Записки научных
семинаров ПОМИ
Том 305, 2003 г.

А. Ю. Лузгарёв, И. М. Певзнер

НЕКОТОРЫЕ ФАКТЫ ИЗ ЖИЗНИ $\mathrm{GL}(5,\mathbb{Z})$

1. Общие определения.

Группа G называется $(2,3)$-порожденной, если она может быть порождена инволюцией и элементом порядка 3. Это равносильно тому, что G является нетривиальным эпиморфным образом $\mathrm{PSL}(2,\mathbb{Z})$.

В статьях [1, 2] доказано, что группы $\mathrm{SL}(n,q)$ являются $(2,3)$-порожденными при нечетном $q \neq 9$, $n \geqslant 5$. Более того, высказано предположение, что $(2,3)$-порожденными являются все конечные простые группы типа Ли, кроме нескольких групп небольшого ранга в характеристиках 2 и 3.

В статье [3] доказано, что $(2,3)$-порожденными являются группы $\mathrm{SL}(n,\mathbb{Z})$ при $n \geqslant 13$, $\mathrm{GL}(n,\mathbb{Z})$ при $n \geqslant 19$. С другой стороны, при $n = 2,4$ группы $\mathrm{SL}(n,\mathbb{Z})$ и $\mathrm{GL}(n,\mathbb{Z})$ не являются $(2,3)$-порожденными. В недавней работе [4] было доказано, что группы $\mathrm{SL}(3,\mathbb{Z})$, $\mathrm{GL}(3,\mathbb{Z})$ не являются $(2,3)$-порожденными. Во многом эта работа определила стиль наших исследований. Наша цель – показать, что $\mathrm{GL}(5,\mathbb{Z})$ и $\mathrm{SL}(5,\mathbb{Z})$ также не являются $(2,3)$-порожденными. В данной статье будет осуществлено сведение этого вопроса к конечному числу случаев, более точно, будет доказана следующая теорема.

Теорема 1. *Предположим, что группа* $\mathrm{GL}(5,\mathbb{Z})$ *является* $(2,3)$-*порожденной. Тогда порождающие ее инволюция и элемент порядка три приводятся (соответственно) к виду*

$$A = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & 0 & 0 & a \\ -1 & -1 & 0 & 0 & b \\ 0 & 0 & 0 & 1 & c \\ 0 & 0 & -1 & -1 & d \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \quad (1)$$

где набор (a,b,c,d) совпадает с одним из следующих:

$$\begin{array}{ll}
(1,-1,-2,-2), & (0,-1,-2,-2),\\
(1,-1,-2,4), & (0,-1,4,-8),\\
(-1,1,-2,-2), & (0,1,-2,-2),\\
(-1,1,-2,4), & (0,1,4,-8),\\
(1,-1,1,-3), & (0,-1,0,-1).
\end{array}$$

Мы рассматриваем правое действие $\mathrm{GL}\,(5,\mathbb{Z})$ на свободном модуле $\mathbb{Z}^5$, представленном векторами-строчками. В дальнейшем p – некое простое число, и $f_p : \mathrm{GL}\,(5,\mathbb{Z}) \to \mathrm{GL}\,(5,p)$ – очевидный гомоморфизм. Мы будем часто пользоваться тем, что $\mathrm{Im}\, f_p$ содержит $\mathrm{SL}\,(5,p)$, и, в частности, $\mathrm{Im}\, f_p$ неприводим в смысле действия на строки и на столбцы.

Пусть $\mathrm{GL}\,(5,\mathbb{Z}) = \langle A, B\rangle$, где $A^2 = B^3 = I$. Очевидно, что $\det A = -1$ и $\det B = 1$. Возьмем произвольный ненулевой вектор $x \in \mathbb{Z}^5$ и рассмотрим вектор $x + xB + xB^2 = x(I + B + B^2)$. Заметим, что $(I - B)^2 = I - 2B + B^2 = (I + B + B^2) - 3B$, и если $I + B + B^2 = 0$, то $(I - B)^2 = -3B$, но $\det(-3B) = -3^5$, а $\det(I-B)^2 \geq 0$, и получаем противоречие. Значит, $I+B+B^2 \neq 0$. Следовательно, существует такой x, что $x + xB + xB^2 \neq 0$, и тогда $(x+xB+xB^2)B = x(I+B+B^2)B = x+xB+xB^2$. Мы нашли, таким образом, ненулевой вектор $\omega = x + xB + xB^2 \in \mathbb{Z}^5$ такой, что $\omega B = \omega$.

Заметим, что A фиксирует поточечно подпространство $W \subset \mathbb{Q}^5$, и $\dim W = 4$ или 2.

2. Первый случай ($\dim W = 4$).

Выберем в $W \cap \mathbb{Z}^5$ базис $\{e_1, e_2, e_3, e_4\}$ и дополним его до базиса $\mathbb{Z}^5$ вектором e_5. Пусть $\omega = (\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5)$ в полученном базисе $\{e_1, e_2, e_3, e_4, e_5\}$. Неприводимость $\mathrm{Im}\, f_p$ влечет $\lambda_5 = \pm 1$. Значит, $\{e_1, e_2, e_3, e_4, \omega\}$ – базис $\mathbb{Z}^5$. Таким образом, при переходе к такому базису наши матрицы имеют вид

$$A = \begin{pmatrix} 1 & 0 & 0 & 0 & 0\\ 0 & 1 & 0 & 0 & 0\\ 0 & 0 & 1 & 0 & 0\\ 0 & 0 & 0 & 1 & 0\\ a & b & c & d & -1 \end{pmatrix}, \quad B = \begin{pmatrix} * & * & * & * & *\\ * & * & * & * & *\\ * & * & * & * & *\\ * & * & * & * & *\\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

где a, b, c, d в совокупности взаимно просты. Пусть π – оператор проектирования $\mathbb{Z}^5$ на $\langle e_1, e_2, e_3, e_4\rangle$ параллельно ω. Рассмотрим векторы $f_1 = (a, b, c, d, 0)$ и $\pi(f_1B)$. Они не могут быть коллинеарны, так как иначе $\langle f_1, \omega\rangle$ было бы инвариантно под действием A и B, ибо $\omega A = f_1 - \omega$, $\omega B = \omega$, $f_1A = f_1$ и $f_1B - \pi(f_1B) \parallel \omega$. Значит, на f_1 и $\pi(f_1B)$ натянуто двумерное подпространство $\mathbb{Z}^5$, и вектор f_1 можно дополнить до базиса этого подпространства некоторым вектором f_2. Тогда $\pi(f_1B) \in \langle f_1, f_2\rangle$, и $f_1B \in \langle f_1, f_2, \omega\rangle$. Далее, рассмотрим $\pi(f_2B)$. Если $\pi(f_2B) \in \langle f_1, f_2\rangle$, то $\langle f_1, f_2, \omega\rangle$ инвариантно, значит, можно дополнить $\{f_1, f_2\}$ до базиса подпространства $\langle f_1, f_2, \pi(f_2B)\rangle$ вектором f_3, и $f_2B \in \langle f_1, f_2, f_3, \omega\rangle$. Аналогично, рассмотрим $\pi(f_3B)$: если $\pi(f_2B) \in \langle f_1, f_2, f_3\rangle$, то $\langle f_1, f_2, f_3, \omega\rangle$ инвариантно, и можно дополнить $\{f_1, f_2, f_3\}$ до базиса $\langle f_1, f_2, f_3, \pi(f_2B)\rangle$ вектором f_4. Теперь $\langle f_1, f_2, f_3, f_4\rangle = \langle e_1, e_2, e_3, e_4\rangle$, значит, $\langle f_1, f_2, f_3, f_4, \omega\rangle$ – базис всего $\mathbb{Z}^5$. В этом базисе матрицы A и B примут вид

$$A' = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & -1 \end{pmatrix}, \quad B' = \begin{pmatrix} * & r & 0 & 0 & * \\ * & * & s & 0 & * \\ * & * & * & t & * \\ * & * & * & * & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Вспоминаем, что ${B'}^3 = I$. Прямые вычисления показывают, что

$${B'}^3 = \begin{pmatrix} * & * & * & rst & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Получаем, что $rst = 0$. Но $r = 0$ означает, что $\pi(f_1B) \parallel f_1$, чего быть не может (см. выше). Аналогично $s = 0$ означает, что $\pi(f_2B) \in \langle f_1, f_2\rangle$, и $t = 0$ – что $\pi(f_3B) \in \langle f_1, f_2, f_3\rangle$. Во всех этих случаях получаем противоречие.

3. Второй случай ($\dim W = 2$).

Рассмотрим собственное подпространство $V \subset \mathbb{Q}^5$, соответствующее собственному числу -1 оператора A. Очевидно, что кратность -1 как собственного числа оператора A равна трем, тогда $\dim V = 3$, и $\mathbb{Q}^5 = V \oplus W$.

Посмотрим, сколько может существовать линейно независимых собственных векторов, соответствующих собственному числу 1 оператора B. Если таковых 5, 4 или 3, то подпространство, порожденное ими, обязано пересекаться с V. Любой целочисленный вектор из их пересечения под действием A меняет знак, а под действием B сохраняется. Получаем противоречие. Если таких собственных векторов 2 (обозначим их ω_1 и ω_2), то пусть y – вектор, не являющийся собственным. Тогда yB не коллинеарен y, и $yB^2 \in \langle y, yB, \omega_1, \omega_2\rangle$, потому что $y + yB + yB^2 \in \langle \omega_1, \omega_2\rangle$. Рассмотрим произвольный вектор $z \notin \langle y, yB, \omega_1, \omega_2\rangle$. Пусть αz – проекция zB на $\langle z\rangle$. Тогда $\alpha^2 z$ – проекция zB^2 на $\langle z\rangle$, и $\alpha^3 z$ – проекция zB^3 на $\langle z\rangle$. Но $zB^3 = z$, то есть $\alpha^3 = 1$. Значит, $\alpha = 1$, и проекция $z + zB + zB^2$ на $\langle z\rangle$ есть $3z$. Однако $z + zB + zB^2$ инвариантен под действием B, то есть лежит в $\langle \omega_1, \omega_2\rangle$, поэтому его проекция на $\langle z\rangle$ равна нулю. Значит, $z = 0$, и снова получаем противоречие. Таким образом, у B есть только один собственный вектор, соответствующий 1 – это ω (с точностью до умножения на константу).

Заметим, что попутно мы показали, что для любого вектора y выполнено $yB^2 \in \langle y, yB, \omega\rangle$ (потому что $y + yB + yB^2 \parallel \omega$).

Выберем в $V \cap \mathbb{Z}^5$ базис $\{e_1, e_2, e_3\}$ и дополним его до базиса в $\mathbb{Z}^5$ векторами e_4' и e_5'. Запишем вектор ω в этом базисе: $\omega = (a_1, a_2, a_3, a_4, a_5)$. Заметим, что из неприводимости $\operatorname{Im} f_p$ для всех простых p следует, что a_4 и a_5 взаимно просты, то есть найдутся $u, v \in \mathbb{Z}$ такие, что $a_4 u + a_5 v = 1$. Тогда мы можем заменить $\{e_4', e_5'\}$ на векторы $e_4 = (0, 0, 0, v, -u)$ и ω, и получим новый базис $\{e_1, e_2, e_3, e_4, \omega\}$. В этом базисе наши операторы будут задаваться следующими матрицами:

$$A = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ * & * & * & 1 & 0 \\ * & * & * & 0 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ * & * & * & * & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Рассмотрим трехмерное подпространство $\mathbb{Q}^5$, порожденное векторами $e_1 B$, $e_2 B$ и $e_3 B$. Оно пересекается с V по подпространству размерности не менее 1. Это означает, что найдется вектор $f_1 \in V \cap \mathbb{Z}^5$ с взаимно простыми в совокупности координатами такой, что $f_1 B$ также лежит в $V \cap \mathbb{Z}^5$. Если $f_1 \parallel f_1 B$, то пространство, порожденное f_1 инвариантно относительно действия A и B.

Значит, на f_1 и f_1B натянуто двумерное подпространство. Выбираем в нем f_2, дополняющий f_1 до базиса. f_2 представляется в виде линейной комбинации f_1 и f_1B. Значит, f_2B представляется в виде линейной комбинации f_1B и f_1B^2, а f_1B^2 выражается через f_1, f_1B и ω, потому что $f_1 + f_1B + f_1B^2$ является собственным вектором матрицы B и, следовательно, коллинеарен ω. Получаем, что f_2B выражается через f_1, f_1B и ω. Дополним f_1 и f_2 до базиса подпространства V некоторым вектором f_3. В базисе $\langle f_1, f_2, f_3, e_4, \omega\rangle$ матрицы операторов примут следующий вид:

$$A' = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ * & * & * & 1 & 0 \\ b_1 & b_2 & b_3 & 0 & 1 \end{pmatrix}, \quad B' = \begin{pmatrix} * & * & 0 & 0 & * \\ * & * & 0 & 0 & * \\ * & * & * & * & * \\ * & * & * & * & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Здесь $b_3 = \pm 1$, потому что иначе для некоторого простого p подпространство $f_p(\langle f_1, f_2, \omega\rangle)$ инвариантно под действием матриц A' и B'. Меняя при необходимости знак f_3, можно считать, что $b_3 = 1$. Пусть $f_3' = f_3 + b_1f_1 + b_2f_2$. В базисе $\langle f_1, f_2, f_3', e_4, \omega\rangle$ матрицы операторов примут следующий вид:

$$A'' = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ * & * & * & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad B'' = \begin{pmatrix} * & * & 0 & 0 & * \\ * & * & 0 & 0 & * \\ k_1 & k_2 & k_3 & k & l \\ * & * & * & * & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Докажем, что $k = \pm 1$. Действительно, иначе после редукции по некоторому простому модулю p образ подпространства $\langle f_1, f_2, f_3', \omega\rangle$ будет инвариантным подпространством для A и B – противоречие. Меняя при необходимости знак у e_4, можем считать, что $k = 1$. Пусть $f_4 = e_4 + k_1f_1 + k_2f_2 + k_3f_3'$. Тогда $f_3'B = k_1f_1 + k_2f_2 + k_3f_3' + e_4 + l\omega = f_4 + l\omega$, и f_4B выражается через $f_3'B^2$ и ω, а $f_3'B^2$ выражается через $f_3', f_3'B$ и ω (выше мы доказали этот факт для произвольного вектора y). Значит, f_4B выражается через $f_3', f_3'B$ и ω, и, так как $f_3'B = f_4 + l\omega$, то $f_4B = \alpha_1f_3' + \alpha_2f_4 + \alpha_3\omega$ для некоторых $\alpha_1, \alpha_2, \alpha_3 \in \mathbb{Q}$. Тогда $f_4B^2 = \alpha_1(f_4 + l\omega) + \alpha_2(\alpha_1f_3' + \alpha_2f_4 + \alpha_3\omega) + l\omega$. Так как $f_3'B = f_4 + l\omega$, то $f_4 = f_3'B - l\omega$, и $f_4B^2 = f_3' - l\omega$. Приравнивая правые части, получаем, что $\alpha_2\alpha_1 = 1$, $\alpha_1 + \alpha_2^2 = 0$, $\alpha_1 l + \alpha_2\alpha_3 + l = -l$. Отсюда

$\alpha_1 = -1$, $\alpha_2 = -1$. Значит, $f_4B = -f_3 - f_4 + \alpha_3\omega$. Тогда в базисе $\langle f_1, f_2, f_3', f_4, \omega\rangle$ матрицы операторов примут вид:

$$A'' = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ \beta_1 & \beta_2 & * & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad B'' = \begin{pmatrix} * & * & 0 & 0 & * \\ * & * & 0 & 0 & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & -1 & -1 & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix},$$

где β_1 и β_2 – некоторые взаимно простые целые числа. Тогда вектор $g_1 = (\beta_1, \beta_2, 0, 0, 0)$ можно дополнить до базиса $\langle f_1, f_2\rangle$ некоторым вектором g_2. Теперь в новом базисе $\{g_1, g_2, f_3', f_4, \omega\}$ матрицы операторов будут выглядеть так:

$$A''' = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & * & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad B''' = \begin{pmatrix} \gamma_1 & \gamma_2 & 0 & 0 & * \\ \delta_1 & \delta_2 & 0 & 0 & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & -1 & -1 & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Заметим, что $\gamma_2 = \pm 1$ (иначе опять противоречие с неприводимостью $\operatorname{Im} f_p$ – подпространство $\langle g_1, f_3', f_4, \omega\rangle$ перейдет в инвариантное для A и B). Меняя при необходимости знак g_2, можно считать, что $\gamma_2 = 1$. Матрица $\begin{pmatrix} \gamma_1 & 1 \\ \delta_1 & \delta_2 \end{pmatrix}$ имеет порядок 3 и след -1. Пусть $Y = \operatorname{diag}\left(\begin{pmatrix} 1 & 0 \\ -\gamma_1 & 1 \end{pmatrix}, 1, 1, 1\right)$. Проводя сопряжение B'' при помощи Y, получаем, что матрицы операторов записываются следующим образом:

$$A'''' = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & r & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \quad B'''' = \begin{pmatrix} 0 & 1 & 0 & 0 & * \\ -1 & -1 & 0 & 0 & * \\ 0 & 0 & 0 & 1 & * \\ 0 & 0 & -1 & -1 & * \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

Теперь пусть $Y' = \operatorname{diag}\left(1, 1, 1, \begin{pmatrix} 1 & r \\ 0 & 1 \end{pmatrix}\right)$. После сопряжения B'''' при помощи Y' матрицы операторов выглядят так (переименуем их обратно в A и B):

$$A = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}, \ B = \begin{pmatrix} 0 & 1 & 0 & 0 & a \\ -1 & -1 & 0 & 0 & b \\ 0 & 0 & 0 & 1 & c \\ 0 & 0 & -1 & -1 & d \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}. \quad (2)$$

4. Дальнейшие шаги.

Рассмотрим вектор $(k, l, 0, 0, 0) \in \mathbb{Z}^5$. Под действием матрицы A он переходит в противоположный, а под действием матрицы B – в вектор $(-l, k-l, 0, 0, ka+lb)$. Напишем условия, при выполнении которых полученный вектор оказывается коллинеарен первоначальному:

$$ka + lb = 0, \quad k(k-l) = l(-l)$$

(как и раньше, достаточно, чтобы это равенство выполнялось по какому-нибудь простому модулю). Сразу заметим, что нас интересует случай, когда a и b не равны одновременно 0 (иначе первые два вектора базиса образуют инвариантное подпространство).

Из этих уравнений получаем: $k = bt$, $l = -at$, и $a^2 + ab + b^2 = 0$. Значит, если $a^2+ab+b^2 \equiv 0 \pmod p$ для некоторого p, то одномерное подпространство, порожденное вектором $(k, l, 0, 0, 0)$, является инвариантным. Если же это не выполняется ни для какого p, то $a^2 + ab + b^2 = 1$ или $a^2 + ab + b^2 = -1$. Решая эти квадратные уравнения, получаем шесть различных возможностей для пары чисел (a, b):

$$(a, b) = (0,1), (0,-1), (-1,0), (-1,1), (1,-1) \ \text{ или } \ (1,0).$$

Рассмотрим теперь вектор $P = (x, 0, y, 2x, 2y)$. Сразу заметим, что он является собственным для матрицы A: $PA = P$. Вычисления показывают, что $PB = (0, x, -2x, y-2x, xa+yc+2xd+2y)$, $PB^2 = (-x, -x, -y+2x, -y, x(b+a)+y(d+c)-2xc+2y)$ и $P + PB + PB^2 = (0, 0, 0, 0, 6y+2xa+2yc+2xd+xb+yd-2xc)$. Поэтому потребуем, чтобы $P + PB + PB^2 = (0, 0, 0, 0, 0)$, что даст нам одно уравнение на x и y. Посмотрим теперь на вектор $PBA = (y-2x, -x, 2x+xa+yc+2xd+2y, y-2x, xa+yc+2xd+2y)$. Попробуем выразить его в виде линейной комбинации P и PB. Замечаем, что $PBA+PB = (y-2x, 0, xa+yc+2xd+2y, 2y-4x, 2xa+2yc+4xd+4y)$, и есть надежда на то, что этот вектор коллинеарен P. Эта надежда записывается в виде еще одного уравнения: $x(xa+yc+2xd+2y) = y(y-2x)$. Значит, если выполнены оба уравнения системы

$$\begin{cases} 6y+2xa+2yc+2xd+xb+yd-2xc=0 \\ x(xa+yc+2xd+2y)-y(y-2x)=0 \end{cases} \tag{3}$$

по какому-нибудь простому модулю p, то векторы P и PB образуют инвариантное подпространство (мы проверили, что PA, PB^2 и PBA через них выражаются).

Попытаемся решить эти уравнения. Первое уравнение линейное и имеет вид $yh=-xg$ (где $h=6+2c+d$, $g=2a+2d-2c+b$). Сначала докажем следующий факт.

Лемма 1. *Если $g \equiv h \equiv 0 \pmod p$ для некоторого простого числа p, то матрицы A и B не порождают $\mathrm{GL}(5,\mathbb{Z})$.*

Доказательство. Тогда первое уравнение системы имеет вид $0=0$ и выполняется всегда, а оставшееся уравнение является однородным квадратным. То есть это квадратное уравнение относительно y/x:

$$-\left(\frac{y}{x}\right)^2+(c+4)\frac{y}{x}+(2d+a)=0. \tag{4}$$

Конечно, может так случиться, что это уравнение вообще не имеет корней в $\mathbb{Z}/p\mathbb{Z}$, но это не так страшно. Рассмотрим алгебраическое замыкание $\mathbb{Z}/p\mathbb{Z}$, которое обозначим через K. В этом поле наше уравнение имеет решение, и, таким образом, найдется вектор $P \in K^5$ такой, что векторы P и PB порождают подпространство, инвариантное относительно действия матриц A и B, рассматриваемых как элементы $\mathrm{GL}(5,K)$. Рассмотрим, например, матрицу T в $\mathrm{GL}(5,\mathbb{Z})$, которая прибавляет к четвертой компоненте вектора первую. Конечно, эта матрица, рассматриваемая как элемент $\mathrm{GL}(5,K)$, делает ровно то же самое. Если матрицы A и B порождают $\mathrm{GL}(5,\mathbb{Z})$, то T записывается как произведение некоторого числа матриц A и B, и PT должно лежать в нашем инвариантном подпространстве K^5. Значит, PT должно быть линейной комбинацией P и PB, но $PT=(x,0,y,3x,2y)$, причем $x \neq 0$, так как оно получилось при решении квадратного уравнения относительно y/x. Значит, коэффициент при PB в этой линейной комбинации равен нулю (на втором месте у вектора PT стоит 0), и PT пропорционален P, чего быть не может. Получили противоречие. $\square$

Рассмотрим выражение

$$(a+2d)h^2+(c+4)hg-g^2. \tag{5}$$

Если оно не равно ± 1, то найдется простое число p, по модулю которого оно равно 0. Если $h \equiv 0 \pmod p$, то из выражения (5) видно, что и $g \equiv 0 \pmod p$, и мы попадаем в условия леммы. Поэтому можно считать $h \not\equiv 0 \pmod p$. Тогда возьмем в качестве x любое число, не делящееся на p, и $y = xg/h$. Легко проверить, что пара (x, y) является нетривиальным решением системы (3) по модулю p (первое уравнение выполняется в силу выбора y, а второе – в силу выбора p, для которого выражение (5) равно нулю). Значит, надежды на инвариантное подпространство в этом случае оправдались.

Оставшийся случай – выражение (5) равно 1 или -1.

Каждый из этих случаев приводит нас к уравнению относительно a, b, c и d, которое мы будем решать в целых числах. К тому же мы знаем, какие значения могут принимать a и b. Введем новую переменную $t = 2c + d$ и заменим в нашем уравнении d на $t-2c$. Оказывается, что получившееся выражение будет квадратным относительно t. Далее мы записываем формулу для решения квадратного уравнения и видим, что дискриминант (он зависит от a, b и t) должен быть квадратом целого числа. Подставляя известные нам значения для a и b, находим соответствующие им значения t, при которых это так, и проверяем, что при этих значениях a, b и t решение квадратного уравнения относительно c также целое. Отдельно рассматривается случай вырожденного квадратного уравнения. Вся эта деятельность приводит к десяти возможностям для набора (a, b, c, d):

$$\begin{array}{ll}
(1,-1,-2,-2), & (0,-1,-2,-2),\\
(1,-1,-2,4), & (0,-1,4,-8),\\
(-1,1,-2,-2), & (0,1,-2,-2),\\
(-1,1,-2,4), & (0,1,4,-8),\\
(1,-1,1,-3), & (0,-1,0,-1).
\end{array}$$

На самом деле число этих возможностей сокращается до пяти следующим образом: для каждой пары матриц (A, B) можно рассмотреть пару (A, B^2), которая порождает (или не порождает) $\mathrm{GL}(5, \mathbb{Z})$ с тем же успехом. Если в такой паре матрицу B^2 привести к виду, указанному в (2), то получится некий другой набор (a, b, c, d). Таким образом наборы разбиваются на пары; достаточно исследовать вопрос о порождении $\mathrm{GL}(5, \mathbb{Z})$ только одним набором из каждой пары (выше парные наборы стоят в одной строке).

Литература

1. L. Di Martino and N. Vavilov, *(2,3)-generation of* $\mathrm{SL}(n,q)$. I. *Cases* $n = 5, 6, 7$. — Comm. Algebra **22**(4) (1994), 1321–1347.
2. L. Di Martino and N. Vavilov, *(2,3)-generation of* $\mathrm{SL}(n,q)$. II. *Cases* $n \geqslant 8$. — Comm. Algebra **24**(2) (1996), 487–515.
3. P. Sanchini and M. C. Tamburini, *Constructive (2,3)-generation: a permutational approach.* — Rend. Sem. Math. Fis. Milano **LXIV** (1994), 141–158.
4. M. C. Tamburini and P. Zucca, *On a question of M. Condor.* — Atti Accad. Naz. Lincei Rend. **11**(9) (2000), 5–7.

Luzgarev A. Yu., Pevzner I. M. Private life of $\mathrm{GL}(5, \mathbb{Z})$.

The paper investigates $(2, 3)$-generation of $\mathrm{GL}(5, \mathbb{Z})$. We reduce the problem to five specific pairs of matrices.

С.-Петербургский
государственный
университет

Поступило 10 ноября 2003 г.