,1,-1,3), \tag{5}$$
$$(1,0,0,2,-3,1,-1,3), \qquad (-6,-1,1,1,3,1,-1,-3), \tag{6}$$
$$(0,2,-2,-3,3,1,-1,1), \qquad (1,-3,3,-4,1,1,-1,3), \tag{7}$$
$$(1,4,-4,-6,5,1,-1,3), \qquad (2,-5,5,-7,3,1,-1,5), \tag{8}$$
$$(-2,1,-1,-2,3,1,-1,2), \qquad (-1,-2,2,-2,2,1,-1,3), \tag{9}$$
$$(-4,2,-2,-1,3,1,-1,4), \qquad (-4,-3,3,0,4,1,-1,3). \tag{10}$$

Тогда группа $\langle \tilde{X}, \tilde{Y} \rangle$ не совпадает с $\mathrm{SL}(6,\mathbb{Z})$.

Замечание 1. Очевидно, что если $\langle X, Y \rangle = \mathrm{SL}(6,\mathbb{Z})$, то и $\langle X, Y^{-1} \rangle = \mathrm{SL}(6,\mathbb{Z})$. Наборы в (3)–(10) сгруппированы таким образом, что если пара X_1, Y_1 вида (1)–(2) отвечает первому набору в строке, а X_2, Y_2 отвечает второму набору, то пары X_2,

Y_2 и X_1, Y_1^{-1} сопряжены при помощи матрицы из $\mathrm{GL}(6,\mathbb{Z})$. Таким образом, достаточно проверить имеет ли место равенство $\langle X, Y\rangle = \mathrm{SL}(6,\mathbb{Z})$ только в восьми случаях вместо 16. (По поводу выбора знака в $\pm X$ см. также лемму 1 далее.)

Замечание 2. Пусть X, Y заданы при помощи (1)–(2), где $(b_1, b_2, b_3, b_4, a_1, a_2, a_3, a_4)$ – один из наборов, перечисленных в (3)–(10). Для всякого простого p можно рассмотреть $X \bmod p$, $Y \bmod p$ как матрицы из $\mathrm{SL}(6,p)$. Компьютерные вычисления свидетельствуют в пользу следующей гипотезы: группа, порожденная матрицами $X \bmod p$ и $Y \bmod p$, совпадает с $\mathrm{SL}(6,p)$. Таким образом, весьма маловероятно, что методы данной работы могут быть использованы для исключения случаев (3)–(10). Используя принципиально другой подход, автор сумел исключить случаи (4) и (6). Этому результату будет посвящена отдельная публикация.

Статья организована следующим образом. В §2 мы изучим потенциальные пары (2, 3)-образующих группы $\mathrm{SL}(6,\mathbb{Z})$ с точностью до $\mathrm{GL}(6,\mathbb{Z})$-сопряжения и найдем их допустимую форму. Отметим, что результаты §2 верны не только для $\mathrm{SL}(6,\mathbb{Z})$, но и для более широкого класса групп; см. условия (A1)–(A5) ниже. Элементы допустимых матриц будут зависеть от восьми целочисленных параметров. В §3 и §4 мы найдем полиномиальные соотношения, которым они должны удовлетворять. Соответствующие уравнения будут решены в §5 и §6.

В завершение этого параграфа мы введем следующие обозначения. Как обычно, $\mathbb{F}_p$ обозначает конечное поле из p элементов, а $\bar{\mathbb{F}}_p$ обозначает его алгебраическое замыкание. Для всякого простого p пусть $f_p : \mathbb{Z} \to \mathbb{F}_p$ есть естественный гомоморфизм редукции по модулю p. Он естественным образом распространяется на целочисленные векторы и матрицы. Используя некоторую вольность в обозначениях, мы сохраняем символ f_p и для этих расширенных обозначений, то есть

$$f_p : \mathbb{Z}^n \to \mathbb{F}_p^n, \qquad f_p : \mathrm{Mat}\,(n,\mathbb{Z}) \to \mathrm{Mat}\,(n,\mathbb{F}_p).$$

2. Допустимые образующие

В этом параграфе мы найдем вид потенциальных пар (2,3)-образующих группы $\mathrm{SL}(6,\mathbb{Z})$. Пусть $X, Y \in \mathrm{SL}(6,\mathbb{Z})$. На протяжении этого параграфа мы предполагаем, что X и Y удовлетворяют следующим условиям:

(A1) $X^2 = Y^3 = I_6$;

(A2) группа $\langle X, Y\rangle$ совершенна;

(A3) $-I_6 \in \langle X, Y\rangle$;

(A4) группа $\langle X, Y\rangle$ является абсолютно неприводимой подгруппой в $\mathrm{SL}(6, \mathbb{Q})$;

(A5) для всякого простого p группа $\langle f_p(X), f_p(Y)\rangle$ абсолютно неприводима.

В частности, любая пара (2,3)-образующих (если таковая имеется) группы $\mathrm{SL}(6, \mathbb{Z})$ должна удовлетворять условиям (A1)–(A5). Выполнение условия (A2) в случае $\langle X, Y\rangle = \mathrm{SL}(6, \mathbb{Z})$ см., например, в [5, 1.2.11 и 1.2.15].

Предположение (A4) влечет, что $X \neq \pm I_6$. Напомним также, что $\det X = 1$ и $X^2 = 1$. Следовательно, матрица X сопряжена в $\mathrm{GL}(6, \mathbb{Q})$ с одной из матриц

$$\mathrm{diag}\,(1, 1, 1, 1, -1, -1), \quad \text{или} \quad \mathrm{diag}\,(1, 1, -1, -1, -1, -1).$$

Следующая лемма позволяет рассматривать только одну возможность для X вместо двух.

Лемма 1. *Если группа* $\langle X, Y\rangle$ *удовлетворяет* (A2), (A3), *то* $\langle -X, Y\rangle = \langle X, Y\rangle$.

Доказательство. Согласно (A3) имеем $\langle -X, Y\rangle \subseteq \langle X, Y\rangle$. Согласно (A2) всякая матрица g из $\langle X, Y\rangle$ может быть представлена в виде

$$g = \prod_{i=1}^{m} [g_{2i-1}(X, Y), g_{2i}(X, Y)]\,,$$

где g_1, …, g_{2m} – это слова в алфавите X, X^{-1}, Y, Y^{-1}. Для всякого j справедливо $g_j(X, Y) = \pm g_j(-X, Y)$. Следовательно, $[g_{2i-1}(X, Y), g_{2i}(X, Y)] = [g_{2i-1}(-X, Y), g_{2i}(-X, Y)]$. Значит, $\langle X, Y\rangle \subseteq \langle -X, Y\rangle$, откуда и следует утверждение. □

Таким образом, не умаляя общности, можно предполагать, что матрица X сопряжена в $\mathrm{GL}(6, \mathbb{Q})$ с $\mathrm{diag}\,(1, 1, 1, 1, -1, -1)$.

Согласно (A4), $Y \neq I_6$. Так как $Y^3 = I_6$, то матрица Y сопряжена в $\mathrm{GL}(6, \mathbb{Q})$ с одной из блочно-диагональных матриц

$$\mathrm{diag}\,(1, 1, J, J), \quad \mathrm{diag}\,(1, 1, 1, 1, J), \quad \mathrm{diag}\,(J, J, J),$$

где

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

Для того чтобы исключить две последние возможности, нам потребуется вариант формулы, принадлежащей Л. Л. Скотту [11]. Введем следующие обозначения. Пусть $G = \langle x, y\rangle$ – группа, а F – некоторое поле. Пусть M – конечномерный FG-модуль, а $\phi : G \to \mathrm{GL}(M)$ – представление группы G. Для $H \subseteq G$ через d_M^H обозначим размерность подпространства в M, поточечно фиксируемого каждым элементом из H:

$$d_M^H = \dim\{v \in M : \phi(g)v = v \quad \text{для любых} \quad g \in H\}.$$

Аналогичным образом определим размерность $\hat{d}_M^H$, отвечающую двойственному представлению $\hat{\phi} : G \to \mathrm{GL}(M)$, $\hat{\phi}(g) = (\phi(g^{-1}))^t$:

$$\hat{d}_M^H = \dim\{v \in M : \hat{\phi}(g)v = v \quad \text{для любых} \quad g \in H\}.$$

Теорема 2 (Скотт, [11]). *В вышеприведенных обозначениях имеем*

$$d_M^{\{x\}} + d_M^{\{y\}} + d_M^{\{xy\}} \leqslant \dim_F M + d_M^G + \hat{d}_M^G.$$

Мы применим эту теорему в случае, когда $x = X$, $y = Y$, а $G = \langle X, Y\rangle$ – абсолютно неприводимая подгруппа в $\mathrm{SL}\,(6, \mathbb{Z})$ (или $\mathrm{SL}\,(6, \mathbb{Q})$). Пусть $M = \mathrm{Mat}(6, \mathbb{Q})$ – это пространство 6×6 матриц над $\mathbb{Q}$. Группа G действует на M посредством сопряжения. В этом случае $d_M^H = \dim C_M(H)$, где $C_M(H)$ – это централизатор H в M. Предположение (A4), утверждающее абсолютную неприводимость группы G, влечет, что $d_M^G = \hat{d}_M^G = 1$, поскольку соответствующие централизаторы состоят из скалярных матриц. Таким образом, формула Скотта приобретает вид

$$d_M^{\{X\}} + d_M^{\{Y\}} + d_M^{\{XY\}} \leqslant 6^2 + 2 = 38. \tag{11}$$

Для произвольного $g \in G$, размерность $d_M^{\{g\}}$ (то есть $\dim C_M(g)$) может быть вычислена в терминах степеней нетривиальных инвариантных множителей матрицы $tI_6 - g$.

Лемма 2([6, с. 207]). *Пусть $g \in \mathrm{GL}(n, F)$, и пусть $n_1 \leqslant \cdots \leqslant n_s$ – степени нетривиальных инвариантных множителей матрицы $tI_n - g$, расположенные в порядке возрастания. Тогда*

$$\dim C_{\mathrm{Mat}(n,F)}(g) = (2s+1)n - 2\sum_{j=1}^{s} jn_j = n + 2\sum_{j=1}^{s}(s-j)n_j.$$

Следствие 1. $\dim C_{\mathrm{Mat}(n,F)}(g) \geqslant n$.

Предполагая, что матрица X подобна $\operatorname{diag}(1,1,1,1,-1,-1)$, имеем $d_M^{\{X\}} = 20$. По следствию 1, имеем $d_M^{\{XY\}} \geqslant 6$. Из (11) вытекает, что $d_M^{\{Y\}} \leqslant 12$. Следовательно, матрица Y не может быть подобна ни $\operatorname{diag}(1,1,1,1,J)$, ни $\operatorname{diag}(J,J,J)$, так как в этих случаях $d_M^{\{Y\}} = 18$. Следовательно, матрица Y сопряжена с $\operatorname{diag}(1,1,J,J)$. В частности, пространство собственных векторов матрицы Y, отвечающих собственному числу 1, двумерно. Обозначим это пространство через $V_{\mathbb{Q}}$:

$$V_{\mathbb{Q}} = \{v \in \mathbb{Q}^6 : Yv = v\}.$$

Положим $V_{\mathbb{Z}} = V_{\mathbb{Q}} \cap \mathbb{Z}^6$. Пусть v_1 и v_2 образуют $\mathbb{Z}$-базис решетки $V_{\mathbb{Z}}$.

Так как характеристический многочлен Y равен $(t^3-1)^2$, то пространство собственных векторов матрицы $f_p(Y)$, отвечающее собственному числу 1, также двумерно, если $p \neq 3$. Следовательно, оно совпадает с $f_p(V_{\mathbb{Z}})$.

Если $p = 3$, то мы приходим к тому же выводу на основании формулы Скотта. А именно, возьмем $x = f_3(X)$, $y = f_3(Y)$, $G = \langle f_3(X), f_3(Y)\rangle$, $M = \mathrm{Mat}(6, \mathbb{F}_3)$. Группа G действует на M посредством сопряжения. Так как характеристический многочлен X равен $(t-1)^4(t+1)^2$, то его редукция по модулю 3 имеет такие же кратности корней. Следовательно, $d_M^{\{f_3(X)\}} = 20$. Действуя аналогично тому, как мы поступали выше, получаем, что $d_M^{\{f_3(Y)\}} \leqslant 12$. Из леммы 2 следует, что инвариантные множители матрицы $tI_6 - f_3(Y)$ должны иметь вид t^3-1, t^3-1. Следовательно, пространство собственных векторов матрицы $f_3(Y)$, отвечающих собственному числу 1, двумерно и совпадает с $f_3(V_{\mathbb{Z}})$ также и в этом случае.

Лемма 3. *Предположим, что матрицы* $X, Y \in \mathrm{SL}(6,\mathbb{Z})$, X *подобна матрице* $\operatorname{diag}(1,1,1,1,-1,-1)$ *и* X, Y *удовлетворяют* (A1), (A4), (A5)*. Тогда*

(a) *множество* $\mathcal{B}_0 = \{v_1, v_2, Xv_1, Xv_2\}$ *является* $\mathbb{Z}$*-базисом решетки* $(V_{\mathbb{Q}} + XV_{\mathbb{Q}}) \cap \mathbb{Z}^6$*;*

(b) *множество* $\mathcal{B} = \{v_1, v_2, Xv_1, Xv_2, YXv_1, YXv_2\}$ *является* $\mathbb{Z}$*-базисом решетки* $\mathbb{Z}^6$*. В частности, в этом базисе матрицы* X *и* Y *приобретают вид* (1)*, где* A*,* B *заданы согласно* (2) *при некоторых целых числах* $a_1, \ldots, a_4$*,* $b_1, \ldots, b_4$*.*

Доказательство. Мы воспользуемся следующим хорошо известным критерием. Пусть W – подпространство $\mathbb{Q}^n$, а $w_1, \dots, w_k \in W \cap \mathbb{Z}^n$. Множество $\{w_1, \dots, w_k\}$ будет $\mathbb{Z}$-базисом решетки $W \cap \mathbb{Z}^n$ в том и только в том случае, когда $\{w_1, \dots, w_k\}$ – $\mathbb{Q}$-базис пространства W и для всякого простого p векторы $f_p(w_1), \dots, f_p(w_k)$ линейно независимы над $\mathbb{F}_p$.

(a) Согласно (A4) группа $\langle X, Y\rangle$ абсолютно неприводима. Поскольку пространство $V_{\mathbb{Q}} \cap XV_{\mathbb{Q}}$ является X- и Y-инвариантным, мы заключаем, что $V_{\mathbb{Q}} \cap XV_{\mathbb{Q}} = \{0\}$. Следовательно,

$$\dim(V_{\mathbb{Q}} + XV_{\mathbb{Q}}) = 4.$$

В частности, $\mathcal{B}_0$ – $\mathbb{Q}$-базис пространства $V_{\mathbb{Q}} + XV_{\mathbb{Q}}$. Также отметим, что векторы из $\mathcal{B}_0$ являются целочисленными.

Согласно (A5) группа $\langle f_p(X), f_p(Y)\rangle$ абсолютно неприводима. Так как пространство $f_p(V_{\mathbb{Z}})$ двумерно и $f_p(Y)$-инвариантно, рассуждения, аналогичные приведенным выше, дают, что для всякого простого p

$$\dim_{\mathbb{F}_p}(f_p(V_{\mathbb{Z}}) + f_p(XV_{\mathbb{Z}})) = 4$$

и векторы $f_p(v_1)$, $f_p(v_2)$, $f_p(Xv_1)$, $f_p(Xv_2)$ линейно независимы над $\mathbb{F}_p$. Применяя указанный выше критерий, мы заключаем, что $\mathcal{B}_0$ является $\mathbb{Z}$-базисом решетки $(V_{\mathbb{Q}} + XV_{\mathbb{Q}}) \cap \mathbb{Z}^6$ и

$$(V_{\mathbb{Q}} + XV_{\mathbb{Q}}) \cap \mathbb{Z}^6 = V_{\mathbb{Z}} + XV_{\mathbb{Z}}. \tag{12}$$

Это завершает доказательство первого утверждения.

(b) Так как матрица X подобна $\mathrm{diag}(1,1,1,1,-1,-1)$, а

$$\dim(V_{\mathbb{Q}} + XV_{\mathbb{Q}}) = 4,$$

то X индуцирует тождественное отображение на $\mathbb{Q}^6/(V_{\mathbb{Q}} + XV_{\mathbb{Q}})$. Следовательно, всякое надпространство пространства $V_{\mathbb{Q}} + XV_{\mathbb{Q}}$ будет X-инвариантным.

Поскольку $Y^3 = I_6$, для всякого вектора $u \in \mathbb{Q}^6$ имеем

$$Y^2u + Yu + u \in V_{\mathbb{Q}}. \tag{13}$$

В частности, для всякого подпространства $U \subseteq \mathbb{Q}^6$ пространство $YU + U + V_{\mathbb{Q}}$ будет Y-инвариантным.

Объединяя вместе эти два результата, мы получаем, что пространство $YXV_{\mathbb{Q}} + XV_{\mathbb{Q}} + V_{\mathbb{Q}}$ является X- и Y-инвариантным. Абсолютная неприводимость группы $\langle X, Y\rangle$ влечет, что $YXV_{\mathbb{Q}} + XV_{\mathbb{Q}} + V_{\mathbb{Q}}$ совпадает с $\mathbb{Q}^6$, а $\mathcal{B}$ есть $\mathbb{Q}$-базис пространства $\mathbb{Q}^6$.

Напомним, что X индуцирует тождественное отображение на $\mathbb{Q}^6/(V_{\mathbb{Q}} + XV_{\mathbb{Q}})$. Также напомним равенство (12). Таким образом, для всякого $u \in \mathbb{Z}^6$ справедливо

$$Xu - u \in (V_{\mathbb{Q}} + XV_{\mathbb{Q}}) \cap \mathbb{Z}^6 = V_{\mathbb{Z}} + XV_{\mathbb{Z}}. \tag{14}$$

Следовательно, X индуцирует тождественное отображение на $\mathbb{Z}^6/(V_{\mathbb{Z}} + XV_{\mathbb{Z}})$, и $f_p(X)$ индуцирует тождественное отображение на $\mathbb{F}_p^6/(f_p(V_{\mathbb{Z}}) + f_p(XV_{\mathbb{Z}}))$. В частности, всякое надпространство пространства $f_p(V_{\mathbb{Z}}) + f_p(XV_{\mathbb{Z}})$ будет $f_p(X)$-инвариантным.

Так как $Y^3 = I_6$, то для всякого $u \in \mathbb{F}_p^6$ вектор $f_p(Y^2)u + f_p(Y)u + u$ является неподвижным вектором для $f_p(Y)$. Напомним, что для всякого простого p пространство собственных векторов матрицы $f_p(Y)$, отвечающих собственному числу 1, совпадает с $f_p(V_{\mathbb{Z}})$. Следовательно,

$$f_p(Y^2)u + f_p(Y)u + u \in f_p(V_{\mathbb{Z}}).$$

Используя абсолютную неприводимость группы $\langle f_p(X), f_p(Y)\rangle$ и рассуждения, аналогичные аргументам в случае характеристики 0, мы получаем, что $f_p(YXV_{\mathbb{Z}}) + f_p(XV_{\mathbb{Z}}) + f_p(V_{\mathbb{Z}}) = \mathbb{F}_p^6$. Следовательно, для всякого p векторы $f_p(v_1)$, $f_p(v_2)$, $f_p(Xv_1)$, $f_p(Xv_2)$, $f_p(YXv_1)$, $f_p(YXv_2)$ линейно независимы. Применяя упомянутый выше критерий, заключаем, что $\mathcal{B}$ является $\mathbb{Z}$-базисом решетки $\mathbb{Z}^6$.

Применим включение (13) к $u = Xv_i$, $i = 1, 2$, и заметим, что векторы в левой части целочисленные. В частности,

$$Y(YXv_i) + YXv_i + Xv_i \in V_{\mathbb{Q}} \cap \mathbb{Z}^6 = V_{\mathbb{Z}}.$$

Таким образом, эти векторы являются линейными комбинациями векторов v_1 и v_2 с целыми коэффициентами. Следовательно, в базисе $\mathcal{B}$ матрица Y приобретает вид (1)–(2) для некоторых целых чисел a_1, a_2, a_3, a_4.

Согласно (14) матрица X в том же самом базисе приобретает вид

$$X = \begin{pmatrix} 0 & I_2 & B \\ I_2 & 0 & B' \\ 0 & 0 & I_2 \end{pmatrix}$$

для некоторых целочисленных матриц B, B'. Так как $X^2 = I_6$, то $B' = -B$. Тем самым мы завершаем доказательство. □

Замечание 3. Матрицы X и Y можно одновременно заменить на сопряженные при помощи $\mathrm{diag}(g, g, g)$, где $g \in \mathrm{GL}(2, \mathbb{Z})$. В случае произвольных матриц A и B выигрыш невелик, поскольку имеется бесконечно много классов $\mathrm{GL}(2, \mathbb{Z})$-сопряженности. Однако мы вернемся к этому преобразованию позднее, когда мы установим дополнительные соотношения между A и B; см. §4.

3. Неприводимость

В этом параграфе мы предполагаем, что $X, Y \in \mathrm{SL}(6, \mathbb{Z})$ и что они удовлетворяют (1)–(2) и (A4), (A5). Наша цель состоит в нахождении дальнейших ограничений на $a_1, \ldots, a_4$ и $b_1, \ldots, b_4$.

Лемма 4. *Пусть F – алгебраически замкнутое поле, и пусть $A, B \in \mathrm{Mat}(2, F)$. Матрицы A и B обладают общим ненулевым собственным вектором в том и только в том случае, когда $\det(AB - BA) = 0$.*

Доказательство. *Необходимость.* Если $v \neq 0$ и $Av = \lambda v$, $Bv = \mu v$, то $(AB-BA)v = (\lambda\mu - \mu\lambda)v = 0$. Следовательно, $\det(AB-BA) = 0$.

Достаточность. Одновременно сопрягая обе матрицы, если необходимо, мы можем предполагать, не умаляя общности, что A совпадает со своей жордановой нормальной формой. Запишем B в виде $B = \left(\begin{smallmatrix} b_1 & b_2 \\ b_3 & b_4 \end{smallmatrix}\right)$.

Случай 1: $A = \mathrm{diag}(\lambda, \lambda)$. В этом случае всякий собственный вектор матрицы B будет также и собственным вектором для A.

Случай 2: $A = \left(\begin{smallmatrix} \lambda_1 & 0 \\ 0 & \lambda_2 \end{smallmatrix}\right)$, $\lambda_1 \neq \lambda_2$. Непосредственно проверяется, что

$$AB - BA = \begin{pmatrix} 0 & (\lambda_1 - \lambda_2)b_2 \\ (\lambda_2 - \lambda_1)b_3 & 0 \end{pmatrix}.$$

Так как $\det(AB - BA) = 0$ и $\lambda_1 - \lambda_2 \neq 0$, то заключаем, что либо $b_2 = 0$, либо $b_3 = 0$. В первом случае общим собственным вектором будет $(0,1)^t$, во втором – $(1,0)^t$.

Случай 3: $A = \left(\begin{smallmatrix} \lambda & 1 \\ 0 & \lambda \end{smallmatrix}\right)$. Непосредственно проверяется, что

$$AB - BA = \begin{pmatrix} b_3 & b_4 - b_1 \\ 0 & -b_3 \end{pmatrix}.$$

Следовательно, $b_3 = 0$, и $(1,0)^t$ будет общим собственным вектором для A и B. □

Лемма 5. *Для целых чисел* $a_1, \dots, a_4$, $b_1, \dots, b_4$ *определим* A, B *согласно* (2) *и* X, Y *согласно* (1). *Предположим, что* X, Y *удовлетворяют* (A5). *Тогда* $\det(AB - BA) = \pm 1$.

Доказательство. Предположим, что $\det(AB - BA) \neq \pm 1$. Пусть p – простое число, делящее $\det(AB - BA)$. Согласно лемме 4 в $\bar{\mathbb{F}}_p^2$ существует ненулевой собственный вектор $(\alpha, \beta)^t$, общий для $f_p(A)$ и $f_p(B)$. Положим $u_1 = (\alpha, \beta, 0, 0, 0, 0)^t$, $u_2 = (0, 0, \alpha, \beta, 0, 0)^t$, $u_3 = (0, 0, 0, 0, \alpha, \beta)^t$. Непосредственно проверяется, что $\langle u_1, u_2, u_3 \rangle$ является $\langle f_p(X), f_p(Y) \rangle$-инвариантным подпространством. Получаем противоречие с (A5). $\square$

Лемма 6. *Для целых чисел* $a_1, \dots, a_4$, $b_1, \dots, b_4$ *определим* A, B *согласно* (2) *и* X, Y *согласно* (1). *Положим*

$$s_0 = a_1a_4 - a_2a_3 - 3a_1 - 3a_4 + 9 = \det(A - 3I_2). \tag{15}$$

Предположим, что X, Y *удовлетворяют* (A5). *Тогда* $s_0 = \pm 1$.

Доказательство. Предположим, что $s_0 \neq \pm 1$, и выберем простое число p, делящее $s_0 = \det(A - 3I_2)$. В частности, найдется ненулевой вектор $(\alpha, \beta)^t \in \mathbb{F}_p^2$, такой, что

$$f_p(A^t - 3I_2) \begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}. \tag{16}$$

Используя (16), убеждаемся, что вектор $(\alpha, \beta, \alpha, \beta, \alpha, \beta)^t$ является $f_p(X^t)$- и $f_p(Y^t)$-инвариантным. В частности, $\langle f_p(X^t), f_p(Y^t) \rangle$ обладает одномерным инвариантным подпространством. Следовательно, $\langle f_p(X), f_p(Y) \rangle$ обладает инвариантным подпространством размерности 5, что противоречит (A5). $\square$

Лемма 7. *Для целых чисел* $a_1, \dots, a_4$, $b_1, \dots, b_4$ *определим* A, B *согласно* (2) *и* X, Y *согласно* (1). *Положим*

$$\begin{aligned} s_1 = {} & a_1a_4 - a_2a_3 + a_1b_4 + b_1a_4 - a_2b_3 - a_3b_2 + 2a_1 + 2a_4 \\ & + 3b_1 + 3b_4 + 3, \end{aligned} \tag{17}$$

$$s_2 = -a_1b_4 - b_1a_4 + a_3b_2 + a_2b_3 - 3b_1b_4 + 3b_2b_3 + a_1 + a_4 + 3. \tag{18}$$

Предположим, что X, Y *удовлетворяют* (A5). *Тогда*

$$(s_1, s_2) \in \{(1,0), (0,1), (1,1), (-1,0), (0,-1), (-1,-1)\}. \tag{19}$$

Доказательство. Прежде всего, мы покажем, что $s_1^2-s_1s_2+s_2^2=1$. Предположим противное. Так как число $s_1^2-s_1s_2+s_2^2$ всегда неотрицательно, то найдется простое число p, делящее $s_1^2-s_1s_2+s_2^2$.

Рассмотрим следующую систему

$$\begin{cases} f_p(3I_2+A)w_1+f_p(A-AB)w_2=0, \\ f_p(I_2-B)w_1+f_p(I_2+A+B+B^2)w_2=0, \end{cases} \tag{20}$$

где четырьмя неизвестными являются координаты векторов w_1 и w_2. Непосредственно проверяется, что определитель этой системы есть в точности $s_1^2-s_1s_2+s_2^2 \pmod{p}$. Таким образом, (20) имеет нетривиальное решение w_1, w_2.

Теперь положим

$$u_1=\begin{pmatrix} w_1 \\ w_1-f_p(B)w_2 \\ w_2 \end{pmatrix}, \qquad u_2=\begin{pmatrix} w_1+f_p(A)w_2 \\ -w_2 \\ w_1-f_p(B)w_2-w_2 \end{pmatrix}.$$

Очевидно, что $f_p(X)u_1=u_1$, $f_p(Y)u_1=u_2$. Из второго уравнения в (20) следует, что $f_p(X)u_2=u_2$, а из первого уравнения в (20) следует, что $f_p(Y)u_2=-u_1-u_2$. Следовательно, u_1 и u_2 порождают двумерное $\langle f_p(X), f_p(Y)\rangle$-инвариантное подпространство, что противоречит (A5). Следовательно, $s_1^2-s_1s_2+s_2^2=1$. Так как s_1 и s_2 – целые числа, мы заключаем, что выполнено (19). □

В действительности, значения s_0, s_1 и s_2 не являются независимыми. Из (15), (17), (18) следует, что $s_1+s_2-s_0\equiv 0 \pmod 3$. Объединяя это сравнение с леммами 6 и 7, мы получаем следующий результат.

Лемма 8. *В предположениях лемм 6 и 7 мы дополнительно имеем* $(s_0,s_1,s_2)\in S$, *где*

$$\begin{aligned} S=\{&(1,1,0),(1,0,1),(-1,1,1),\\ &(-1,-1,0),(-1,0,-1),(1,-1,-1)\}. \end{aligned} \tag{21}$$

4. Дальнейшие упрощения

Мы сохраняем обозначения предыдущего параграфа. Положим $C=AB-BA$. Очевидно, что $\mathrm{trace}(C)=0$. Согласно лемме 5 имеем $\det C=\pm 1$. Наша следующая цель состоит в нахождении матрицы наиболее простого вида, сопряженной с C в $\mathrm{GL}(2,\mathbb{Z})$.

Лемма 9. (a) *Пусть* $C \in \mathrm{Mat}(2, \mathbb{Z})$. *Если* $\mathrm{trace}(C) = 0$ *и* $\det C = \pm 1$, *то матрица* C *сопряжена в* $\mathrm{GL}(2, \mathbb{Z})$ *с одной из следующих матриц:*

$$C_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \qquad C_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad C_3 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}. \tag{22}$$

(b) *В обозначениях леммы 5 предположим дополнительно, что* $\langle X, Y \rangle = \mathrm{SL}(6, \mathbb{Z})$. *Тогда, не умаляя общности, можно считать, что* $AB - BA$ *совпадает с одной из матриц* C_1, C_2, C_3.

Замечание 4. Матрица C_3 не сопряжена ни с C_1, ни с C_2, так как их определители различны. Матрицы C_1 и C_2 не сопряжены в $\mathrm{GL}(2, \mathbb{Z})$, хотя они сопряжены в $\mathrm{GL}(2, \mathbb{Q})$.

Доказательство леммы 9. (a) Запишем C в виде $C = \left(\begin{smallmatrix} c_1 & c_2 \\ c_3 & -c_1 \end{smallmatrix}\right)$, где

$$-c_1^2 - c_2 c_3 = \pm 1. \tag{23}$$

Утверждение пункта (a) будем доказывать индукцией по $|c_1|$.

Случай 1: $c_1 = 0$. Тогда $c_2 = \pm 1$, $c_3 = \pm 1$, и C совпадает с одной из матриц C_2, C_3, $-C_2$, $-C_3$. Утверждение теперь следует из тождеств $C_1(-C_2)C_1^{-1} = C_2$ и $C_1(-C_3)C_1^{-1} = C_3$.

Случай 2: $|c_1| = 1$ и либо $c_2 = 0$, либо $c_3 = 0$. Предположим сначала, что $c_3 = 0$. Если c_2 четно, представим его в виде $c_2 = 2s$, $s \in \mathbb{Z}$. Тогда

$$\begin{pmatrix} 0 & 1 \\ 1 & -s \end{pmatrix} \begin{pmatrix} -1 & 2s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -s \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2s \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Если c_2 нечетно, представим его в виде $c_2 = 2s + 1$, $s \in \mathbb{Z}$. Тогда

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

Чтобы получить аналогичные соотношения в случае $c_2 = 0$, достаточно транспонировать приведенные выше четыре тождества.

Шаг индукции. Теперь мы можем предполагать, что либо $|c_1| = 1$ и $|c_2| > 0$, $|c_3| > 0$, либо $|c_1| \geqslant 2$. В последнем случае имеем

$|c_2c_3| = c_1^2 \pm 1 > 0$. В частности, $|c_2| > 0$, $|c_3| > 0$ также и в этом случае.

Так как $(|c_1| + 1)^2 > c_1^2 + 1 \geqslant c_1^2 \pm 1 = |c_2c_3|$, то имеет место по крайней мере одно из неравенств $|c_2| \leqslant |c_1|$, $|c_3| \leqslant |c_1|$. Если $|c_2| \leqslant |c_1|$, положим $s = [c_1/c_2]$ ($[\cdot]$ означает целую часть) и рассмотрим

$$\begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix} \begin{pmatrix} c_1 & c_2 \\ c_3 & -c_1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ s & 1 \end{pmatrix}^{-1} = \begin{pmatrix} c_1 - c_2 s & c_2 \\ c_3 + 2c_1 s - c_2 s^2 & -c_1 + c_2 s \end{pmatrix}.$$

Так как $0 \leqslant |c_1 - c_2 s| < |c_2| \leqslant |c_1|$, мы можем применить индукционное предположение.

Аналогичным образом, если $|c_3| \leqslant |c_1|$, положим $s = [c_1/c_3]$ и рассмотрим

$$\begin{pmatrix} 1 & -s \\ 0 & 1 \end{pmatrix} \begin{pmatrix} c_1 & c_2 \\ c_3 & -c_1 \end{pmatrix} \begin{pmatrix} 1 & -s \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} c_1 - c_3 s & c_2 + 2c_1 s - c_3 s^2 \\ c_3 & -c_1 + c_3 s \end{pmatrix}.$$

Так как $0 \leqslant |c_1 - c_3 s| < |c_3| \leqslant |c_1|$, мы можем применить индукционное предположение. Это завершает доказательство пункта (a).

(b) Пусть $g \in \mathrm{GL}(2, \mathbb{Z})$ – это такая матрица, которая осуществляет сопряжение $AB - BA$ с C_i для некоторого $i \in \{1, 2, 3\}$. Ясно, что пара X, Y порождает или не порождает $\mathrm{SL}(6, \mathbb{Z})$ одновременно с любой $\mathrm{GL}(6, \mathbb{Z})$-сопряженной с ней парой. Заменяя X и Y на сопряженные с ними при помощи $\mathrm{diag}(g, g, g)$, мы завершаем доказательство. □

Наша следующая цель состоит в том, чтобы показать, что матрицы X и Y в случае

$$AB - BA = C_1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{24}$$

не порождают $\mathrm{SL}(6, \mathbb{Z})$. Более точно, мы докажем следующую лемму.

Лемма 10. *В условиях лемм 6 и 7 предположим, кроме того, что A и B удовлетворяют* (24). *Тогда $\langle f_2(X), f_2(Y) \rangle \neq \mathrm{SL}(6, 2)$. В частности, $\langle X, Y \rangle \neq \mathrm{SL}(6, \mathbb{Z})$.*

Доказательство. Предположение (24) влечет, что

$$(a_1 - a_4)b_2 - a_2(b_1 - b_4) = 0, \tag{25}$$

$$-(a_1 - a_4)b_3 + a_3(b_1 - b_4) = 0, \tag{26}$$

$$a_2 b_3 - a_3 b_2 = 1. \tag{27}$$

Складывая равенство (25), умноженное на b_3, с (26), умноженным на b_2, и принимая во внимание (27), получаем, что

$$b_1 = b_4. \tag{28}$$

Складывая равенство (25), умноженное на a_3, с (26), умноженным на a_2, и принимая во внимание (27), получаем, что

$$a_1 = a_4. \tag{29}$$

Лемма 6 влечет

$$a_1^2 - a_2 a_3 \equiv 0 \pmod 2. \tag{30}$$

Объединяя (27)–(30) с (17), получаем, что s_1 четно. Из леммы 7 следует, что $s_1 = 0$ и $s_2 = \pm 1$. Рассмотрим s_2 по модулю 2 и примем во внимание (27)–(30). Это дает нам сравнение

$$b_1^2 - b_2 b_3 \equiv 1 \pmod 2. \tag{31}$$

Заменим систему (27), (30), (31) на соответствующие сравнения по модулю 2. Непосредственно проверяется, что по модулю 2 имеется в точности шесть допустимых наборов вычетов $(b_1, b_2, b_3, b_4, a_1, a_2, a_3, a_4)$, а именно:

$$\begin{array}{ll}
(0,1,1,0,0,0,1,0), & (1,1,0,1,0,0,1,0), \\
(0,1,1,0,0,1,0,0), & (1,0,1,1,0,1,0,0), \\
(1,0,1,1,1,1,1,1), & (1,1,0,1,1,1,1,1).
\end{array}$$

Используя систему компьютерной алгебры MAGMA, было проверено, что во всех шести случаях группа $\langle f_2(X), f_2(Y)\rangle$ имеет порядок 324. В частности, она является собственной подгруппой группы $\mathrm{SL}(6,2)$. Завершающее утверждение леммы теперь тривиально. □

Теперь мы рассмотрим случай, когда $AB - BA = C_2$ или $AB - BA = C_3$.

Лемма 11. *В условиях леммы 5 предположим также, что $AB - BA = C_2$ или $AB - BA = C_3$, где матрицы C_2, C_3 определены в (22). Тогда*

$$(a_1 - a_4)b_2 - a_2(b_1 - b_4) = 1. \tag{32}$$

Кроме того, если $AB - BA = C_3$, то

$$b_3 = b_2, \qquad a_3 = a_2; \tag{33}$$

если $AB - BA = C_2$, *то*

$$b_3 = -b_2, \qquad a_3 = -a_2. \tag{34}$$

Доказательство. Непосредственное вычисление дает равенство (32). Кроме того,

$$-(a_1 - a_4)b_3 + a_3(b_1 - b_4) = \pm 1, \tag{35}$$

$$a_2 b_3 - a_3 b_2 = 0. \tag{36}$$

Умножим теперь (32) на b_3, (35) на b_2 и сложим их. Принимая во внимание (36), устанавливаем, что $b_2 \pm b_3 = 0$. Аналогичным образом, умножая (32) на a_3, а (35) на a_2, мы получаем, что $a_2 \pm a_3 = 0$. Более того, знаки в $b_2 \pm b_3$ и $a_2 \pm a_3$ либо одновременно $+$ (если мы брали C_2) или одновременно $-$ (если мы брали C_3). □

Замечание 5. Пусть $AB - BA = C_i$, где $i = 2$ или 3. Не умаляя общности, всегда можно заменить матрицы Y и X на сопряженные с ними при помощи $\mathrm{diag}(C_i, C_i, C_i)$. Это соответствует замене A и B на сопряженные с ними при помощи C_i. Ясно, что такое сопряжение сохраняет равенство $AB - BA = C_i$, а также правую часть формулы (15). Оно также сохраняет нетривиальную разрешимость системы (20). Таким образом, данное преобразование не влияет на результаты лемм 6 и 7.

С другой стороны, используя равенства (33), (34) леммы 11, мы получаем, что в случае, когда $AB - BA = C_2$,

$$C_2 \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} C_2^{-1} = \begin{pmatrix} a_4 & a_3 \\ a_2 & a_1 \end{pmatrix} = \begin{pmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{pmatrix}.$$

Аналогично, в случае $AB - BA = C_3$,

$$C_3 \begin{pmatrix} a_1 & a_2 \\ a_3 & a_4 \end{pmatrix} C_3^{-1} = \begin{pmatrix} a_4 & -a_3 \\ -a_2 & a_1 \end{pmatrix} = \begin{pmatrix} a_4 & -a_2 \\ -a_3 & a_1 \end{pmatrix}.$$

Аналогичные тождества имеют место и для матрицы B. Таким образом, мы заключаем, что преобразование

$$(b_1, b_2, b_3, b_4, a_1, a_2, a_3, a_4) \mapsto (b_4, -b_2, -b_3, b_1, a_4, -a_2, -a_3, a_1)$$

соответствует одновременному сопряжению матриц X и Y. Следовательно, всегда можно предполагать, не умаляя общности, что

$$a_2 \geqslant 0. \tag{37}$$

5. Решения с $b_2 = 0$

В этом параграфе мы рассмотрим случай, когда $b_2 = 0$. Согласно лемме 11 получаем, что $b_3 = 0$ и $a_2(b_1 - b_4) = -1$. Следовательно, $a_2 = \pm 1$. На основании замечания 5 достаточно искать решения с $a_2 = 1$. Если $a_2 = 1$, то уравнение (32) приобретает вид

$$b_4 = b_1 + 1. \tag{38}$$

Вновь по лемме 11 получаем, что $a_3 = \pm 1$. Наконец, $s_0 = \pm 1$ по лемме 6. Для каждого набора знаков мы найдем допустимые значения a_1 и a_4. Затем на основании (38) мы исключим b_4 из s_1 и s_2 и проверим, будут ли s_1 и s_2 удовлетворять (19); см. лемму 7.

Случай 1: $a_2 = 1$, $a_3 = 1$, $s_0 = 1$. Согласно лемме 6 имеем $(a_1 - 3)(a_4 - 3) = 2$. В таблице 1.I перечислены допустимые целые значения a_1 и a_4. В каждом из случаев также представлено явное задание s_1 как функции от b_1. Из представления s_1 видно, что ни одно из этих решений не удовлетворяет условию $s_1 \in \{-1, 0, 1\}$.

Случай 2: $a_2 = 1$, $a_3 = -1$, $s_0 = -1$. Согласно лемме 6 имеем $(a_1 - 3)(a_4 - 3) = -2$. В таблице 1.II перечислены значения a_1 и a_4, а также вид s_1 как функции от b_1. В первых трех случаях не выполнено условие $s_1 \in \{-1, 0, 1\}$. Чтобы удовлетворить это условие в последнем случае, мы должны потребовать, что $b_1 = -2$. Но тогда $s_2 = 11$, что противоречит лемме 7.

Таблица 1

I			II		
a_1	a_4	s_1	a_1	a_4	s_1
5	4	$15b_1 + 48$	5	2	$13b_1 + 36$
4	5	$15b_1 + 47$	2	5	$13b_1 + 33$
1	2	$9b_1 + 14$	4	1	$11b_1 + 25$
2	1	$9b_1 + 15$	1	4	$11b_1 + 22$

Случай 3: $a_2 = 1$, $a_3 = 1$, $s_0 = -1$. Согласно лемме 6 имеем $(a_1 - 3)(a_4 - 3) = 0$. Таким образом, $a_1 = 3$ или $a_4 = 3$.

Если $a_1 = 3$, то $s_1 + s_2 = -3b_1^2 + 3b_1 + 6a_4 + 17 \equiv -1 \pmod 6$. Принимая во внимание лемму 7 и, в частности, формулу (19), мы приходим к выводу, что $s_1 + s_2 = -1$. Это равенство позволяет исключить a_4:

$$a_4 = \frac{b_1^2 - b_1}{2} - 3. \tag{39}$$

Используя последнее равенство вместе с (38) и известными значениями параметров a_1, a_2, a_3, b_2, b_3, мы получаем на основании (17), что $s_1 = (b_1^3 + 4b_1^2 + 7b_1 - 2)/2$. Очевидно, что $s_1 > 1$ при $b_1 \geqslant 1$, $s_1 < -1$ при $b_1 \leqslant -4$, $s_1 \notin \{-1, 0, 1\}$ при $b_1 = -1, -2, -3$. Таким образом, остается единственная возможность $b_1 = 0$. Используя (38) и (39), находим, что

$$(b_1, b_2, b_3, b_4, a_1, a_2, a_3, a_4) = (0, 0, 0, 1, 3, 1, 1, -3).$$

Это дает нам первый исключительный набор в (3).

Если $a_4 = 3$, то $s_1 + s_2 = -3b_1^2 + 3b_1 + 6a_1 + 17 \equiv -1 \pmod 6$. Рассуждая аналогично предыдущему подслучаю, мы последовательно устанавливаем, что $s_1 + s_2 = -1$, $a_1 = (b_1^2 - b_1)/2 - 3$ и $s_1 = (b_1^3 + 5b_1^2 + 6b_1 - 14)/2$. Очевидно, что $s_1 > 1$ при $b_1 \geqslant 2$, $s_1 < -1$ при $b_1 \leqslant -5$, $s_1 \notin \{-1, 0, 1\}$ при $b_1 = 0, -1, -2, -3, -4$. Таким образом, остается единственная возможность $b_1 = 1$, и мы получаем, что

$$(b_1, b_2, b_3, b_4, a_1, a_2, a_3, a_4) = (1, 0, 0, 2, -3, 1, 1, 3).$$

Это дает первый набор в (4).

Случай 4: $a_2 = 1$, $a_3 = -1$, $s_0 = 1$. Согласно лемме 6 имеем $(a_1 - 3)(a_4 - 3) = 0$. Таким образом, $a_1 = 3$ или $a_4 = 3$.

Если $a_1 = 3$, то, рассуждая аналогично случаю 3, получаем, что $s_1 + s_2 = -3b_1^2 + 3b_1 + 6a_4 + 19 \equiv 1 \pmod 6$. Вместе с леммой 7 это влечет, что $(s_1, s_2) \in \{(0, 1), (1, 0)\}$. Следовательно, $s_1 + s_2 = 1$, $a_4 = (b_1^2 - b_1)/2 - 3$ и $s_1 = (b_1^3 + 4b_1^2 + 7b_1 + 2)/2$. Очевидно, что $s_1 > 1$ при $b_1 \geqslant 1$, $s_1 < -1$ при $b_1 \leqslant -4$, $s_1 \notin \{0, 1\}$ при $b_1 = -1, -2, -3$. Остается единственная возможность $b_1 = 0$, что приводит к решению

$$(b_1, b_2, b_3, b_4, a_1, a_2, a_3, a_4) = (0, 0, 0, 1, 3, 1, -1, -3).$$

Это дает нам первый набор в (5).

Если $a_4 = 3$, то $s_1 + s_2 = -3b_1^2 + 3b_1 + 6a_1 + 19 \equiv 1 \pmod 6$. Повторяя те же рассуждения, что и выше, мы последовательно устанавливаем, что $s_1 + s_2 = 1$, $a_1 = (b_1^2 - b_1)/2 - 3$ и $s_1 = (b_1^3 + 5b_1^2 + 6b_1 - 10)/2$. Очевидно, что $s_1 > 1$ при $b_1 \geqslant 2$; $s_1 < -1$ при $b_1 \leqslant -5$;

$s_1 \notin \{-1, 0, 1\}$ при $b_1 = 0, -1, -2, -3, -4$. Остается единственная возможность $b_1 = 1$. Она приводит к следующему решению:

$$(b_1, b_2, b_3, b_4, a_1, a_2, a_3, a_4) = (1, 0, 0, 2, -3, 1, -1, 3).$$

что дает нам первый набор в (6).

6. Решения с $b_2 \neq 0$

Определим s_0, s_1 и s_2 согласно (15), (17) и (18), соответственно. Напомним также определение множества S, данное в (21). Наша цель состоит в том, чтобы для каждого набора $(r_0, r_1, r_2) \in S$ решить систему из четырех уравнений: (32) и

$$s_0 - r_0 = 0, \tag{40}$$

$$s_1 - r_1 = 0, \tag{41}$$

$$s_2 - r_2 = 0 \tag{42}$$

при дополнительных условиях (37) и либо (33), либо (34). Так как случай $b_2 = 0$ был полностью разобран в предыдущем параграфе, далее мы будем всегда предполагать, что $b_2 \neq 0$.

6.1. Выполнены соотношения (33)**.**

Предположим, что выполнены соотношения (33). Домножим (32) на 6, (40) на $-b_2$, (41) на b_2, (42) на b_2 и сложим эти равенства. Из полученного уравнения выводим, на основании (15), (17) и (18), что

$$a_1 = \frac{6a_2(b_1 - b_4) + 3b_2(b_1b_4 - b_1 - b_2^2 - b_4 + 1) + b_2(r_1 + r_2 - r_0) + 6}{12b_2}. \tag{43}$$

Для того, чтобы найти a_4, умножим (32) на 6, (40) на b_2, (41) на $-b_2$, (42) на $-b_2$ и сложим их. Рассуждая, как и выше, получаем, что

$$a_4 = \frac{6a_2(b_4 - b_1) + 3b_2(b_1b_4 - b_1 - b_2^2 - b_4 + 1) + b_2(r_1 + r_2 - r_0) - 6}{12b_2}. \tag{44}$$

Далее мы подставим значения a_1 и a_4 в (42). Отметим, что $(b_1 - b_4)^2 + 4b_2^2 \geqslant 4b_2^2 > 0$. Таким образом, из получившегося в результате уравнения следует, что

$$a_2 = \frac{-3(b_1 + b_4 + 10)b_2^3 + d_1b_2 - 6(b_1 - b_4)}{6\big((b_1 - b_4)^2 + 4b_2^2\big)}, \tag{45}$$

где

$$d_1 = 3(b_1+b_4)b_1b_4 - 3(b_1+b_4)^2 + 30b_1b_4$$
$$+ (b_1+b_4)(r_1+r_2-r_0+9) + 2(r_0-r_1+5r_2-21). \qquad (46)$$

Положим

$$\begin{cases} z_1 = b_1b_4 - b_2^2, \\ z_2 = b_1 + b_4. \end{cases} \qquad (47)$$

Подставляя (43), (44) в (41) и исключая a_2 на основании (45) и (46), мы получим, что

$$F(r_0, r_1, r_2, z_1, z_2) = 0,$$

где

$$\begin{aligned} F(r_0,r_1,r_2,z_1,z_2) &= -z_1^3 - 3z_1^2z_2 - 3z_1z_2^2 + 7z_2^3 \\ &- \frac{9+2r_1+2r_2-2r_0}{3}z_1^2 - \frac{90+2r_1+8r_2-2r_0}{3}z_1z_2 \\ &+ \frac{63-8r_1-2r_2-4r_0}{3}z_2^2 \\ &- \frac{459+(r_1+r_2-r_0)^2-96r_1+84r_2-48r_0}{9}z_1 \\ &+ \frac{189+(r_1-2r_2-r_0)^2-9r_2^2+30r_1-24r_2-30r_0}{9}z_2 \\ &- \frac{(r_1-5r_2-r_0)^2+42r_1-210r_2-42r_0+477}{9}. \end{aligned} \qquad (48)$$

Лемма 12. *Пусть $(r_0, r_1, r_2) \in S$. Тогда уравнение*

$$F(r_1, r_2, r_0, z_1, z_2) = 0$$

имеет в точности следующие целые решения (z_1, z_2):

- $z_1 = -7$, $z_2 = -5$ *и* $z_1 = -5$, $z_2 = -3$ *для* $r_1 = r_2 = 1$, $r_0 = -1$;
- $z_1 = 0$, $z_2 = 1$ *и* $z_1 = 2$, $z_2 = 3$ *для* $r_1 = -1$, $r_2 = 0$, $r_0 = -1$.

Доказательство. Вначале сделаем два полезных замечания. Во-первых, многочлен F можно представить в виде

$$F = (z_2 - z_1)(z_1^2 + 4z_1z_2 + 7z_2^2) + k_1z_1^2 + k_2z_1z_2$$
$$+ k_3z_2^2 + k_4z_1 + k_5z_2 + k_6,$$

где параметрические коэффициенты $k_1, \ldots, k_6$ приведены в таблице 2. Во-вторых,

$$z_1^2 + 4z_1z_2 + 7z_2^2 = (z_1 + 2z_2)^2 + 3z_2^2$$
$$= \left(\sqrt{7}z_2 + \frac{2}{\sqrt{7}}z_1\right)^2 + \frac{3}{7}z_1^2.$$

В частности,

$$z_1^2 + 4z_1z_2 + 7z_2^2 \geqslant \frac{3}{7}(\max\{|z_1|, |z_2|\})^2. \tag{49}$$

Таблица 2

r_0	r_1	r_2	k_1	k_2	k_3	k_4	k_5	k_6
1	1	0	−3	− 30	17	− 35	21	− 53
1	0	1	−3	− 32	19	− 55	15	− 29
1	− 1	− 1	−1	− 26	23	− 48	16	− 68
−1	− 1	0	−3	− 30	25	− 67	21	− 53
−1	0	− 1	−3	− 28	23	− 47	27	− 85
−1	1	1	−5	− 34	19	− 56	24	− 40

Компьютерный поиск решений уравнения $F(r_0, r_1, r_2, z_1, z_2) = 0$ в области $-100 \leqslant z_1 \leqslant 100$, $-100 \leqslant z_2 \leqslant 100$, $(r_0, r_1, r_2) \in S$ дает нам лишь те решения, что указаны в формулировке леммы.

Далее рассмотрим случай, когда $\max\{|z_1|, |z_2|\} > 100$. В частности, это предположение вместе с (49) и данными таблицы 2 влечет, что

$$|k_4z_1 + k_5z_2 + k_6| \leqslant (|k_4| + |k_5|)\max\{|z_1|, |z_2|\} + |k_6|$$
$$< (|k_4| + |k_5| + 1)\max\{|z_1|, |z_2|\} < 90\max\{|z_1|, |z_2|\}$$
$$< \max\{|z_1|, |z_2|\}^2 \leqslant 3(z_1^2 + 4z_1z_2 + 7z_2^2). \tag{50}$$

Из данных таблицы 2 также следует, что квадратичные формы

$$6(z_1^2 + 4z_1z_2 + 7z_2^2) + k_1z_1^2 + k_2z_1z_2 + k_3z_2^2,$$
$$26(z_1^2 + 4z_1z_2 + 7z_2^2) - k_1z_1^2 - k_2z_1z_2 - k_3z_2^2$$

положительно определены при всех $(r_0, r_1, r_2) \in S$. Следовательно, в предположении справедливости неравенств $\max\{|z_1|, |z_2|\} >$

100 и либо $z_2 - z_1 \geqslant 10$, либо $z_2 - z_1 \leqslant -30$, слагаемое $(z_2 - z_1)(z_1^2 + 4z_1z_2 + 7z_2^2)$ доминирует над другими слагаемыми в F. Иными словами, F будет положительным, если $z_2 - z_1 \geqslant 10$, и F будет отрицательным, если $z_2 - z_1 \leqslant -30$.

Наконец, для целого t в пределах $-30 < t < 10$ положим $z_2 = z_1 + t$ и запишем $F(r_0, r_1, r_2, z_1, z_1 + t)$ в виде $F(r_0, r_1, r_2, z_1, z_1 + t) = \alpha z_1^2 + \beta z_1 + \gamma$. Непосредственно проверяется, что во всех рассматриваемых случаях коэффициент α ненулевой. Кроме того, если $\beta^2 - 4\alpha\gamma \geqslant 0$, то можно указать следующую границу для вещественных корней многочлена $\alpha z_1^2 + \beta z_1 + \gamma$:

$$|z_1| \leqslant (|\beta| + \sqrt{\beta^2 - 4\alpha\gamma})/|2\alpha|.$$

Непосредственные вычисления показывают, что для всякого $-30 < t < 10$ и всяких $(r_0, r_1, r_2) \in S$ вещественные корни многочлена $\alpha z_1^2 + \beta z_1 + \gamma$ удовлетворяют неравенству $|z_1| \leqslant 11$. Следовательно, $|z_2| \leqslant |z_1| + |t| \leqslant 41$, и мы вновь находимся в области $-100 \leqslant z_1, z_2 \leqslant 100$. Это завершает доказательство. $\square$

Для того, чтобы найти $a_1, \ldots, a_4$, $b_1, \ldots, b_4$, проанализируем теперь перечисленные в лемме 12 решения.

Случай 1: $r_1 = r_2 = 1$, $r_0 = -1$, $z_1 = -7$, $z_2 = -5$. Подставляя эти значения в (47) и исключая b_4, мы получаем, что

$$4b_2^2 + (2b_1 + 5)^2 = 53.$$

Это уравнение имеет четыре целочисленных решения относительно b_1, b_2. Значение b_4 можно определить из второго уравнения в (47). Используя (45), (46), (43) и (44) мы последовательно находим a_2, a_1 и a_4. Наконец, b_3 и a_3 можно определить на основании (33). Результаты собраны в таблице 3. Оказывается, что значения $a_1, \ldots, a_4$ будут целыми лишь в двух случаях. Только второе решение удовлетворяет неравенству (37). Оно дает нам второй исключительный набор в (4).

Таблица 3

b_1	b_2	b_3	b_4	a_1	a_2	a_3	a_4
1	1	1	−6	−3	−1	−1	3
−6	−1	−1	1	3	1	1	−3
1	−1	−1	−6	39/53			
−6	1	1	1	−39/53			

Случай 2: $r_1 = r_2 = 1$, $r_0 = -1$, $z_1 = -5$, $z_2 = -3$. Подставляя эти значения в (47) и исключая b_4, получаем, что

$$4b_2^2 + (2b_1 + 3)^2 = 29.$$

Это уравнение имеет четыре решения в целых числах. Рассуждая аналогично предыдущему случаю мы находим, что только два из них приводят к целым значениям $a_1, \ldots, a_4$. Результаты собраны в таблице 4. Только второе решение удовлетворяет неравенству (37). Это дает нам второй исключительный набор в (3).

Таблица 4

b_1	b_2	b_3	b_4	a_1	a_2	a_3	a_4
-4	1	1	1	3	-1	-1	-3
1	-1	-1	-4	-3	1	1	3
-4	-1	-1	1	$39/29$			
1	1	1	-4	$-39/29$			

Случай 3: $r_1 = -1$, $r_2 = 0$, $r_0 = -1$, $z_1 = 2$, $z_2 = 3$. Поставляя эти значения в (47) и исключая b_4, получаем, что

$$4b_2^2 + (2b_1 - 3)^2 = 1.$$

Следовательно, $b_2 = 0$, но решения с $b_2 = 0$ уже были рассмотрены в §5.

Случай 4: $r_1 = -1$, $r_2 = 0$, $r_0 = -1$, $z_1 = 0$, $z_2 = 1$. Подставляя эти значения в (47) и исключая b_4, получим, что

$$4b_2^2 + (2b_1 - 1)^2 = 1.$$

Вновь $b_2 = 0$, но решения с $b_2 = 0$ уже были рассмотрены в §5.

6.2. Выполнены соотношения (34).

Теперь предположим, что выполнены соотношения (34). Вспомним определение s_0, s_1 и s_2; см. (15), (17), (18). Умножим (32) на 6, (40) на $-b_2$, (41) на b_2, (42) на b_2 и сложим эти равенства. Из получившегося в результате уравнения следует, что

$$a_1 = \frac{6a_2(b_1 - b_4) + 3b_2(b_1b_4 - b_1 + b_2^2 - b_4 + 1) + b_2(r_1 + r_2 - r_0) + 6}{12b_2}. \tag{51}$$

Далее, умножим (32) на на 6, (40) на b_2, (41) на $-b_2$, (42) на $-b_2$ и сложим эти равенства. Из получившегося уравнения следует, что

$$a_4 = \frac{6a_2(b_4 - b_1) + 3b_2(b_1b_4 - b_1 + b_2^2 - b_4 + 1) + b_2(r_1 + r_2 - r_0) - 6}{12b_2}. \tag{52}$$

Подставим теперь (51) и (52) в (42) и рассмотрим числитель дроби, стоящей в левой части полученного уравнения, как многочлен от a_2. Коэффициент его главного члена с точностью до постоянного рационального множителя раскладывается на множители следующим образом: $(b_1 - 2b_2 - b_4)(b_1 + 2b_2 - b_4)$. Таким образом, дальнейший анализ будет зависеть от того, обращается ли $(b_1 - 2b_2 - b_4)(b_1 + 2b_2 - b_4)$ в 0 или нет.

6.2.1. $b_1 = 2b_2 + b_4$**.**

Предположим, что $b_1 = 2b_2 + b_4$. Подставляя это равенство вместе с (51), (52) в (42), получаем, что

$$\begin{aligned}-3(b_2 + b_4)^3 - 9(b_2 + b_4)^2 - (9 + r_1 + r_2 - r_0)(b_2 + b_4)&\\ - (r_0 - r_1 + 5r_2) + 27 = 0.&\end{aligned} \tag{53}$$

Рассмотрение кубического многочлена из левой части, возникающего при различных значениях $(r_0, r_1, r_2) \in S$, приводит к следующей лемме.

Лемма 13. *Пусть $(r_0, r_1, r_2) \in S$. Тогда уравнение (53) имеет рациональное решение (b_2, b_4) только в следующих случаях: $r_0 = 1$, $r_1 = 0$, $r_2 = 1$ или $r_0 = -1$, $r_1 = 1$, $r_2 = 1$. В обоих случаях имеем $b_4 = 1 - b_2$.*

Оба случая, перечисленные в лемме 13 приводят, однако, к нецелым значениям a_1 или a_4. А именно, подставляя приведенные выше выражения для b_1 и b_4 в (51) и (52), получаем, что в первом случае $a_1 = a_2 + 1/(2b_2)$, а во втором $a_1 + a_4 = 1/2$. Мы приходим к заключению, что равенство $b_1 = 2b_2 + b_4$ невозможно.

6.2.2. $b_1 = -2b_2 + b_4$**.**

Предположим, что $b_1 = -2b_2 + b_4$. Подставляя это выражение вместе с (51), (52) в (42), получаем, что

$$\begin{aligned}3(b_2 - b_4)^3 - 9(b_2 - b_4)^2 + (9 + r_1 + r_2 - r_0)(b_2 - b_4)&\\ - (r_0 - r_1 + 5r_2) + 15 = 0.&\end{aligned} \tag{54}$$

Рассмотрение кубического многочлена, возникающего в левой части для троек $(r_0, r_1, r_2) \in S$, приводит к следующей лемме.

Лемма 14. *Пусть* $(r_0, r_1, r_2) \in S$. *Тогда уравнение* (54) *имеет рациональное решение* (b_2, b_4) *только в следующих случаях:* $r_0 = 1$, $r_1 = -1$, $r_2 = -1$ *или* $r_0 = -1$, $r_1 = 0$, $r_2 = -1$. *В обоих случаях имеем* $b_4 = b_2 + 1$.

Однако оба случая, перечисленные в лемме 14, приводят к нецелым значениям для a_1 или a_4. А именно, подставляя приведенные выше выражения для b_1 и b_4 в (51) и (52), получаем, что в первом случае $a_1 + a_4 = -1/2$, тогда как во втором случае $a_1 = -a_2 + 1/(2b_2)$. Мы заключаем, что случай $b_1 = -2b_2 + b_4$ также невозможен.

6.2.3. $b_1 \neq 2b_2 + b_4$, $b_1 \neq -2b_2 + b_4$.

Разбор этого случая сходен с анализом, проведенным в разделе 6.1. Мы воспроизводим здесь основные шаги и вычислительные данные ради удобства читателя.

Подставляя (51) и (52) в уравнение (42) и используя предположения этого раздела, мы находим a_2:

$$a_2 = \frac{3(b_1 + b_4 + 10)b_2^3 + d_1 b_2 - 6(b_1 - b_4)}{6\big((b_1 - b_4)^2 - 4b_2^2\big)}, \tag{55}$$

где

$$d_1 = 3(b_1 + b_4)b_1 b_4 - 3(b_1 + b_4)^2 + 30 b_1 b_4$$

$$-(b_1 + b_4)(r_0 - r_1 - r_2 - 9) - 2(r_1 - 5r_2 - r_0 + 21). \tag{56}$$

Положим теперь

$$\begin{cases} z_1 = b_1 b_4 + b_2^2, \\ z_2 = b_1 + b_4. \end{cases} \tag{57}$$

Подставим (51), (52) в (41) и исключим a_2 на основании (55), (56). Левую часть получившегося уравнения можно представить в виде дроби, числитель которой равен

$$F(r_0, r_1, r_2, z_1, z_2) + 8,$$

где F – тот же многочлен, что и в (48).

Лемма 15. *Пусть* $(r_0, r_1, r_2) \in S$. *Тогда уравнение*

$$F(r_0, r_1, r_2, z_1, z_2) + 8 = 0$$

имеет в точности следующие целые решения (z_1, z_2)*:*

- $(z_1, z_2) \in \{(0,1), (2,3), (4,-3), (10,-5)\}$ *при* $r_0 = 1,\ r_1 = 1,\ r_2 = 0$*;*
- $(z_1, z_2) \in \{(-5,-4), (1,2), (5,-4), (6,-3), (8,-5), (9,-4)\}$ *при* $r_0 = 1,\ r_1 = 0,\ r_2 = 1$*;*
- $(z_1, z_2) \in \{(-5,-5), (-3,-3), (1,2), (5,-3), (6,-3), (8,-5), (11,-5)\}$ *при* $r_0 = 1,\ r_1 = -1,\ r_2 = -1$*;*
- $(z_1, z_2) \in \{(-5,-4), (1,2)\}$ *при* $r_0 = -1,\ r_1 = 0,\ r_2 = -1$*;*
- $(z_1, z_2) \in \{(1,2)\}$ *при* $r_0 = -1,\ r_1 = 1,\ r_2 = 1$.

Доказательство. Компьютерный поиск в области $-100 \leqslant z_1 \leqslant 100$, $-100 \leqslant z_2 \leqslant 100$, $(r_0, r_1, r_2) \in S$ дает нам только те решения, что перечислены в формулировке леммы.

Теперь предположим, что $\max\{|z_1|, |z_2|\} > 100$ и либо $z_2 - z_1 \geqslant 10$, либо $z_2 - z_1 \leqslant -30$. Этот случай полностью аналогичен соответствующему случаю в доказательстве леммы 12, поскольку меняется лишь свободный член k_6, а неравенства (50) остаются верными.

Наконец, предположим, что $-30 < z_2 - z_1 < 10$. Для каждого целого t, $-30 < t < 10$, положим $z_2 = z_1 + t$ и запишем $F(r_0, r_1, r_2, z_1, z_1 + t) + 8$ в виде $F(r_0, r_1, r_2, z_1, z_1 + t) + 8 = \varepsilon z_1^2 + \delta z_1 + \gamma$. Непосредственно проверяется, что во всех рассматриваемых случаях коэффициент ε всегда отличен от 0. Для t в пределах $-30 < t < 10$ и для $(r_0, r_1, r_2) \in S$, используя те же оценки, что и в доказательстве леммы 12, мы можем дать следующую оценку для вещественных корней многочлена $\varepsilon z_1^2 + \delta z_1 + \gamma$: $|z_1| \leqslant 12$. Следовательно, $|z_2| \leqslant |z_1| + |t| \leqslant 42$, и мы вновь находимся в области $-100 \leqslant z_1, z_2 \leqslant 100$. Это завершает доказательство. $\square$

Теперь проанализируем решения, перечисленные в лемме 15. Исключая b_4 из (57), имеем

$$\begin{cases} b_4 = z_2 - b_1, \\ (2b_2 - 2b_1 + z_2)(2b_2 + 2b_1 - z_2) = 4z_1 - z_2^2. \end{cases} \tag{58}$$

Таким образом, $2b_2-2b_1+z_2=\alpha$, $2b_2+2b_1-z_2=\beta$, где $\alpha\beta=4z_1-z_2^2$ и α, β одновременно целые. Отсюда мы получаем, что

$$b_2=\frac{\alpha+\beta}{4},\qquad b_1=\frac{\beta-\alpha+2z_2}{4}. \tag{59}$$

Замечание 6. Если z_2 четно, то $\beta\equiv\alpha(\bmod 4)$, поскольку $b_1\in\mathbb{Z}$. Кроме того, в этом случае $4z_1-z_2^2\equiv 0(\bmod 4)$. Следовательно, в случае четного z_2 оба числа α и β должны быть четны.

Наша цель состоит в анализе всех пар (z_1,z_2), перечисленных в лемме 15. В каждом случае мы находим допустимые целые множители α, β. В случае, когда z_2 четно, мы дополнительно используем замечание 6. Значения b_1, b_2, b_4 можно найти из (59) и (58). Затем, на основании (55), (56), (51) и (52) мы последовательно находим a_2, a_1 и a_4. Наконец, b_3, a_3 можно определить на основании (34). Отметим, что для некоторых пар α, β получающиеся в результате значения a_2 или a_1 могут оказаться нецелыми. Такие случаи следует исключить из дальнейшего рассмотрения.

Случай 1: $z_1=1$, $z_2=2$. Согласно (58) имеем $b_2=\pm(b_1-1)$ и $b_4=2-b_1$. Следовательно, $b_1\mp 2b_2-b_4=0$, но эти возможности были исключены в подразделах 6.2.1 и 6.2.2.

Случай 2: $z_1=0$, $z_2=1$ или $z_1=2$, $z_2=3$. В этих случаях $4z_1-z_2^2=-1$. Таким образом, либо $\alpha=1$, $\beta=-1$, либо $\alpha=-1$, $\beta=1$. Следовательно, $b_2=0$, но этот случай уже был рассмотрен в § 5.

Результаты для остальных случаев собраны в таблице 5. Таблица содержит все допустимые пары (α,β). В случае, когда $z_1=-5$ и $z_2=-4$, мы исключаем пары $\alpha=6$, $\beta=-6$ и $\alpha=-6$, $\beta=6$, поскольку для них $b_2=0$. В таблице перечислены значения $b_1,\dots,b_4$, $a_1,\dots,a_4$ в том случае, когда все они целые. В противном случае мы прекращаем перечисление на первом найденном нецелом значении (обычно, это a_2). Анализ данных в таблице 5 дает нам 20 новых целых решений a_1, …,a_4, b_1, …,b_4. Только десять из них удовлетворяют неравенству (37). Они дают нам вторые наборы в (5), (6), а также оба набора в каждом из случаев (7)–(10).

Доказательство теоремы 1 следует теперь из результатов §5 и из анализа данных таблиц 3, 4 и 5.

Таблица 5.

r_0	r_1	r_2	z_1	z_2	α	β	b_1	b_2	b_3	b_4	a_1	a_2	a_3	a_4
1	1	0	4	−3	1	7	0	2	−2	−3	3	1	−1	1
					−1	−7	−3	−2	2	0	1	−1	1	3
					7	1	−3	2	−2	0		1/7		
					−7	−1	0	−2	2	−3		−1/7		
1	1	0	10	−5	1	15	1	4	−4	−6	5	1	−1	3
					−1	−15	−6	−4	4	1	3	−1	1	5
					3	5	−2	2	−2	−3		1/3		
					5	3	−3	2	−2	−2		1/5		
					15	1	−6	4	−4	1		1/15		
					−3	−5	−3	−2	2	−2		−1/3		
					−5	−3	−2	−2	2	−3		−1/5		
					−15	−1	1	−4	4	−6		−1/15		
1	0	1	−5	−4	−18	2	3	−4	4	−7		7/2		
					18	−2	−7	4	−4	3		−7/2		
					−2	18	3	4	−4	−7		−73/18		
					2	−18	−7	−4	4	3		73/18		
1	0	1	5	−4	2	2	−2	1	−1	−2	3	1	−1	2
					−2	−2	−2	−1	1	−2	2	−1	1	3
1	0	1	6	−3	5	3	−2	2	−2	−1	3	−1	1	2
					−5	−3	−1	−2	2	−2	2	1	−1	3
					1	15	2	4	−4	−5		−7/5		
					−1	−15	−5	−4	4	2		7/5		
					3	5	−1	2	−2	−2		−13/15		
					−3	−5	−2	−2	2	−1		13/15		
					15	1	−5	4	−4	2		−7/3		
					−15	−1	2	−4	4	−5		7/3		
1	0	1	8	−5	7	1	−4	2	−2	−1	3	1	−1	4
					−7	−1	−1	−2	2	−4	4	−1	1	3
					1	7	−1	2	−2	−4		13/7		
					−1	−7	−4	−2	2	−1		−13/7		
1	0	1	9	−4	2	10	0	3	−3	−4	3	−1	1	4
					−2	−10	−4	−3	3	0	4	1	−1	3
					10	2	−4	3	−3	0		−7/5		
					−10	−2	0	−3	3	−4		7/5		

Продолжение таблицы 5.

r_0 r_1 r_2	z_1 z_2	α	β	b_1	b_2	b_3	b_4	a_1	a_2	a_3	a_4
-1 0 -1	-5 -4	-2	18	3	4	-4	-7		$-9/2$		
		2	-18	-7	-4	4	3		$9/2$		
		-18	2	3	-4	4	-7		$71/18$		
		18	-2	-7	4	-4	3		$-71/18$		
1 -1 -1	-5 -5	5	-9	-6	-1	1	1	3	1	-1	-3
		-5	9	1	1	-1	-6	-3	-1	1	3
		1	-45	-14	-11	11	9		$49/5$		
		-1	45	9	11	-11	-14		$-49/5$		
		3	-15	-7	-3	3	2		$41/15$		
		-3	15	2	3	-3	-7		$-41/15$		
		9	-5	-6	1	-1	1		$-31/45$		
		-9	5	1	-1	1	-6		$31/45$		
		15	-3	-7	3	-3	2		$-7/3$		
		-15	3	2	-3	3	-7		$7/3$		
		45	-1	-14	11	-11	9		$-79/9$		
		-45	1	9	-11	11	-14		$79/9$		
1 -1 -1	-3 -3	7	-3	-4	1	-1	1	3	-1	1	-3
		-7	3	1	-1	1	-4	-3	1	-1	3
		1	-21	-7	-5	5	4		$47/7$		
		-1	21	4	5	-5	-7		$-47/7$		
		3	-7	-4	-1	1	1		$31/21$		
		-3	7	1	1	-1	-4		$-31/21$		
		21	-1	-7	5	-5	4		$-17/3$		
		-21	1	4	-5	5	-7		$17/3$		
1 -1 -1	5 -3	11	1	-4	3	-3	1	3	-1	1	1
		-11	-1	1	-3	3	-4	1	1	-1	3
		1	11	1	3	-3	-4		$-1/11$		
		-1	-11	-4	-3	3	1		$1/11$		
1 -1 -1	11 -5	19	1	-7	5	-5	2	5	-1	1	3
		-19	-1	2	-5	5	-7	3	1	-1	5
		1	19	2	5	-5	-7		$-1/19$		
		-1	-19	-7	-5	5	2		$1/19$		

Продолжение таблицы 5.

r_0 r_1 r_2	z_1 z_2	α	β	b_1	b_2	b_3	b_4	a_1	a_2	a_3	a_4
$1\ -1\ -1$	$6\ -3$	1	15	2	4	-4	-5	$3/2$	-1		
		-1	-15	-5	-4	4	2		1		$3/2$
		3	5	-1	2	-2	-2		$-2/3$		
		-3	-5	-2	-2	2	-1		$2/3$		
		5	3	-2	2	-2	-1		$-4/5$		
		-5	-3	-1	-2	2	-2		$4/5$		
		15	1	-5	4	-4	2		$-29/15$		
		-15	-1	2	-4	4	-5		$29/15$		
$1\ -1\ -1$	$8\ -5$	1	7	-1	2	-2	-4		2		$3/2$
		-1	-7	-4	-2	2	-1	$3/2$	-2		
		7	1	-4	2	-2	-1		$8/7$		
		-7	-1	-1	-2	2	-4		$-8/7$		

Литература

1. L. Di Martino, *The normal structure of the classical modular group*, — Atti del Convegno in onore di F. Brioschi, Istit. Lombardo Accad. Sci. Lett. Rend. (1991).
2. L. Di Martino and M. C. Tamburini, *2-Generation of finite simple groups and some related topics*, — In: Generators and Relations in Groups and Geometries, A.Barlotti et al. (eds.). (1991), 195–233.
3. L. Di Martino and N. Vavilov, (2,3)*-generation of* $\mathrm{SL}_n(q)$*.* I: *Cases* $n = 5, 6, 7$. — Comm. Algebra **22** (1994) no. 4, 1321–1347.
4. L. Di Martino and N. Vavilov, (2,3)*-generation of* $\mathrm{SL}_n(q)$*.* II: *Cases* $n \geq 8$. — Comm. Algebra **24** (1996), 487–515.
5. A. J. Hahn and O. T. O'Meara, *The classical groups and* K*-theory.* — Grundlehr. der math. Wiss. **291**, Springer-Verlag (1989).
6. N. Jacobson, *Basic Algebra* I. 2nd edition, W. H. Freeman and Company, New York (1985).
7. А. Ю. Лузгарев, И. М. Певзнер, *Некоторые факты из жизни* GL(5,$\mathbb{Z}$). — Зап. научн. семин. ПОМИ **305** (2003), 153–162.
8. G. A. Miller, *On the groups generated by two operations.* — Bull. Amer. Math. Soc. **7** (1901), 424–426.
9. Я. Н. Нужин, *Об одном вопросе М. Кондера.* — Матем. заметки **70**, No. 1, (2001) 79–87.
10. P. Sanchini and M. C. Tamburini, *Constructive* (2,3)*-generation: a permutational approach.* — Rend. Sem. Math. Fis. Milano **LXIV** (1994), 141–158.
11. L. L. Scott, *Matrices and cohomology.* — Ann. Math. **105** (1977), 473–492.
12. M. C. Tamburini and J. S. Wilson, *On the* (2,3)*-generation of some classical groups.* II. — J. Algebra **176** (1995), 667–680.
13. M. C. Tamburini, J. S. Wilson and N. Gavioli, *On the* (2,3)*-generation of some classical groups.* I. — J. Algebra **168** (1994), 353–370.

14. M. C. Tamburini, P. Zucca, *On a question of M. Conder.* — Atti Accad. Naz. Lincei, Cl. Sci. Fis. Mat. Nat., IX. Ser., Rend. Lincei, Mat. Appl. **11**, No. 1 (2000), 5–7.

Vsemirnov M. A. Is the group $\mathrm{SL}(6,\mathbb{Z})$ (2,3)-generated?

The problem whether the group $\mathrm{SL}(6,\mathbb{Z})$ can be generated by an involution and an element of order three is considered. The problem is reduced to the question whether $\mathrm{SL}(6,\mathbb{Z})$ is generated by one of eight explicitly written pairs of matrices.

С.-Петербургское отделение
Математического института
им.В. А. Стеклова РАН

E-mail: vsemir@pdmi.ras.ru

Поступило 10 февраля 2006 г.