Владикавказский математический журнал
2009, Том 11, выпуск 4, С. 59–62

УДК **512.544.2**

ПОРОЖДАЮЩИЕ ТРОЙКИ ИНВОЛЮЦИЙ ЛИНЕЙНЫХ ГРУПП РАЗМЕРНОСТИ 2 НАД КОЛЬЦОМ ЦЕЛЫХ ЧИСЕЛ

Я. Н. Нужин, И. А. Тимофеенко

Для групп $GL_2(\mathbb{Z})$ и $PGL_2(\mathbb{Z})$ найдено минимальное число порождающих инволюций, произведение которых равно 1. Установлено, что $PGL_2(\mathbb{Z})$ порождается тремя инволюциями, две из которых перестановочны, а $GL_2(\mathbb{Z})$ такими инволюциями не обладает.

Ключевые слова: кольцо целых чисел, линейная группа, порождающие тройки инволюций.

Пусть $GL_n(\mathbb{Z})$ — группа обратимых $(n \times n)$-матриц над кольцом целых чисел $\mathbb{Z}$, $SL_n(\mathbb{Z})$ — ее подгруппа матриц с определителем, равным 1, $PGL_n(\mathbb{Z})$ и $PSL_n(\mathbb{Z})$ — соответственно их фактор-группы по подгруппам скалярных матриц.

В данной заметке для линейных групп размерности 2 над кольцом целых чисел рассматриваются следующие задачи.

А) *Порождается ли данная группа G тремя инволюциями?*

Б) *Порождается ли данная группа G тремя инволюциями, две из которых перестановочны?*

В) *Каково минимальное число порождающих инволюций $n(G)$ группы G, произведение которых равно 1?*

В группе $SL_2(\mathbb{Z})$ единственная инволюция, а группа $PSL_2(\mathbb{Z})$ является свободным произведением двух циклических групп порядка 2 и 3 [1]. Поэтому эти группы не порождаются никаким множеством инволюций и для них вопросы А), Б), В) закрыты.

Для группы $G = PGL_2(\mathbb{Z})$ получен положительный ответ на вопрос Б) и доказано, что $n(G) = 5$.

Для группы $G = GL_2(\mathbb{Z})$ на вопрос А) получен положительный ответ, а на вопрос Б) — отрицательный, и доказано, что $n(G) = 6$.

1. Порождаемость тремя инволюциями

Как обычно, через $t_{ij}(k)$, $k \in \mathbb{Z}$, $i \neq j$, будем обозначать трансвекции, т. е. матрицы $E_n + ke_{ij}$, где E_n — единичная $(n \times n)$-матрица, а e_{ij} — матричные единицы.

Следующая лемма хорошо известна (см., например, [2, с. 107]).

Лемма 1.1. *Группа $SL_n(\mathbb{Z})$ порождается трансвекциями $t_{ij}(1)$, $i \neq j$, $i, j = 1, 2, \ldots, n$. В частности, группа $SL_2(\mathbb{Z})$ порождается двумя матрицами*

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

В действительности лемма 1.1 справедлива для любого евклидова кольца. Из леммы 1.1 легко следует

[1]Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект № 01-09-00-717.

Лемма 1.2. *Группа $GL_n(\mathbb{Z})$ порождается трансвекциями $t_{ij}(1)$, $i \neq j$, $i, j = 1, 2, \dots n$, и любой другой матрицей с определителем -1.*

Предложение 1.3. *Группа $GL_2(\mathbb{Z})$ порождается тремя инволюциями*

$$\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \beta = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix}.$$

$\lhd$ Так как определитель матрицы α равен -1 (как, впрочем, и двух других) и

$$\beta\gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \alpha\beta\gamma\alpha = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$

то по лемме 1.2 инволюции α, β, γ порождают группу $GL_2(\mathbb{Z})$. $\rhd$

Конечно, группа $PGL_2(\mathbb{Z})$ порождается образами инволюций α, β, γ из предложения 1.3 при естественном гомоморфизме $GL_2(\mathbb{Z}) \to PGL_2(\mathbb{Z})$, поэтому справедливо

Предложение 1.4. *Группа $PGL_2(\mathbb{Z})$ порождается тремя инволюциями.*

В группе $SL_2(\mathbb{Z})$ всего лишь одна инволюция, поэтому справедливо

Предложение 1.5. *Группа $SL_2(\mathbb{Z})$ не порождается никаким множеством инволюций.*

В 1890 г. Р. Фрике и Ф. Клейн [1] доказали, что группа $PSL_2(\mathbb{Z})$ является свободным произведением групп порядка 2 и 3. В действительности, они установили равенство

$$PSL_2(\mathbb{Z}) = \langle\bar{\alpha}\rangle * \langle\bar{\beta}\rangle,$$

где $\bar{\alpha}$, $\bar{\beta}$ являются образами в $PSL_2(\mathbb{Z})$ соответственно матриц

$$\alpha = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \quad \beta = \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Следовательно, справедливо

Предложение 1.6. *Группа $PSL_2(\mathbb{Z})$ не порождается никаким множеством инволюций.*

2. Порождаемость тремя инволюциями, две из которых перестановочны

В следующем предложении для элементов группы $PGL_2(\mathbb{Z})$ используется матричная запись, при этом два элемента считаются равными, если они различаются лишь умножением на скалярную матрицу. Так как мультипликативная группа кольца $\mathbb{Z}$ имеет порядок 2, то это легко увидеть.

Предложение 2.1. *Группа $PGL_2(\mathbb{Z})$ порождается тремя инволюциями*

$$\alpha = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \beta = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \gamma = \begin{pmatrix} -1 & -1 \\ 0 & 1 \end{pmatrix},$$

причем первые две из них перестановочны.

$\lhd$ Заметим, что инволюции α, β, γ такие же, как и в предложении 1.3, поэтому они порождают $PGL_2(\mathbb{Z})$. Отличие лишь в том, что в группе $PGL_2(\mathbb{Z})$ инволюции α, β перестановочны, так как квадрат их произведения является скалярной матрицей. $\rhd$

Лемма 2.2. *Любая подгруппа M, порожденная тремя нецентральными инволюциями из группы $GL_2(\mathbb{C})$ над полем комплексных чисел $\mathbb{C}$, две из которых перестановочны, имеет следующую структуру:*

$$M = \langle\gamma, \delta\rangle \cdot \langle\alpha, \beta\rangle, \tag{1}$$

где

$$\alpha^2 = \beta^2 = \gamma^2 = \delta^2 = (\alpha\beta)^2 = \alpha\gamma\alpha\delta = \beta\gamma\beta\delta = 1. \tag{2}$$

Более того, группа M либо конечна, либо $M = \langle\gamma, \delta\rangle \leftthreetimes \langle\alpha, \beta\rangle$.

$\lhd$ Пусть три различные нецентральные инволюции α, β, γ из группы $GL_2(\mathbb{C})$ порождают подгруппу M, причем инволюции α, β перестановочны. С точностью до сопряжения в $GL_2(\mathbb{C})$ можно считать, что

$$\alpha = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \beta = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Так как инволюции α, β перестановочны, то

$$\alpha\beta = \begin{pmatrix} -a & -b \\ c & d \end{pmatrix} = \begin{pmatrix} -a & b \\ -c & d \end{pmatrix} = \beta\alpha.$$

Отсюда $b = c = 0$ и, следовательно, $ad = -1$, а так как инволюции α, β различны, то $a = 1$, $b = -1$. Таким образом,

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

Пусть для некоторых $a, b, c, d \in \mathbb{C}$

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Положим

$$\delta = \alpha\gamma\alpha = \begin{pmatrix} a & -b \\ -c & d \end{pmatrix} = \beta\gamma\beta.$$

Тогда равенства (2) выполняются и любое слово из подгруппы M имеет один из следующих четырех видов:

$$\begin{array}{rcl} \alpha\delta & \dots & \alpha\delta\varepsilon, \\ \alpha\delta & \dots & \alpha\delta\alpha\varepsilon, \\ \delta\alpha\delta & \dots & \alpha\delta\varepsilon, \\ \delta\alpha\delta & \dots & \alpha\delta\alpha\varepsilon, \end{array}$$

где $\varepsilon = 1$, α, β, $\alpha\beta$. Следовательно, выполняется и равенство (1) и, более того, подгруппа

$$\langle\gamma, \delta\rangle = \langle\gamma\delta\rangle \leftthreetimes \langle\gamma\rangle$$

нормальна в M. Покажем, что группа M либо конечна, либо $M = \langle\gamma, \delta\rangle \leftthreetimes \langle\alpha, \beta\rangle$.

Любой элемент из подгруппы $\langle\gamma, \delta\rangle$ имеет вид $(\gamma\delta)^k$ или $(\gamma\delta)^k\gamma$.

Если $(\gamma\delta)^k \in \langle\alpha, \beta\rangle$, то $(\gamma\delta)^{2k} = 1$ и, следовательно, группа M конечна.

Пусть $(\gamma\delta)^k\gamma \in \langle\alpha, \beta\rangle$. Тогда $(\gamma\delta)^k\gamma = \alpha$, β, $\alpha\beta$ или 1.

Если $(\gamma\delta)^k\gamma = \alpha$, то в силу тождества $\delta = \alpha\gamma\alpha$ получаем равенство $(\delta\gamma)^k\delta = \alpha$. Отсюда $(\gamma\delta)^{2k+1} = 1$ и, следовательно, группа M конечна. Случай $(\gamma\delta)^k\gamma = \beta$ подобен.

Определитель матрицы $(\gamma\delta)^k\gamma$ равен -1, поэтому матрица $(\gamma\delta)^k\gamma$ не может совпадать с матрицами $\alpha\beta$ или 1, так как определитель последних двух равен 1. $\rhd$

Предложение 2.3. *Группа $GL_2(\mathbb{Z})$ не порождается тремя инволюциями, две из которых перестановочны.*

$\lhd$ Ясно, что в любой порождающей тройке инволюций группы $GL_2(\mathbb{Z})$ не может быть центральной инволюции, поэтому в силу леммы 2.2 она не может порождаться тремя инволюциями, две из которых перестановочны. $\rhd$

3. Порождающие мультиплеты инволюций

Для группы G через $n(G)$ обозначим минимальное число порождающих инволюций, произведение которых равно 1. Ясно, что если G' — гомоморфный образ группы G, то $n(G') \leqslant n(G)$. Доказательство следующей леммы является легким упражнением.

Лемма 3.1. *Если $n(G) = 4$, то в G найдется нетривиальная циклическая нормальная подгруппа.*

Предложение 3.2. $n(PGL_2(\mathbb{Z})) = 5$.

$\lhd$ В силу предложения 2.1 группа $PGL_2(\mathbb{Z})$ порождается некоторыми тремя инволюциями α, β, γ, первые две из которых перестановочны. Тогда, очевидно, она порождается и пятью инволюциями α, β, γ, γ, $\beta\alpha$, произведение которых равно 1. Таким образом, $n(PGL_2(\mathbb{Z})) \leqslant 5$. Для любого простого числа p существует гомоморфизм $PGL_2(\mathbb{Z}) \to PGL_2(p)$ и при $p \geqslant 5$ в группе $PGL_2(p)$ нет нетривиальных циклических нормальных подгрупп, поэтому по лемме 3.1 $n(PGL_2(\mathbb{Z})) = 5$. $\rhd$

Предложение 3.3. $n(GL_2(\mathbb{Z})) = 6$.

$\lhd$ В силу предложения 1.3 группа $GL_2(\mathbb{Z})$ порождается тремя инволюциями, поэтому $n(GL_2(\mathbb{Z})) \leqslant 6$.

Предположим, что $n(GL_2(\mathbb{Z})) = 5$ и $\alpha_1, \ldots, \alpha_5$ — порождающие инволюции, произведение которых равно 1. В группе $GL_2(\mathbb{Z})$ определитель любой нецентральной инволюции равен -1. Поэтому среди инволюций $\alpha_1, \ldots, \alpha_5$ найдется центральная инволюция (иначе получим равенство $(-1)^5 = 1$). Но тогда $n(PGL_2(\mathbb{Z})) = 4$ и мы получаем противоречие с предложением 3.2. $\rhd$

Литература

1. *Fricke R., Klein F.* Vorlesungen uber die theore der elliptischen modulfunktionen. Vol. 1.—Leipzig: Teubner, 1890.—764 p.; Vol. 2.—Leipzig: Teubner, 1892.—712 p.
2. *Стейнберг Р.* Лекции о группах Шевалле.—М.: Мир, 1975.—262 с.

Статья поступила 10 ноября 2009 г.

Нужин Яков Нифантьевич
Сибирский федеральный университет, *профессор*
Россия, 660074, Красноярск, ул. Киренского 26
E-mail: `nuzhin2008@rambler.ru`

Тимофеенко Иван Алексеевич
Сибирский федеральный университет
Россия, 660074, Красноярск, ул. Киренского 26
E-mail: `ivan.timofeenko@gmail.com`