ТРУДЫ ИНСТИТУТА МАТЕМАТИКИ И МЕХАНИКИ УрО РАН

Том 31 № 4 2025

УДК 512.5

О ПОРОЖДАЕМОСТИ ГРУПП $GL_n(q)$ И $PGL_n(q)$ ТРЕМЯ ИНВОЛЮЦИЯМИ, ДВЕ ИЗ КОТОРЫХ ПЕРЕСТАНОВОЧНЫ[1]

И. А. Марковская, Я. Н. Нужин

Группу, порожденную тремя инволюциями, две их которых перестановочны, будем называть $(2\times 2,2)$-порожденной. Класс таких групп замкнут относительно гомоморфных образов, если по определению единичную группу считаем таковой и не исключаем совпадения двух или всех трех инволюций. В частности, в нашем определении любая диэдральная группа является $(2\times 2,2)$-порожденной. Вопрос о $(2\times 2,2)$-порождаемости конечных простых групп был поставлен В. Д. Мазуровым в Коуровской тетради в 1980 году. Ответ на этот вопрос известен, и он положителен, за исключением трех знакопеременных групп, некоторых групп лиева типа ранга не больше трех и четырех спорадических групп. В данной статье рассматривается $(2\times 2,2)$-порождаемость общей линейной группы $GL_n(q)$ над конечным полем порядка q и ее проективного образа $PGL_n(q)$. Доказано, что $GL_n(q)$ (соответственно $PGL_n(q)$) тогда и только тогда является $(2\times 2,2)$-порожденной, когда либо а) $q=2$ и $n=2$ или $n\geq 5$, либо б) $q=3$ и $n\geq 5$ (соответственно когда либо а) $n=2$ и q любое, либо б) $n\geq 4$ и $(n,q-1)=2$, либо в) $n\geq 5$ и $(n,q-1)=1$).

Ключевые слова: общая и проективная линейные группы, конечное поле, порождающие тройки инволюций.

I. A. Markovskaya, Ya. N. Nuzhin. On generation of the groups $GL_n(q)$ and $PGL_n(q)$ by three involutions, two of which commute.

A group generated by three involutions, two of which commute, will be called $(2\times 2,2)$-generated. The class of such groups is closed with respect to homomorphic images, if, by definition, we consider the identity group as such and do not exclude the coincidence of two or all three involutions. For finite simple groups, the question of generation by three involutions, two of which commute, was formulated by V. D. Mazurov in the Kourovka notebook in 1980. The answer to this question is known, and it is positive, excluding three alternating groups, some groups of Lie type of rank no more than three, and four sporadic groups. This article considers the $(2\times 2,2)$-generation of the general linear group over a finite field and its projective image $PGL_n(q)$.
It is proven that $GL_n(q)$ (respectively $PGL_n(q)$) is $(2\times 2,2)$-generated if and only if a) $q=2$ and $n=2$ or $n\geq 5$, or b) $q=3$ and $n\geq 5$ (respectively, when either a) $n=2$ and any q, or b) $n\geq 4$ and $(n,q-1)=2$, or c) $n\geq 5$ and $(n,q-1)=1$).

Keywords: general and projective linear groups, finite field, generating triples of involutions.

MSC: 20G40

DOI: 10.21538/0134-4889-2025-31-4-fon-03

Введение

Вопрос о порождении конечных простых групп тремя инволюциями, две их которых перестановочны, был поставлен В. Д. Мазуровым в Коуровской тетради [1] в 1980 году. Ответ на этот вопрос известен, и он положителен, за исключением знакопеременных групп A_6, A_7, A_8, некоторых групп лиева типа ранга не больше трех и спорадических группы M_{11}, M_{22}, M_{23}, McL. Полный список исключений можно найти, например, в [2]. Далее для краткости группу, порожденную тремя инволюциями, две из которых перестановочны, будем называть $(2\times 2,2)$-*порожденной*. Класс данных групп замкнут относительно гомоморфных образов, если по определению единичную группу считаем таковой и не исключаем совпадения двух или всех трех инволюций. Согласно нашему определению группа порядка два и любая диэдральная группа являются $(2\times 2,2)$-порожденными.

Основными результатами статьи являются две следующие теоремы.

[1]Работа выполнена при поддержке Российского научного фонда, проект 25-21-20059, https://rscf.ru/project/25-21-20059/ .

Теорема 1. *Группа $GL_n(q)$ тогда и только тогда является $(2\times 2, 2)$-порожденной, когда либо а) $q = 2$ и $n = 2$ или $n \geq 5$, либо б) $q = 3$ и $n \geq 5$.*

Теорема 2. *Группа $PGL_n(q)$ тогда и только тогда является $(2 \times 2, 2)$-порожденной, когда либо* а) *$n = 2$ и q любое, либо* б) *$n \geq 4$ и $(n, q-1) = 2$, либо* в) *$n \geq 5$ и $(n, q-1) = 1$.*

Условие $(n, q-1) = 1$ влечет изоморфизмы $PGL_n(q) \simeq SL_n(q) \simeq PSL_n(q)$ (см. далее лемму 4). Ответ о $(2 \times 2, 2)$-порожденности группы $PSL_n(q)$ был получен ранее Я. Н. Нужиным (см., например [2]). $(2 \times 2, 2)$-порожденность группы $PGL_2(q)$ установили Д. Сёрве и М. Черкасов [3].

Для большей наглядности утверждения теорем 1 и 2 представлены табл. 1 и 2 соответственно.

Таблица 1

$(2 \times 2, 2)$ – порожденность группы $GL_n(q)$

$GL_n(q)$	ответ
$n = 2,\ q = 2$	да
$n = 2,\ q \neq 2$	нет
$n = 3,\ q$ — любое	нет
$n = 4,\ q$ — любое	нет
$n \geq 5,\ q = 2, 3$	да
$n \geq 5,\ q \neq 2, 3$	нет

Таблица 2

$(2 \times 2, 2)$ – порожденность группы $PGL_n(q)$

$PGL_n(q)$	ответ
$n = 2,\ q$ — любое	да
$n = 3,\ q$ — любое	нет
$n \geq 4,\ (n, q-1) > 2$	нет
$n \geq 4,\ (n, q-1) = 2$	да
$n = 4,\ (n, q-1) = 1$	нет
$n \geq 5,\ (n, q-1) = 1$	да

$(2 \times 2, 2)$-порожденные группы возникают в качестве групп автоморфизмов регулярных 3-политопов — определенных конечных частично упорядоченных множеств. М. Кондер и Д. Оливерос установили, что если конечная группа G порождается тремя различными инволюциями, две из которых перестановочны, и если G не имеет циклических нормальных подгрупп, то G является группой автоморфизмов регулярного 3-политопа [4, следствие 4.2]. Поэтому таковыми будут $(2 \times 2, 2)$-порожденные группы $PGL_n(q)$ из теоремы 2, за исключением группы $PGL_2(2)$, изоморфной группе подстановок S_3, поскольку все они не имеют циклических нормальных подгрупп. Список почти простых групп, для которых уже доказано, что они являются группами автоморфизмов регулярных n-политопов для определенных n, можно найти в детальном обзоре Д. Лиманса [5]; там же сформулирован ряд проблем и гипотез по этой тематике.

1. Обозначения и предварительные результаты

Прежде всего, зафиксируем в виде леммы утверждение, которое непосредственно следует из определения $(2 \times 2, 2)$-порожденной группы, указанного во введении.

Лемма 1. *Класс $(2 \times 2, 2)$-порожденных групп замкнут относительно гомоморфных образов.*

Обозначим через $\langle M\rangle$ группу, порожденную множеством M из какой-либо группы. Заметим, что если образы порождают фактор-группу, то их прообразы не обязаны порождать всю исходную группу. Однако справедливо следующее элементарное, но полезное утверждение.

Лемма 2. *Пусть H — нормальная подгруппа группы G. Для произвольного набора элементов $g_1,\dots,g_m\in G$ следующие два равенства эквивалентны*:
1) $G/H=\langle g_1H,\dots,g_mH\rangle$;
2) $G=\langle g_1,\dots,g_m,H\rangle$.

Далее K — ассоциативно-коммутативное кольцо с единицей 1, K^* — его мультипликативная группа, $SL_n(K)$ — подгруппа матриц с определителем 1 общей линейной группы $GL_n(K)$ над кольцом K, $PGL_n(K)$ — проективный образ группы $GL_n(K)$. Линейную группу типа X_n над конечным полем $\mathbb{F}_q$ из q элементов будем обозначать через $X_n(q)$. Элементарные трансвекции

$$t_{ij}(k)=E_n+ke_{ij},\quad i,j=1,2,\dots,n,\quad i\neq j,\quad k\in\mathbb{R},$$

будем называть просто трансвекциями, где E_n — единичная матрица степени n, а e_{ij} — $(n\times n)$-матрица с 1 на позиции (i,j) и нулями в остальных местах. Как обычно, $diag(k_1,\dots,k_n)$ — диагональная матрица. Кольцо целых чисел будем обозначать через $\mathbb{Z}$.

Ненулевой элемент u поля $\mathbb{F}_q$ называется *собственным* (соответственно *примитивным*) элементом, если он не содержится ни в каком его собственном подполе (соответственно, если он порождает мультипликативную группу $\mathbb{F}_q^*$).

Лемма 3.

$$GL_n(K)=SL_n(K)\leftthreetimes\langle diag(k,1,\dots,1)\mid k\in K^*\rangle. \tag{1.1}$$

В частности, если u — примитивный элемент поля $\mathbb{F}_q$, то

$$GL_n(q)=SL_n(q)\leftthreetimes\langle diag(u,1,\dots,1)\rangle. \tag{1.2}$$

Доказательство. Если $k\in K^*$, $A\in GL_n(K)$ и $\det(A)=k$, то определитель матрицы $B=A\,diag(k^{-1},1,\dots,1)$ равен 1 и, очевидно, $A=B\,diag(k,1,\dots,1)$. □

Заметим, что равенство (1.1) справедливо независимо от того, порождается ли группа $SL_n(K)$ своими трансвекциями.

Через $D_n(K)$ (соответственно через $C_n(K)$) обозначим подгруппу всех диагональных (соответственно скалярных) матриц в $GL_n(K)$. По определению

$$C_n(K)=\{diag(k,k,\dots,k)\mid k\in K^*\}.$$

Наибольший общий делитель двух натуральных чисел n и m обозначим через (n,m).

Лемма 4. *Пусть группа K^* имеет конечный порядок и $(n,|K^*|)=1$. Тогда $GL_n(K)=SL_n(K)\times C_n(K)$ и, следовательно, $PGL_n(K)\simeq SL_n(K)=PSL_n(K)$.*

Доказательство. В силу $(n,|K^*|)=1$ пересечение $SL_n(K)\cap C_n(K)$ единично и любой элемент из K^* представляется в виде k^n для подходящего $k\in K^*$. Остается заметить, что

$$diag(k^{n-1},k^{-1},\dots,k^{-1})\,diag(k,k,\dots,k)=diag(k^n,1,\dots,1),$$

причем, первая диагональная матрица в левой части равенства лежит в $SL_n(K)$, и применить лемму 3. □

Пусть I — идеал кольца K. Тогда естественный кольцевой гомоморфизм $\rho_I\colon K\to K/I$ определяет сюръективный гомоморфизм $\psi_I\colon M_n(K)\to M_n(K/I)$ кольца $n\times n$-матриц $M_n(K)$ с обычными операциями сложения и умножения, где для любой матрицы $(a_{ij})\in M_n(K)$ по определению $\psi_I\colon(a_{ij})\to(\rho_I(a_{ij}))$. С другой стороны, гомоморфизм ρ_I индуцирует гомоморфизм групп $\varphi_I\colon GL_n(K)\to GL_n(K/I)$, $\varphi_I\colon SL_n(K)\to SL_n(K/I)$, где также по определению $\varphi_I\colon(a_{ij})\to(\rho_I(a_{ij}))$. Д. А. Супруненко назвал φ_I гомоморфизмом Минковского [6, с. 95]. Однако, как показывает следующая лемма, гомоморфизм φ_I уже не обязан быть сюръективным, как гомоморфизм ψ_I.

Лемма 5. *Пусть I — идеал кольца $\mathbb{Z}$, порожденный простым числом p, φ_I — гомоморфизм Минковского, определенный выше. Тогда группы $\varphi_I(GL_n(\mathbb{Z}))$ и $GL_n(p)$ изоморфны тогда и только тогда, когда p равно 2 или 3. В частности, при $p \geq 5$ гомоморфизм φ_I не является сюръективным.*

Доказательство. Образ $\rho_I(\mathbb{Z})$ изоморфен полю $\mathbb{F}_p$. Поэтому можно считать, что $\varphi_I(GL_n(\mathbb{Z}))$ лежит в $GL_n(p)$. Группы $GL_n(\mathbb{Z})$ и $GL_n(p)$ порождаются всеми своими трансвекциями и диагональными матрицами. Гомоморфизм φ_I переводит трансвекции в трансвекции, а диагональные матрицы — в диагональные. Поскольку группа $\mathbb{Z}^*$ имеет порядок 2, то $GL_n(\mathbb{Z}) = SL_n(\mathbb{Z}) \leftthreetimes \langle diag(-1, 1, \ldots, 1)\rangle$ по лемме 3. Поэтому $\varphi_I(GL_n(\mathbb{Z}))$ является собственной подгруппой в $GL_n(p)$ тогда и только тогда, когда $p \geq 5$. □

Утверждение следующей леммы — это частный случай теоремы 1 из статьи второго автора [7].

Лемма 6. *Пусть φ — естественное представление размерности $n \geq 2$ группы $GL_n(F)$ над полем F характеристики, отличной от 2. Тогда тензорный симметрический квадрат φ^2 является неприводимым представлением, причем $Ker(\varphi^2) = \{1, -1\}$.*

Известный результат Л. Л. Скотта [8, теорема 1] указывает способ получения отрицательного ответа на вопрос такого типа: существуют ли для данной группы G порождающие элементы $g_1, g_2, \ldots, g_k$ с определенными свойствами, для которых $g_1 g_2 \ldots g_k = 1$? Чаще применяют его следующее следствие.

Лемма 7. *Пусть неприводимая подгруппа G группы $GL_n(F)$, $n \geq 2$, над полем F порождается элементами $g_1, g_2, \ldots, g_k$ с условием $g_1 g_2 \ldots g_k = 1$. Через $d(g_i)$ обозначим коразмерность подпространства неподвижных элементов $V_n(g_i) = \{v \in V_n \mid g_i v = v\}$, где V_n — векторное пространство размерности n над полем F. Тогда*

$$d(g_1) + \cdots + d(g_k) \geq 2n. \tag{1.3}$$

Лемма 8. *Пусть h — произвольный диагональный элемент группы $GL_n(F)$ над полем F, $u \in F^*$, n — матрица-перестановка, соответствующая циклу $(12 \ldots n)$. Тогда для любого $i = 1, 2, \ldots, n-1$ группа, порожденная мономиальным элементом hn и трансвекцией $t_{ii+1}(u)$ или $t_{i+1i}(u)$, имеет неединичные пересечения со всеми подгруппами $t_{km}(F)$.*

Доказательство. Подгруппа $\langle hn\rangle$ действует сопряжениями транзитивно на множестве подгрупп

$$\mathfrak{T} = \{t_{12}(F), \ldots, t_{n-1n}(F), t_{n1}(F)\}.$$

Поэтому подгруппа $\langle hn, t_{ii+1}(u)\rangle$ имеет неединичное пересечение с каждой подгруппой из $\mathfrak{T}$. При $n = 2$ мы уже имеем неединичные пересечения со всеми подгруппами $t_{km}(F)$. В случае $n \geq 3$, коммутируя между собой эти пересечения, получим неединичные пересечения со всеми подгруппами $t_{km}(F)$. Для группы $\langle hn, t_{i+1i}(u)\rangle$ рассуждения аналогичные. □

Частным случаем теоремы 1 из [9], когда группа Шевалле изоморфна $SL_n(q)$, является

Лемма 9. *Пусть подгруппа M группы $SL_n(q)$, $n \geq 3$, имеет неединичные пересечения со всеми подгруппами $t_{km}(\mathbb{F}_q)$ и порождается этими пересечениями. Тогда с точностью до сопряжения диагональным элементом из $GL_n(q)$ подгруппа M совпадает с $SL_n(q')$ для некоторого подполя $\mathbb{F}_{q'} \leq \mathbb{F}_q$. Более того, если для некоторых i, j трансвекции $t_{ij}(u)$ и $t_{ji}(u)$ лежат в M, где u — примитивный элемент поля $\mathbb{F}_q$, то $M = SL_n(q)$.*

Из основной теоремы 1 статьи В. М. Левчука [10], которая обобщает и усиливает известную теорему Л. Диксона о группе, порожденной двумя противоположными трансвекциями над конечным полем нечетной характеристики, следует

Лемма 10. а) *Пусть $q \neq 9$, $V \subseteq \mathbb{F}_q^*$, $|V| \geq 2$ и некоторый собственный элемент и поля $\mathbb{F}_q$ лежит в V. Тогда $\langle t_{12}(V),\ t_{21}(1)\rangle = SL_2(q)$.*

б) *Если $u, v \in \mathbb{F}_q^*$, то для некоторого $w \in \mathbb{F}_q^*$ матрицы*

$$A = \begin{pmatrix} 0 & -w^{-1} \\ w & 0 \end{pmatrix} \quad и \quad A^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

лежат в группе, порожденной трансвекциями $t_{12}(u)$ и $t_{21}(v)$.

в) *Если q нечетно, u — примитивный элемент поля $\mathbb{F}_q$, то $\langle t_{12}(u),\ t_{21}(1)\rangle = SL_2(q)$.*

Лемма 11. *При $(n, q-1) > 2$ группа $PGL_n(q)$ не порождается никаким множеством инволюций. В частности, если $q-1$ делит n и $q > 3$, то группа $PGL_n(q)$ не порождается никаким множеством инволюций.*

Доказательство. Прежде всего заметим, что предположение $(n, q-1) > 2$ влечет строгое включение

$$\langle -1, t^n \mid t \in \mathbb{F}_q^* \rangle < \mathbb{F}_q^*. \tag{1.4}$$

Действительно, если $(n, q-1)$ делится на нечетное простое число p, то индекс подгруппы $\langle -1, t^n \mid t \in \mathbb{F}_q^* \mid \rangle$ в группе $\mathbb{F}_q^*$ не меньше p. Если $(n, q-1) = 2^s$, то $s \geq 2$ и данный индекс не меньше 2. В любом случае неравенство (1.4) справедливо.

Пусть образ матрицы $A \in GL_n(q)$ является инволюцией в $PGL_n(q)$. Тогда ее квадрат — скалярная матрица. Поэтому либо все собственные значения матрицы A равны ± 1, либо все ее собственные значения отличны от ± 1 и A^2 — не единичная скалярная матрица.

Если собственные значения равны ± 1 для всех прообразов из некоторого множества инволюций M группы $PGL_n(q)$, то в силу (1.4) прообразы M вместе со всеми скалярными матрицами породят собственную подгруппу группы $GL_n(q)$, поскольку в последней имеются матрицы с определителем порядка $q-1$. Следовательно, в этом случае по лемме 2 множество инволюций M не может порождать группу $PGL_n(q)$.

Пусть A — прообраз некоторой инволюции из $PGL_n(q)$ и A^2 — не единичная скалярная матрица. Тогда квадрат любого собственного значения матрицы A равен фиксированному элементу $t \in \mathbb{F}_q^*$. Поэтому

$$\det(A) = \begin{cases} \pm t^k & \text{если } n = 2k, \\ \pm t^k \sqrt{t} & \text{если } n = 2k+1. \end{cases}$$

Пусть $n = 2k$. Если $(k, q-1) > 2$, то также, как и при доказательстве неравенства (1.4), получаем, что $\langle -1, t^k \mid t \in \mathbb{F}_q^* \rangle$ — собственная подгруппа в $\mathbb{F}_q^*$. Пусть $(k, q-1) \leq 2$. Тогда $(k, q-1) = 2$ и $(n, q-1) = 4$, поскольку $(n, q-1) > 2$. Так как 4 делит $q-1$, то -1 лежит в подгруппе квадратов. Следовательно, в этом случае $\langle -1, t^k \mid t \in \mathbb{F}_q^* \rangle$ также является собственной подгруппой в $\mathbb{F}_q^*$. Таким образом, определители прообразов всех инволюций из $PGL_n(q)$ лежат в собственной подгруппе $\langle -1, t^k \mid t \in \mathbb{F}_q^* \rangle$ группы $\mathbb{F}_q^*$. Поэтому никакое множество инволюций не порождает группу $PGL_n(q)$ по лемме 2, поскольку все их прообразы порождают собственную подгруппу в $GL_n(q)$.

При $n = 2k+1$, очевидно, $\sqrt{t} \in \mathbb{F}_q^*$ и $\det(A) = \pm\sqrt{t}^n$. Поэтому $\langle -1, \sqrt{t}^n \mid \sqrt{t} \in \mathbb{F}_q^* \rangle$ — собственная подгруппа группы $\mathbb{F}_q^*$ согласно (1.4). Сейчас, также как и выше, получаем, что никакое множество инволюций не порождает группу $PGL_n(q)$. □

Далее при вычислениях мы используем следующие сокращения: $a^b = bab^{-1}$, $[a, b] = aba^{-1}b^{-1}$.

2. Доказательство теоремы 1

С л у ч а й $q \geq 4$. В группе $GL_n(q)$ определитель любой инволюции равен ± 1, а при $q \geq 4$ в ней есть матрицы с определителем, отличным от ± 1. Поэтому при $q \geq 4$ группа $GL_n(q)$ не является $(2 \times 2, 2)$-порожденной.

С л у ч а й $q = 2$. Очевидно, $GL_n(2) = PGL_n(2) = SL_n(2) = PSL_n(2)$. При $n \geq 3$ группа $GL_n(2)$ простая и в силу [2] является $(2 \times 2, 2)$-порожденной тогда и только тогда, когда $n \geq 5$, а $GL_2(2)$ — диэдральная группа и ввиду нашего определения она $(2 \times 2, 2)$-порождена.

С л у ч а й $n \geq 5$, $q = 3$. В [11] доказано, что при $n \geq 5$ группа $GL_n(\mathbb{Z})$ $(2 \times 2, 2)$-порожденная. Поэтому согласно леммам 1 и 5 такой является и группа $GL_n(3)$ при $n \geq 5$.

С л у ч а й $n = 4$, $q = 3$. Предположим противное. Пусть группа $GL_4(3)$ порождается тремя инволюциями α, β, γ, первые две из которых перестановочны. Тогда, исходя из лемм 1 и 6 группа, изоморфная $PGL_4(3)$, порождается образами $\varphi^2(\alpha), \varphi^2(\beta), \varphi^2(\gamma)$, где φ^2 — симметрический тензорный квадрат естественного представления φ группы $GL_4(3)$, причем 10-мерное представление φ^2 неприводимо.

Собственные значения любой инволюции из группы GL_n над полем нечетной характеристики равны ± 1. Поэтому в силу теории Жордана в группе $GL_4(3)$ — четыре класса сопряженных инволюций с представителями

$$\alpha_1 = diag(-1, 1, 1, 1), \quad \alpha_2 = diag(-1, -1, 1, 1),$$
$$\alpha_3 = diag(-1, -1, -1, 1), \quad \alpha_4 = diag(-1, -1, -1, -1).$$

Так как инволюции α и β перестановочны, то

$$\varphi^2(\alpha)\,\varphi^2(\beta)\,(\varphi^2(\alpha)\varphi^2(\beta))\,\varphi^2(\gamma)\,\varphi^2(\gamma) = 1. \tag{2.1}$$

Пусть числа $d(\varphi^2(\alpha_i))$ такие, как в лемме 7. Тогда $d(\varphi^2(\alpha_1)) = 3$, $d(\varphi^2(\alpha_2)) = 4$, $d(\varphi^2(\alpha_3)) = 3$, $d(\varphi^2(\alpha_4)) = 0$. Поэтому неравенство (1.3) из леммы 7 может выполняться только тогда, когда все 5 инволюций из равенства (2.1) лежат в классе сопряженности с представителем $\varphi^2(\alpha_2)$. Более того, неравенство (1.3) в этом случае превращается в равенство $4 \cdot 5 = 10 \cdot 2$. Но определитель матрицы α_2 равен 1. Поэтому, если все инволюции в равенстве (2.1) лежат в классе сопряженности с представителем $\varphi^2(\alpha_2)$, то они порождают только какую-то подгруппу в группе $PSL_4(3)$, но не всю группу $PGL_4(3)$. Противоречие.

С л у ч а й $n = 3$, $q = 3$. По лемме 4 имеем $GL_3(3) = SL_3(3) \times \langle -E_3 \rangle$. Поэтому в силу леммы 1, если группа $GL_3(3)$ $(2 \times 2, 2)$-порожденая, то и группа $SL_3(3)$ $(= PSL_3(3))$ является $(2 \times 2, 2)$-порожденной, но это не так (см. [2]). Следовательно, группа $GL_3(3)$ не является $(2 \times 2, 2)$-порожденной.

С л у ч а й $n = 2$, $q = 3$. В группе $GL_2(3)$ два класса сопряженных инволюций с представителями

$$\delta = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \iota = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Централизатор $Z(\delta)$ инволюции δ в группе $GL_2(3)$ имеет порядок 4 и помимо единичной матрицы содержит δ, ι и $\delta\iota$. Пусть C_δ — класс сопряженных элементов с представителем δ. Тогда

$$|C_\delta| = |GL_2(3)|/|Z(\delta)| = 48/4 = 12$$

и C_δ состоит из всех мономиальных и треугольных матриц с определителем -1. Поскольку $C_\iota = \{\iota\}$, то $C_\delta \cup \{\iota\}$ совпадает с множеством всех инволюций из $GL_2(3)$. Пусть подгруппа M из $GL_2(3)$ порождается тремя инволюциями α, β, γ, причем первые две из них перестановочны. Не теряя общности, можно считать, что α и β лежат в $Z(\delta)$ и, в частности, они являются диагональными матрицами. Третья инволюция γ, очевидно, лежит во множестве $C_\alpha \cup \{\iota\}$. Нетрудно заметить, что тогда подгруппа M состоит либо из мономиальных, либо из треугольных матриц. Следовательно, группа $GL_2(3)$ не является $(2 \times 2, 2)$-порожденной.

Теорема 1 доказана.

3. Доказательство теоремы 2

Д. Сёрве и М. Черкасов [3] установили, что при $q \neq 2$ группа $PGL_2(q)$ порождается тремя различными инволюциями, две из которых перестановочны. Группа $PGL_2(2)$ порождается двумя инволюциями, и по нашему определению она $(2 \times 2, 2)$-порождена.

Пусть $n \geq 3$. В соответствии с леммой 11 при $(n, q-1) > 2$ группа $PGL_n(q)$ не порождается никаким множеством инволюций. При $(n, q-1) = 1$ группы $PGL_n(q)$ и $PSL_n(q)$ изоморфны в силу леммы 4. Ответ о $(2 \times 2, 2)$-порожденности группы $PSL_n(q)$ получен ранее вторым автором статьи в трех работах (Алгебра и логика, Т. 29, № 2 (1990), 192–206; Т. 36, № 1 (1997), 7–96; Т. 36, № 4 (1997), 422–440). Доказано, что среди групп $PSL_n(q)$, $n \geq 2$, только следующие не является $(2 \times 2, 2)$-порожденными:

а) $PSL_2(7) \simeq PSL_3(2)$, $PSL_2(9) \simeq A_6$;

б) $PSL_3(q)$ при любом q;

в) $PSL_4(2^m)$.

Поэтому при заполнении строк табл. 2 происходит следующий собирательный процесс.

Для $n = 3$, когда $3 \mid q-1$, мы применяем лемму 1, а когда $(3, q-1) = 1$ используем п. б). Так заполняется третья строка сверху. Четвертая строка сверху заполняется по лемме 11. Утверждение во второй строке снизу следует из п. в). Наконец, утверждение первой строки снизу следует, из того, что при $n \geq 5$ и $(n, q-1) = 1$ группа $PSL_n(q)$ является $(2 \times 2, 2)$-порожденной.

Таким образом, остается рассмотреть только случай $n \geq 4$ при $(n, q-1) = 2$, и в этом случае, как утверждает теорема 2, группа $PGL_n(q)$ является $(2 \times 2, 2)$-порожденной.

Итак, пусть $n \geq 4$ и $(n, q-1) = 2$. Тогда $n = 2k$ и q нечетно. Положим

$$\mu = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}, \quad \tau = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & 1 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}.$$

Индукцией по размерности n матрицы τ несложно установить равенство

$$\det\tau = \begin{cases} 1, & \text{если } n \equiv 0(\mathrm{mod}4), \\ -1, & \text{если } n \equiv 2(\mathrm{mod}4). \end{cases} \tag{3.1}$$

Пусть $k \geq 3$, u — примитивный элемент поля $\mathbb{F}_q$, $\epsilon = \pm 1$ и

$$\epsilon = (-1)^k. \tag{3.2}$$

Отметим, что параметр ϵ нам потребуется для того, чтобы определитель матрицы β, указанной ниже, был равен u^{-k}. Положим $d(\epsilon u) = diag(\epsilon u^{-1}, \ldots, \epsilon u^{-1}, 1, \ldots, 1)$, где у диагональной матрицы $d(\epsilon u)$ на первых k позициях стоит ϵu^{-1}, а на остальных стоит 1. Покажем, что матрицы α, β, γ, первые две из которых перестановочны, порождают группу $GL_n(q)$, где

$$\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 1 & -1 & 0 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & \cdots & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 0 & \cdots & 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\beta = d(\epsilon u)\tau = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \epsilon u^{-1} \\ 0 & 0 & \cdots & 0 & \epsilon u^{-1} & 0 \\ 0 & 0 & \cdots & \epsilon u^{-1} & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 1 & \cdots & 0 & 0 & 0 \\ 1 & 0 & \cdots & 0 & 0 & 0 \end{pmatrix}, \quad \gamma = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 & 0 \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 1 & 0 & \cdots & 0 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 0 & 1 \end{pmatrix}.$$

Тем самым мы покажем, что группа $PGL_n(q)$ является $(2 \times 2, 2)$-порожденной, поскольку образы матриц α, β, γ в $PGL_n(q)$ — инволюции. Положим

$$M = \langle \alpha, \beta, \gamma \rangle, \quad \eta := \beta\gamma = diag(\epsilon u^{-1}, \dots, \epsilon u^{-1}, 1, \dots, 1)\mu = \begin{pmatrix} 0 & 0 & \cdots & 0 & 0 & \epsilon u^{-1} \\ \epsilon u^{-1} & 0 & \cdots & 0 & 0 & 0 \\ 0 & \epsilon u^{-1} & \cdots & 0 & 0 & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & 0 & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \end{pmatrix}.$$

Пусть $k > 3$. Тогда

$$\alpha^\eta = t_{32}(\pm 1)t_{n1}(\pm u)\, diag(1, 1, -1, -1, 1, \dots, 1, -1, -1),$$

$$\alpha^{\eta^2} = t_{43}(\pm 1)t_{12}(\pm u)\, diag(-1, 1, 1, -1, -1, 1, \dots, 1, -1),$$

$$[\alpha, \alpha^\eta] = t_{31}(\pm 1)t_{n-1,1}(\pm u), \quad ([\alpha, \alpha^\eta]\alpha^{\eta^2})^2 = t_{41}(\pm 1)t_{32}(\pm u)t_{42}(\pm u)t_{n-1,2}(\pm u^2).$$

Положим $\theta := (([\alpha, \alpha^\eta]\alpha^{\eta^2})^2)^\eta$. Тогда

при $n = 8$ $\theta = t_{43}(\pm u)t_{52}(\pm u)t_{53}(\pm u^2)t_{n3}(\pm u^3)$,
при $n \geq 10$ $\theta = t_{43}(\pm u)t_{52}(\pm 1)t_{53}(\pm u)t_{n3}(\pm u^3)$,
при $n = 8$ $[\theta, [\alpha, \alpha^\eta]] = t_{41}(\pm u)t_{51}(\pm u^2)t_{n1}(\pm u^3)$,
при $n \geq 10$ $[\theta, [\alpha, \alpha^\eta]] = t_{41}(\pm u)t_{51}(\pm u)t_{n1}(\pm u^3)$.

Дальнейшие вычисления справедливы как для $n = 8$, так и для $n \geq 10$. Имеем

$$[\alpha, [\theta, [\alpha, \alpha^\eta]]] = t_{n-1,1}(\pm u^3), \quad [\alpha, [\theta, [\alpha, \alpha^\eta]]]^\beta = t_{2n}(\pm u^2),$$

$$[[\theta, [\alpha, \alpha^\eta]], [\alpha, [\theta, [\alpha, \alpha^\eta]]]^\beta] = t_{21}(\pm u^5).$$

По лемме 8 группа, порожденная элементами η и $t_{21}(u^5)$, имеет нетривиальное пересечение со всеми подгруппами $t_{ij}(\mathbb{F}_q)$. Поэтому в силу леммы 9 существует диагональная матрица $d \in GL_n(q)$ такая, что подгруппа M^d содержит $SL_n(q')$ для некоторого подполя $\mathbb{F}_{q'} \leq \mathbb{F}_q$. Трансвекция $t_{n-1,1}(u^3)$ и произведение двух трансвекций $t_{31}(\pm 1)t_{n-1,1}(u)$ лежат в M, поэтому $vu, vu^3 \in \mathbb{F}_{q'}$ для подходящего $v \in \mathbb{F}_q$. Отсюда $u^2 \in \mathbb{F}_{q'}$. Поскольку u — примитивный элемент поля $\mathbb{F}_q$, то u^2 — его собственный элемент. Следовательно, $\mathbb{F}_{q'} = \mathbb{F}_q$. Таким образом, M содержит $SL_n(q)$.

Далее, $\det\beta = -(\epsilon u)^{-k}$ с учетом (3.1), а в силу (3.2) имеем $\det\beta = u^{-k}$. Ввиду того что u — примитивный элемент поля $\mathbb{F}_q$, при нечетном k мультипликативный порядок элемента u^{-k} будет равен $q - 1$, ибо в этом случае $(k, q - 1) = 1$. Поэтому подгруппа, порожденная матрицей β, вместе с подгруппой $SL_n(q)$ совпадает со всей группой $GL_n(q)$ в силу равенства (1.2) из леммы 3. Следовательно, $M = GL_n(q)$ при нечетном k. Если k четно, то $(q - 1)/2$ нечетно в соответствие с предположением $(n, q - 1) = 2$. В данном случае мультипликативный порядок элемента u^{-k} равен $(q - 1)/2$, а определитель матрицы γ равен -1 в силу (3.1). Значит, мультипликативный порядок определителя произведения $\beta\gamma$ равен $q - 1$. Поэтому равенство $M = GL_n(q)$ справедливо и в этом случае согласно (1.2) из леммы 3.

Пусть $k = 3$. В этом случае $n = 6$, $\epsilon = -1$, матрица α незначительно отличается от принятых выше обозначений:

$$\alpha = \begin{pmatrix} -1 & 0 & 0 & 0 & 0 & 0 \\ -1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & 0 & 0 & -1 \end{pmatrix} = t_{21}(1)t_{56}(1)diag(-1,1,1,1,1,-1),$$

$$\beta = diag(-u^{-1},-u^{-1},-u^{-1},1,1,1)\tau = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -u^{-1} \\ 0 & 0 & 0 & 0 & -u^{-1} & 0 \\ 0 & 0 & 0 & -u^{-1} & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix},$$

$$\gamma = \tau\mu = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

$$\eta := \beta\gamma = diag(-u^{-1},-u^{-1},-u^{-1},1,1,1)\mu = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & -u^{-1} \\ -u^{-1} & 0 & 0 & 0 & 0 & 0 \\ 0 & -u^{-1} & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}.$$

Вычисления показывают, что

$$\alpha^{\eta} = t_{32}(1)t_{61}(-u)\,diag(-1,-1,1,1,1,1), \quad \alpha^{\eta^2} = t_{43}(-u)t_{12}(-u)\,diag(1,-1,-1,1,1,1),$$

$$\alpha^{\eta^3} = t_{54}(-u)t_{23}(-u)\,diag(1,1,-1,-1,1,1), \quad \alpha^{\eta^4} = t_{65}(-u)t_{34}(1)\,diag(1,1,1,-1,-1,1),$$

$$[\alpha,\alpha^{\eta}] = t_{31}(-1)t_{51}(-u), \quad [\alpha^{\eta^4},[\alpha,\alpha^{\eta}]] = t_{51}(2u)t_{61}(-u^2), \quad [\alpha,[\alpha^{\eta^4},[\alpha,\alpha^{\eta}]]] = t_{51}(-u^2-4u).$$

При $q \neq 3$ в поле $\mathbb{F}_q$ существует такой примитивный элемент u, что $u^2+4u \neq 0$.

Пусть $q \neq 3$ и u — примитивный элемент с условием $u^2+4u \neq 0$. Тогда

$$t_{51}(u^2+4u) \in M,$$

$$(\alpha^{\eta^4}t_{51}(u^2+4u))^2 = t_{61}(u(u^2+4u)) \in M, \quad (t_{61}(u(u^2+4u)))^{\eta} = t_{12}(u(u^2+4u)) \in M.$$

Исходя из последнего включения и леммы 8, для $hn = \eta$ получаем, что подгруппа M нетривиально пересекается со всеми корневыми подгруппами. Применяя п. б) леммы 10, имеем, что диагональная матрица $diag(1,1,1,1,-1,-1)$ лежит в M. Отсюда

$$[diag(1,1,1,1,-1,-1),[\alpha,\alpha^{\eta}]] = t_{51}(2u) \in M, \quad (t_{51}(2u))^{\gamma} = t_{15}(2u) \in M.$$

Сейчас в силу леммы 9 получаем включение $SL_n(q) < M$. Так как $\det\beta = u^{-3}$ и $(3, q-1) = 1$, то мультипликативный порядок определителя матрицы β равен $q-1$. Поэтому $M = GL_n(q)$ в силу равенства (1.2) из леммы 3.

Случай $q = 3$ следует из $(2 \times 2, 2)$-порожденности группы $GL_6(\mathbb{Z})$ [11, теорема 1] и лемм 1 и 5.

Пусть $n = 4$. В этом случае числа q и $(q-1)/2$ нечетны. Доказательство разбивается на два подслучая в зависимости от того, равна трем характеристика $char\mathbb{F}_q$ поля $\mathbb{F}_q$ или нет. Более того, в каждом из двух подслучаев будут свои порождающие тройки инволюций.

Пусть $char\mathbb{F}_q = 3$. Положим

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

Матрицы α, β, γ являются инволюциями в $PGL_4(q)$, причем первые две из них перестановочны. Матричные вычисления в группе $GL_4(q)$ показывают, что

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

$$(\gamma^{\alpha\beta}\gamma)^2 = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & u & 1 & 0 \\ -u & 0 & 0 & 1 \end{pmatrix}, \quad \gamma\gamma^{\alpha\beta}\gamma = \begin{pmatrix} -1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -u & u & 0 & 1 \end{pmatrix},$$

$$(\gamma\gamma^{\alpha\beta}\gamma)^\beta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & -u & -u \\ 0 & 0 & -1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \delta := (\gamma^{\alpha\beta}\gamma)^2(\gamma\gamma^{\alpha\beta}\gamma)^\beta = \begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & u & u \\ 0 & u & -u^2-1 & -u^2+1 \\ -u & 0 & 0 & 1 \end{pmatrix},$$

$$\delta^\alpha = \begin{pmatrix} 1 & 0 & 0 & u \\ -u^2+1 & -u^2-1 & -u & 0 \\ -u & -u & -1 & 0 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad \delta\delta^\alpha = \begin{pmatrix} -1 & 0 & 0 & -u \\ -1 & 1 & 0 & -u \\ -u & 0 & 1 & u^2-1 \\ -u & 0 & 0 & -u-1 \end{pmatrix},$$

$$\gamma\delta\delta^\alpha = \begin{pmatrix} 1 & 0 & 0 & u \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & -u^2-1 \\ 0 & 0 & 0 & -1 \end{pmatrix}, \quad \gamma^\alpha = \begin{pmatrix} 1 & 0 & 0 & u \\ 0 & 1 & 0 & u \\ 0 & 0 & 1 & -1 \\ 0 & 0 & 0 & -1 \end{pmatrix},$$

$$\theta := \gamma\delta\delta^\alpha\gamma^\alpha = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & u \\ 0 & 0 & 1 & u^2 \\ 0 & 0 & 0 & 1 \end{pmatrix} = t_{24}(u)t_{34}(u^2), \quad \theta^\beta = \begin{pmatrix} 1 & -u^2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & -u & 0 & 1 \end{pmatrix},$$

$$\theta^\beta\gamma\gamma^{\alpha\beta}\gamma = \begin{pmatrix} -1 & -u^2-1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ -u & 0 & 0 & 1 \end{pmatrix}, \quad (\theta^\beta\gamma\gamma^{\alpha\beta}\gamma)^2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & u^3+u & 0 & 1 \end{pmatrix} = t_{42}(u^3+u).$$

Заметим, что $u^3 + u \neq 0$. Далее,

$$(t_{42}(u^3+u))^{\alpha\beta} = t_{31}(u^3+u), \quad (t_{42}(u^3+u))^\alpha = t_{13}(-u^3-u),$$

$$[\gamma^{\alpha\beta}, t_{31}(u^3+u)] = t_{32}(u^3+u), \quad (t_{32}(u^3+u))^\alpha = t_{23}(-u^3-u).$$

Отсюда в силу п. б) леммы 10 получаем для некоторых ненулевых $w_1, w_2 \in \mathbb{F}_q$ мономиальные матрицы

$$\eta_1 := \begin{pmatrix} 0 & 0 & -w_1^{-1} & 0 \\ 0 & 1 & 0 & 0 \\ w_1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \eta_2 := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & -w_2^{-1} & 0 \\ 0 & w_2 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

и диагональные матрицы $diag(-1,1,-1,1), diag(1,-1,-1,1)$. Следовательно, в подгруппе M лежат также матрицы

$$(t_{24}(u)t_{34}(u^2)\, diag(-1,1,-1,1))^2 = t_{24}(-u), \quad (t_{24}(-u))^{\beta} = t_{42}(u).$$

Подгруппа, порожденная мономиальными матрицами $\alpha\beta$, η_1, η_2, содержит прообраз любой матрицы-перестановки. Поэтому в силу лемм 8 и 9 она вместе с трансвекциями $t_{24}(u)$ и $t_{42}(u)$ порождает $SL_4(q)$. Так как определитель матрицы γ равен -1, то M совпадает с подгруппой всех матриц из $GL_4(q)$, определитель которых равен ± 1.

Поскольку u — примитивный элемент поля $\mathbb{F}_q$, а число $(q-1)/2$ нечетно, то элемент $-u^4$ также является примитивным для поля $\mathbb{F}_q$. Поэтому по лемме 3 матрицы $diag(u,u,u,u)\alpha$, β, γ порождают всю $GL_4(q)$, а их образы являются инволюциями и порождают группу $PGL_4(q)$, причем первые две из них перестановочны.

Пусть $char\mathbb{F}_q \neq 3$. Положим

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

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

Матричные вычисления в группе $GL_4(q)$ показывают, что

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

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

Поэтому в M имеются элементы

$$diag(-1,-1,1,1) = \big((\gamma\gamma^{\alpha\beta}\gamma)\alpha\beta\big)^{\alpha}\big(\gamma\gamma^{\alpha\beta}\gamma\big), \quad t_{31}(2u)t_{41}(2u) = [diag(-1,-1,1,1), \gamma],$$

а следовательно, и

$$diag(-1,1,1,1)\, t_{21}(1) = \gamma t_{31}(-u)t_{41}(-u), \quad t_{14}(u)t_{24}(u) = (t_{31}(-u)t_{41}(-u))^{\gamma}.$$

Наконец,

$$(t_{14}(u)t_{24}(u))\,((diag(-1,1,1,1)t_{21}(1)))^2 = t_{24}(3u),$$

Так как $char\mathbb{F}_q \neq 3$, то $t_{24}(u) \in M$. Дальнейшие выкладки подобны выкладкам из подслучая $char\mathbb{F}_q = 3$, и мы их опускаем. Таким образом, при $char\mathbb{F}_q \neq 3$ группа $PGL_4(q)$ также является $(2 \times 2, 2)$-порожденной.

Теорема доказана.

Авторы глубоко признательны рецензенту за указанные опечатки и полезные замечания, которые несомненно способствовали улучшению текста статьи.

СПИСОК ЛИТЕРАТУРЫ

1. The Kourovka notebook. Unsolved problems in group theory / eds. V.D. Mazurov, E.I. Khukhro. 20th ed. Novosibirsk: Inst. Math. SO RAN Publ., 2022. 269 p. URL: https://kourovka-notebook.org/ .
2. **Нужин Я.Н.** О порождающих множествах инволюций простых конечных групп // Алгебра и логика. 2019. Vol. 58, № 3. P. 426–434. https://doi.org/10.33048/alglog.2019.58.310
3. **Sjerve D., Cherkassoff M.** On groups generated by three involutions, two of which commute // CRM Proceedings and Lecture Notes. Vol 6. Providence: Amer. Math. Soc., 1994. P. 169–185. https://doi.org/10.1090/crmp/006/09
4. **Conder M., Oliveros D.** The intersection condition for regular polytopes // J. Combin. Theory Ser. A. 2013. Vol. 120, no. 6. P. 1291–1304. https://doi.org/10.1016/j.jcta.2013.03.009
5. **Leemans D.** String C-group representations of almost simple groups: A survey // Contemporary Math. 2021. Vol. 764. P. 157–178. https://doi.org/10.1090/conm/764/15335
6. **Супруненко Д.А.** Группы матриц, М.: Наука, 1972, 351 р.
7. **Нужин Я.Н.** Тензорные представления и порождающие множества инволюций некоторых матричных групп // Тр. Ин-та математики и механики УрО РАН. 2020. Vol. 26, № 3. С. 133–141. https://doi.org/10.21538/0134-4889-2020-26-3-133-141
8. **Scott L.L.** Matricies and cohomology // Annals of Math. 1977. Vol. 105, no. 3. P. 473–492. https://doi.org/10.2307/1970920
9. **Левчук В. М.** О порождающих множествах корневых элементов групп Шевалле над полем // Алгебра и логика. 1983. Vol. 22, №5. P. 504–517.
10. **Левчук В. М.** Замечание к теореме Л. Диксона // Алгебра и логика. 1983. Vol. 22, № 4. P. 421–434.
11. **Markovskaya I. A., Nuzhin Ya. N.** On generation of the groups $GL_n(Z)$ and $PGL_n(Z)$ by three involutions, two of which commute // J. Siberian Federal Univ. Mathematics & Physics 2023. Vol. 16, №4. P. 413–419. EDN: BHNJYZ .

Поступила 11.04.2025
После доработки 25.04.2025
Принята к публикации 28.04.2025
Опубликована онлайн 12.05.2025

Марковская Ирина Александровна
аспирант
Институт математики и фундаментальной информатики,
Сибирский федеральный университет
г. Красноярск
e-mail: mark.i.a@mail.ru

Нужин Яков Нифантьевич
д-р физ.-мат. наук, профессор
зав. кафедрой
Институт математики и фундаментальной информатики,
Сибирский федеральный университе
г. Красноярск
e-mail: nuzhin2008@rambler.ru

REFERENCES

1. The Kourovka notebook. Unsolved problems in group theory / eds. V.D. Mazurov, E.I. Khukhro. 20th ed. Novosibirsk: Inst. Math. SO RAN Publ., 2022. 269 p. URL: https://kourovka-notebook.org/ .
2. Nuzhin Ya.N. Generating sets of involutions of finite simple groups. *Algebra and Logic*, 2019, vol. 58, no. 3, pp. 288–293 https://doi.org/10.1007/s10469-019-09547-x
3. Sjerve D., Cherkassoff M. On groups generated by three involutions, two of which commute. *CRM Proceedings and Lecture Notes*, Providence, Amer. Math. Soc., 1994, pp. 169–185. https://doi.org/10.1090/crmp/006/09
4. Conder M., Oliveros D. The intersection condition for regular polytopes. *J. Combin. Theory Ser. A*, 2013, vol. 120, no. 6, pp. 1291–1304.
5. Leemans D. String C-group representations of almost simple groups: A survey. *Contemporary Math.*, 2021, vol. 764, pp. 157–178.
6. Suprunenko D.A. Matrix groups. Providence: AMS, 1976, 252 p. ISBN: 0821813412 . Original Russian text published in Suprunenko D.A. Gruppy matrits, Moscow: Nauka Publ., 1972, 352 p.
7. Nuzhin Ya.N. Tensor representations and generating sets of involutions of some matrix groups. *Trudy Instituta Matematiki i Mekhaniki URO RAN*, 2020, vol. 26, no. 3, pp. 133–141. https://doi.org/10.21538/0134-4889-2020-26-3-133-141
8. Scott L.L. Matricies and cohomology. *Annals of Math.*, 1977, vol. 105, no. 3, pp. 473–492. https://doi.org/10.2307/1970920
9. Levchuk V.M. Generating sets of root elements of Chevalley groups over a field. *Algebra and Logic*, 1983, vol. 22, pp. 362–371. https://doi.org/10.1007/BF01982113
10. Levchuk V.M. Remark on a theorem of L. Dickson. *Algebra and Logic*, 1983, vol. 22, pp. 306–316. https://doi.org/10.1007/BF01979677
11. Markovskaya I.A., Nuzhin Ya.N. On generation of the groups $GL_n(Z)$ and $PGL_n(Z)$ by three involutions, two of which commute. *J. Siberian Federal Univ. Mathematics & Physics*, 2023, vol. 16, no. 4, pp. 413–419.

Received April 11, 2024
Revised April 25, 2024
Accepted April 28, 2025
Published online May 12, 2025

Funding Agency: This work was supported by Russian Science Foundation, project 25-21-20059, https://rscf.ru/project/25-21-20059/ .

Irina Aleksandrovna Markovskaya, doctoral student, Institute of Mathematics and Computer Science of the Siberian Federal University, Krasnoyarsk, 660041 Russia, e-mail: mark.i.a@mail.ru .

Yakov Nifantievich Nuzhin, Dr. Phys.-Math. Sci., Prof. Institute of Mathematics and Computer Science of the Siberian Federal University, Krasnoyarsk, 660041 Russia,
e-mail: nuzhin2008@rambler.ru .

Cite this article as: I. A. Markovskaya, Ya. N. Nuzhin. On generation of the groups $GL_n(q)$ and $PGL_n(q)$ by three involutions, two of which commute. *Trudy Instituta Matematiki i Mekhaniki UrO RAN*, 2025, vol. 31, no. 4, pp. 247–259.