Препринт ПОМИ — 26/2006

ГРУППА $\mathrm{GL}(6,\mathbb{Z})$ $(2,3)$-ПОРОЖДЕНА

М. А. Всемирнов [1]
Санкт-Петербургское отделение Математического института
им. В. А. Стеклова Российской академии наук
191023, С.-Петербург, наб. р. Фонтанки, д. 27
http://logic.pdmi.ras.ru˜ vsemir
e-mail: vsemir@pdmi.ras.ru

29 декабря 2006 г.

Аннотация

В данной работе доказывается, что группа $\mathrm{GL}(6,\mathbb{Z})$ может быть порождена парой матриц, имеющих порядок 2 и 3, соответственно. Образующие предъявлены в явном виде.

[1] При поддержке программы фундаментальных исследований РАН "Современные проблемы теоретической математики" и гранта "Научные школы" (грант НШ-8464-2006-1)

Хорошо известно, что модулярная группа $\mathrm{PSL}(2,\mathbb{Z})$ изоморфна свободному произведению циклической группы порядка 2 циклической группы порядка 3: $\mathrm{PSL}(2,\mathbb{Z}) \simeq C_2 * C_3$. Следовательно, за исключением тривиальных примеров $\{1\}$, C_2 и C_3, любой другой гомоморфный образ модулярной группы порождается инволюцией и элементом порядка три. Такие группы также известны как $(2,3)$-*порожденные* группы.

Как показано в [5], группы $\mathrm{SL}(n,\mathbb{Z})$ и $\mathrm{GL}(n,\mathbb{Z})$ являются $(2,3)$-порожденными при $n \geq 13$ и $n \geq 19$, соответственно. С другой стороны, $\mathrm{SL}(4,\mathbb{Z})$ и $\mathrm{GL}(4,\mathbb{Z})$ не $(2,3)$-порожденные, поскольку $(2,3)$-порожденной не является даже $\mathrm{SL}(4,2) \simeq \mathrm{GL}(4,2) \simeq \mathrm{Alt}(8)$. Также известно, что $\mathrm{SL}(3,\mathbb{Z})$ и $\mathrm{GL}(3,\mathbb{Z})$ не $(2,3)$-порождены [4], [6].

Задача о $(2,3)$-порожденности групп $\mathrm{GL}(5,\mathbb{Z})$ и $\mathrm{SL}(6,\mathbb{Z})$ рассматривалась в [3] и [7], соответственно. Эти работы не дают окончательного ответа, однако содержат сведение исходной задачи к разбору конечного числа явно указанных случаев. Ряд исследователей полагал, что ответ должен быть отрицательным и в большинстве оставшихся неразобранными случаев при $n \leq 12$. В данной работе мы покажем, что, вопреки этим ожиданиям, группу $\mathrm{GL}(6,\mathbb{Z})$ все же можно породить инволюцией и элементом порядка 3.

Теорема 1. *Группа* $\mathrm{GL}(6,\mathbb{Z})$ *является* $(2,3)$*-порожденной. А именно, пусть*

$$x = \begin{pmatrix} 1 & -3 & 0 & 0 & 0 & 2 \\ 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & -1 & 0 & 0 \\ 0 & -1 & -1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix}, \qquad y = \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & -1 & 0 & 1 & 0 & -1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & -2 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{pmatrix}.$$

Тогда $x^2 = y^3 = I$ *и* $\mathrm{GL}(6,\mathbb{Z}) = \langle x, y\rangle$.

Далее используются следующие обозначения. Как обычно e_{ij}, $1 \leq i,j \leq 6$ — это элементы стандартного базиса матричной алгебры (так называемые "матричные единицы"), а $t_{ij}(\xi)$ — элементарная трансвекция

$$t_{ij}(\xi) = I + \xi e_{ij}, \qquad i \neq j,\ \xi \in \mathbb{Z}.$$

Доказательство теоремы 1. Утверждение о порядках матриц x и y очевидно. Для доказательства совпадения $\langle x, y\rangle$ и $\mathrm{GL}(6,\mathbb{Z})$ мы используем хорошо известный факт, что при $n \geq 3$ группа $\mathrm{SL}(n,\mathbb{Z})$ порождается элементарными транвекциями $t_{ij}(1)$, $1 \leq i \neq j \leq n$; см., например, [2]. Таким образом, наша задача сводится к нахождению этих трансвекций в группе $\langle x, y\rangle$. Однако начнем мы с более слабого результата, утверждающего, что $\langle x, y\rangle$ содержит достаточно много трансвекции вида $t_{ij}(4)$.

Непосредственные вычисления дают нам, что

$$\begin{aligned} z_1 &:= (xyxy^2)^6 = t_{12}(4), && (1)\\ z_2 &:= yz_1y^2 = t_{34}(4), && (2)\\ z_3 &:= y^2z_1y = t_{56}(4). && (3) \end{aligned}$$

Положим

$$\begin{aligned} z_4 &:= xyz_1y^2x = I + 4e_{42} + 4e_{43},\\ z_5 &:= xy^2xy(xyxy^2)^2(xy)^2xy^2(xy)^2(xyxy^2)^2,\\ z_6 &:= xy^2xyx. \end{aligned}$$

Несложно проверить, что

$$\begin{aligned} z_7 &:= z_5^{-1}z_4z_5 = I + 8e_{41} + 4e_{43} - 8e_{45} + 12e_{46},\\ z_8 &:= z_5z_4z_5^{-1} = I + 16e_{41} - 40e_{42} - 12e_{43} - 4e_{45} + 36e_{46},\\ z_9 &:= z_6z_5z_4z_5^{-1}z_6^{-1} = I + 8e_{41} - 8e_{42} - 4e_{43} - 4e_{45} + 8e_{46},\\ z_{10} &:= z_6z_5^{-1}z_4z_5z_6^{-1} = I + 20e_{41} - 56e_{42} - 16e_{43} - 8e_{45} + 36e_{46},\\ z_{11} &:= z_5^2z_4z_5^{-2} = I - 92e_{41} + 244e_{42} + 120e_{43} - 232e_{46}. \end{aligned}$$

В частности, z_4, z_7, z_8, z_9, z_{10} и z_{11} попарно коммутируют. Из приведенных равенств легко выводится, что

$$\begin{aligned} z_{12} &:= z_4^{19}z_7^5z_8^{-23}z_9^{-7}z_{10}^{10}z_{11}^{-2} = t_{42}(4), && (4)\\ z_{13} &:= z_4z_{12}^{-1} = t_{43}(4). && (5) \end{aligned}$$

Замечание 1. К сожалению, на данном этапе, используя только z_4, $z_7,\ldots$, z_{11}, можно найти лишь $t_{41}(12)$, $t_{45}(12)$, $t_{46}(12)$, но не $t_{41}(4)$, $t_{45}(4)$, $t_{46}(4)$. Поэтому нам потребуются и другие соотношения.

Далее имеем:

$$
\begin{aligned}
z_{14} &:= xz_{12}x = t_{32}(4), && (6)\\
z_{15} &:= yz_{14}y^2 = t_{54}(4), && (7)\\
z_{16} &:= y^2z_{14}y = t_{16}(4), && (8)\\
z_{17} &:= y^2xyz_{14}^{-1}y^2xyz_{14}z_2^{-1} = t_{31}(4), && (9)\\
z_{18} &:= yz_{12}yz_{16}^{-1}z_3yz_2^{-2} = t_{64}(4), && (10)\\
z_{19} &:= y^2z_{17}yz_1^{-1} = t_{15}(4). && (11)
\end{aligned}
$$

Положим теперь

$$
\begin{aligned}
z_{20} &:= (y^2x)^2yx(y^2x)^3yxy^2xyx,\\
z_{21} &:= (yxyxy^2x)^2yxy^2xyx.
\end{aligned}
$$

Получаем, что

$$
\begin{aligned}
z_{22} &:= z_{21}z_2z_{21}^{-1}z_2z_{15}^3z_{18}^2 = t_{14}(4), && (12)\\
z_{23} &:= z_{20}z_2^{-1}z_{20}^{-1}z_{22}^{-1}z_2^4z_{15}^4z_{18}^2 = t_{24}(4), && (13)\\
z_{24} &:= xz_{22}^{-1}xz_1^{-1} = t_{13}(4), && (14)\\
z_{25} &:= yz_{22}y^2 = t_{36}(4), && (15)\\
z_{26} &:= y^2z_{22}y = t_{52}(4), && (16)\\
z_{27} &:= y^2z_{23}yz_1^{-1}z_{14}^{-2} = t_{62}(4), && (17)\\
z_{28} &:= xz_{25}x = t_{46}(4), && (18)\\
z_{29} &:= y^2z_{12}yz_{16}^{-1}z_{25}z_3 = t_{26}(4), && (19)\\
z_{30} &:= yxy^2xz_{10}xyxy^2z_2^{-4}z_{14}^{-2}z_{17}^5z_{25}^3 = t_{35}(4), && (20)\\
z_{31} &:= xz_{30}^{-1}xz_{12}^{-2}z_{28} = t_{45}(4), && (21)\\
z_{32} &:= z_{10}z_8^{-1}z_{12}^4z_{13}z_{31} = t_{41}(4). && (22)
\end{aligned}
$$

Соотношения (1)–(22) дают нам 22 трансвекции $t_{ij}(4)$. Можно продолжить в том же духе и найти соотношения, задающие оставшиеся трансвекции (а именно $t_{21}(4)$, $t_{23}(4)$, $t_{25}(4)$, $t_{51}(4)$, $t_{53}(4)$, $t_{61}(4)$, $t_{63}(4)$, $t_{65}(4)$) в виде слов от x и y. Однако мы опускаем эти соотношения, поскольку они не используются в дальнейшем.

Теперь мы готовы к тому, чтобы выразить трансвекции $t_{ij}(1)$ через x и y. Коммутационное тождество

$$
t_{ij}(\xi)t_{jk}(\zeta)t_{ij}(\xi)^{-1}t_{jk}(\zeta)^{-1} = t_{ij}(\xi)t_{jk}(\zeta)t_{ij}(-\xi)t_{jk}(-\zeta) = t_{ik}(\xi\zeta), \qquad (23)
$$

верное для всех попарно различных индексов i, j, k, позволяет ограничиться нахождением $t_{ij}(1)$ и $t_{jk}(1)$ для какого-то одного фиксированного j. Положим

$$
\begin{aligned}
h_1 &:= (xyxy^2)^3,\\
h_2 &:= (xy^2)^2(xyxy^2)^2xy^2x,\\
h_3 &:= z_1^{-2}z_{26}z_{27}(h_1h_2h_1^{-1}h_2^{-1})^2 = I + 6e_{41} + 9e_{42} - 6e_{45} + 6e_{46},\\
h_4 &:= z_5h_3z_5^{-1} = I - 6e_{41} + 18e_{42} - 18e_{43} + 15e_{45} + 12e_{46},\\
h_5 &:= z_5^{-1}h_3z_5 = I + 75e_{41} + 81e_{42} + 81e_{43} - 102e_{45} + 183e_{46},\\
h_6 &:= z_5z_6^{-1}h_3z_6z_5^{-1} = I - 144e_{41} + 384e_{42} + 204e_{43} - 6e_{45} - 375e_{46},\\
h_7 &:= z_6h_3z_6^{-1} = I + 27e_{41} - 75e_{42} - 21e_{43} - 6e_{45} + 54e_{46}.
\end{aligned}
$$

Заметим, что h_3, h_4, h_5, h_6, h_7 и z_{12}, z_{13}, z_{28}, z_{31}, z_{32} коммутируют. Тогда

$$h_8 := z_{12}^{-95}z_{13}^{-66}z_{28}^{36}z_{31}^{27}z_{32}^{12}h_3^{-1}h_5h_6h_7 = t_{42}(1), \tag{24}$$
$$h_9 := z_{12}^{42}z_{13}^{6}z_{28}^{-24}z_{31}^{7}z_{32}^{-15}h_4^{-1}h_7^2 = t_{45}(1), \tag{25}$$
$$h_{10} := z_{12}^{-105}z_{13}^{-42}z_{28}^{88}z_{31}^{-6}z_{32}^{39}h_4^2h_6 = t_{46}(1), \tag{26}$$
$$h_{11} := xh_8x = t_{32}(1), \tag{27}$$
$$h_{12} := yh_{11}y^2 = t_{54}(1) \tag{28}$$
$$h_{13} := y^2h_{11}y = t_{16}(1), \tag{29}$$
$$h_{14} := xh_{10}x = t_{36}(1), \tag{30}$$
$$h_{15} := y^2h_{14}y = t_{14}(1), \tag{31}$$
$$h_{16} := h_{12}h_{10}h_{12}^{-1}h_{10}^{-1} = t_{56}(1), \tag{32}$$
$$h_{17} := h_{15}h_8h_{15}^{-1}h_8^{-1} = t_{12}(1), \tag{33}$$
$$h_{18} := h_{15}h_9h_{15}^{-1}h_9^{-1} = t_{15}(1), \tag{34}$$
$$h_{19} := yh_{17}y^2 = t_{34}(1), \tag{35}$$
$$h_{20} := yh_{18}y^2h_{19} = t_{31}(1), \tag{36}$$
$$h_{21} := xh_{11}^3h_{14}^{-2}h_{20}^{-1}x = t_{41}(1), \tag{37}$$
$$h_{22} := xh_{19}h_{11}^{-1}x = t_{43}(1), \tag{38}$$
$$h_{23} := y^2h_{10}h_{13}h_{14}^{-1}h_{16}y = t_{24}(1), \tag{39}$$
$$h_{24} := yh_8h_{11}^{-1}h_{17}^{-1}y^2 = t_{64}(1). \tag{40}$$

Соотношения (37), (24), (38), (25), (26), (31), (39), (35), (28), (40) дают нам, что при всех $i,k \in \{1,2,3,5,6\}$ трансвекции $t_{i4}(1)$ и $t_{4k}(1)$ принадлежат $\langle x,y\rangle$. Используя тождество (23), заключаем, что все трансвекции $t_{ij}(1)$ принадлежат $\langle x,y\rangle$.

Следовательно, группа $\langle x, y\rangle$ содержит $\mathrm{SL}(6,\mathbb{Z}) = \langle t_{ij}(1) : 1 \leq i \neq j \leq 6\rangle$. Последняя имеет индекс 2 в $\mathrm{GL}(6,\mathbb{Z})$. Очевидно, что $\langle x, y\rangle$ содержит матрицу определителя -1; например, в качестве таковой можно взять x. Следовательно, $\langle x, y\rangle = \mathrm{GL}(6,\mathbb{Z})$. □

В заключение, кратко опишем метод, при помощи которого были найдены матрицы x и y. Отправной точкой явилась следующая пара параметрических матриц

$$x_1 = \begin{pmatrix} 0 & 0 & 1 & 0 & r_1 & r_2 \\ 0 & 0 & 0 & 1 & r_3 & r_4 \\ 1 & 0 & 0 & 0 & -r_2 & -r_1 \\ 0 & 1 & 0 & 0 & -r_4 & -r_3 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}, \qquad y_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & r_5 & r_6 \\ 0 & 1 & 0 & 0 & r_7 & r_8 \\ 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 & 0 & -1 \end{pmatrix}.$$

Они имеют порядок 2 и 3, соответственно. Следующий шаг состоит в нахождении параметров $r_1,\ldots,r_8$, для которых некоторая степень коммутатора $[x, y]$ является трансвекцией (не обязательно элементарной). Для этой цели естественно ограничиться случаем, когда 1 является двойным корнем характеристического многочлена для $[x, y]$, а остальные корни простые и имеют конечный мультипликативный порядок. Более точно, было наложено следующее условие: характеристический многочлен матрицы $[x, y]$ равен

$$(w^2 + w + 1)(w^2 - w + 1)(w^2 - 2w + 1).$$

Это условие можно записать в виде системы полиномиальных уравнений в неизвестных $r_1,\ldots,r_8$. Автор не ставил целью полностью решить эту систему. Вместо этого, перебирались "небольшие" ее решения и "просеивались" с целью исключения тех случаев, когда x_1 и y_1 с большой долей вероятности не порождают $\mathrm{GL}(6,\mathbb{Z})$. Применялся следующий вероятностный тест. Для каждого простого числа $p < 100$, вычислялись порядки 100 случайных элементов из группы $\langle x_1 \bmod p, y_1 \bmod p\rangle$. Если наименьшее общее кратное этих порядков не делилось на $p^6 - 1$ или $p^5 - 1$, то соответствующее решение отбрасывалось. Данный этап неизбежно требовал привлечения компьютерных вычислений. Автор применял систему компьютерной алгебры MAGMA [1]. Используя описанный выше метод, автор нашел следующее решение, которое проходило все тесты:

$r_1 = r_2 = r_4 = 0$, $r_3 = r_5 = 1$, $r_6 = r_8 = -2$, $r_7 = -1$. Затем был выбран новый базис решетки $\mathbb{Z}^6$, такой, что матрица $[x,y]^6$ и некоторые сопряженные с ней имели достаточно простой вид; см. (1)–(3). Так были найдены матрицы x и y.

Следует подчеркнуть, что применявшийся тест никоим образом не гарантирует, что найденные матрицы порождают всю группу $\mathrm{GL}(6,\mathbb{Z})$. К счастью, в данном случае оказывается, что $\langle x,y\rangle = \mathrm{GL}(6,\mathbb{Z})$, и приведенное выше строгое доказательство теоремы 1 полностью независимо от каких-либо предварительных вычислений.

Список литературы

[1] W. Bosma, J. Cannon, and C. Playoust. The Magma algebra system. I. The user language. Computational algebra and number theory (London, 1993). *J. Symbolic Comput.* **24** (1997), no. 3–4, 235–265.

[2] A. J. Hahn and O. T. O'Meara. *The classical groups and K-theory*, Grundlehren der mathematischen Wissenschaften, **291**, Springer-Verlag, 1989.

[3] A.Yu. Luzgarev and I.M. Pevzner. On a private life of $\mathrm{GL}(5,\mathbb{Z})$. *Zap. Nauchn. Sem. POMI* **305** (2003), 153–162 (in Russian).

[4] Ya. N. Nuzhin. On a question of M. Conder. *Mat. Zametki* **70** (2001) no.1, 79–87 (in Russian).

[5] P. Sanchini and M.C. Tamburini. Constructive $(2,3)$-generation: a permutational approach. *Rend. Sem. Math. Fis. Milano* **LXIV** (1994), 141–158.

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

[7] M.A. Vsemirnov. Is the group $\mathrm{SL}(6,\mathbb{Z})$ $(2,3)$-generated? *Zap. Nauchn. Sem. POMI* **330** (2006), 101–130 (in Russian).