

МИНИМАЛЬНОЕ ЧИСЛО
ПОРОЖДАЮЩИХ СОПРЯЖЕННЫХ ИНВОЛЮЦИЙ,
ПРОИЗВЕДЕНИЕ КОТОРЫХ РАВНО 1,
ГРУПП $PSp_4(q)$

Р.И. ГВОЗДЕВ, Я.Н. НУЖИН, Т.С. ПЕТРУТЬ,
А.М. СОКОЛОВСКАЯ

Представлено И.Б. ГОРШКОВЫМ

Abstract: The solution of the following problem by G. Malle, J. Saxl and T. Weigel has been completed for the projective symplectic groups $PSp_4(q)$, (see also question 14.69c) from the Kourovka Notebook). For each finite simple non-Abelian group G , find $n_c(G)$ which is the minimal number of generating conjugate involutions whose product is equal to 1. It turns out that if $G = PSp_4(q)$, then $n_c(G) = 5$ for $q \neq 2, 3$, $n_c(G) = 6$ for $q = 3$, and $n_c(G) = 10$ for $q = 2$ (in this case, the group G is not simple).

Keywords: Finite simple group, symplectic group, finite field, generating sets of involutions.

1 Введение

В 1994 году Г. Малле, Я. Саксл и Т. Вайгель в работе [1] записали следующую задачу (см. также Коуровскую тетрадь [2, вопрос 14.69в]).

R.I. GVOZDEV, YA.N. NUZHIN, T.S. PETRUT, A.M. SOKOLOVSKAYA, THE MINIMUM NUMBER OF GENERATING CONJUGATE INVOLUTIONS WHOSE PRODUCT IS EQUAL TO 1, OF THE GROUPS $PSp_4(q)$.

© 2025 Р.И. ГВОЗДЕВ, Я.Н. НУЖИН, Т.С. ПЕТРУТЬ, А.М. СОКОЛОВСКАЯ.

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

Поступила 16 декабря 2024 г., опубликована 15 сентября 2025 г.

А) Для каждой конечной простой неабелевой группы G найти $n_c(G)$ — минимальное число порождающих сопряженных инволюций, произведение которых равно 1.

Такое число $n_c(G)$ существует, поскольку каждая конечная простая неабелева группа G порождается любым своим классом сопряженных инволюций. К настоящему времени задача А) решена для спорадических и знакопеременных групп и $PSL_n(q)$ при нечетном q , для $q \neq 9$ при $n \geq 4$ и $q \not\equiv 3 \pmod{4}$ при $n = 6$ [3]; группы $PSL_n(9)$ при $n \geq 4$ рассмотрены в [4, 5]. Также её решение завершено в [6] для групп с одним классом сопряженных инволюций, к которым относятся все группы лиева типа ранга 1 и три группы ранга 2, а именно, $PSL_3(q)$ при любом q и при нечетном q группы $G_2(q)$ и ${}^3D_4(q^3)$. Группы ранга 2 разбиваются на семь типов и в лиевой терминологии обозначаются так:

$$A_2(q), B_2(q), {}^2A_3(q^2), {}^2A_4(q^2), G_2(q), {}^3D_4(q^3), {}^2F_4(2^{2k+1}). \quad (1)$$

Первые четыре группы из списка (1) изоморфны классическим группам $PSL_3(q)$, $PSp_4(q)$, $PSU_4(q^2)$ и $PSU_5(q^2)$ соответственно. К настоящему времени число $n_c(G)$ известно, и оно равно 5 или 6, для следующих групп лиева типа ранга 2:

- $PSL_3(q)$ при нечетном q [3];
- $PSL_3(2^k)$ [6];
- $PSp_4(q)$ при $q \equiv 3 \pmod{4}$, $q \neq 3$, [7];
- $PSU_4(q^2)$ при $q \equiv 3 \pmod{4}$, $q \neq 3$, [7];
- $PSU_4(2^{2k})$ [8];
- $PSU_5(2^{2k})$ [7];
- $G_2(q)$ и ${}^3D_4(q^3)$ при нечетном q [9].

Мы завершаем решение задачи А) для проективных симплектических групп $PSp_4(q)$, рассмотрев случаи $q \equiv 1 \pmod{4}$, $q = 2^k$ и $q = 3$. Доказана

Теорема 1. а) $n_c(PSp_4(q)) = 5$, если $q \equiv 1 \pmod{4}$ или $q = 2^n$, $n > 1$.

б) $n_c(PSp_4(3)) = 6$.

в) $n_c(PSp_4(2)) = 10$.

В [7] доказано, что $n_c(PSp_4(q)) = 5$, если $q \equiv 3 \pmod{4}$ и $q \neq 3$. Объединяя этот результат с теоремой 1, получаем

Следствие 1. а) $n_c(PSp_4(q)) = 5$, при $q \neq 2, 3$.

б) $n_c(PSp_4(3)) = 6$.

в) $n_c(PSp_4(2)) = 10$.

Утверждение п. а) теоремы 1 вытекает из следующей теоремы.

Теорема 2. Группа $PSp_4(q)$ при $q \equiv 1 \pmod{4}$ или $q = 2^n$, $n > 1$, порождается тремя инволюциями α , β , γ , первые две из которых перестановочны, и все четыре инволюции α , β , γ и $\alpha\beta$ сопряжены.

Аналогичный результат был получен в работе [7] для групп $PSp_4(q)$ при $q \equiv 3 \pmod{4}$ и $q \neq 3$. Объединяя его с теоремой 2, получаем

Следствие 2. *Группа $PSp_4(q)$ при $q \neq 2, 3$ порождается тремя инволюциями α, β, γ , первые две из которых перестановочны, и все четыре инволюции α, β, γ и $\alpha\beta$ сопряжены.*

Доказательство теоремы 2 при $q \neq 2, 3$, как и указанного выше результата из [7], состоит в том, что необходимые тройки порождающих инволюций указываются явно. Причем для исключительных случаев $q = 5$ и $q = 9$ порождающие найдены при помощи компьютерных вычислений в системе GAP, однако, окончательный вариант доказательства доступен для проверки без использования компьютера.

В заключение отметим следующий полезный при решении задачи А) результат М. А. Всемирнова и Я. Н. Нужиной [10]: любая конечная простая неабелева группа, отличная от $PSU_3(3^2)$ и A_8 , порождается тремя сопряженными инволюциями. Используя этот результат и учитывая, что $n_c(PSU_3(3^2)) = n_c(A_8) = 7$, и что $5 \leq n_c(G)$ для любой конечной простой неабелевой группы G [11, лемма 4], получаем для таких групп точные оценки числа $n_c(G)$ снизу и сверху

$$5 \leq n_c(G) \leq 7. \quad (2)$$

Заметим, что пункт в) теоремы 1 не противоречит верхней оценке из (2), так как группа $PSp_4(2)$ не является простой.

2 Обозначения и предварительные результаты

Пусть Φ — приведенная неразложимая система корней, $\Phi(K)$ — присоединенная группа Шевалле типа Φ над полем K . Группа $\Phi(K)$ порождается корневыми подгруппами

$$X_r = \{x_r(t) \mid t \in K\}, \quad r \in \Phi.$$

Для ненулевых элементов $t \in K^*$ определены мономиальные

$$n_r(t) = x_r(t)x_{-r}(-t^{-1})x_r(t)$$

и диагональные

$$h_r(t) = n_r(t)n_r(-1)$$

элементы группы $\Phi(K)$. Для краткости положим

$$n_r = n_r(1).$$

Другие обозначения, связанные с группами лиева типа, такие же как в книге Р. Картера [12]. В статье приняты также такие сокращения: $\langle M \rangle$ — подгруппа, порожденная подмножеством M из некоторой группы G ,

$$x^y = yxy^{-1},$$

$$[x, y] = xyx^{-1}y^{-1}.$$

Пусть χ — K -характер решетки корней $\mathbb{Z}\Phi$, n_w — прообраз в N элемента $w \in W$ при естественном гомоморфизме мономиальной подгруппы N на группу Вейля W . Тогда

$$n_w h(\chi) n_w^{-1} = h(\chi'), \quad (3)$$

где $\chi'(r) = \chi(w^{-1}(r))$ для всех $r \in \Phi$ [12, теорема 7.2.2]. В частности,

$$n_r h_s(t) n_r^{-1} = h_{w_r(s)}(t), \quad r, s \in \Phi. \quad (4)$$

Диагональные элементы действуют на корневых элементах следующим образом

$$h(\chi) x_s(u) h^{-1}(\chi) = x_s(u\chi(s)), \quad s \in \Phi, \quad (5)$$

в частности, если $h(\chi) = h_r(t)$, то

$$h_r(t) x_s(u) h_r^{-1}(t) = x_s(ut^{\frac{2(r,s)}{(r,r)}}), \quad r, s \in \Phi. \quad (6)$$

Через Φ^+ обозначим множество положительных корней.

Лемма 1. [7, лемма 9] Пусть χ — K -характер, $r_1, \dots, r_k \in \Phi^+$, $r_i + r_j \notin \Phi$ для любых i, j , и $\chi(r_i) \neq 1$ для каждого i . Тогда элементы $h(\chi)$ и $h(\chi) x_{r_1}(t_1) \cdots x_{r_k}(t_k)$ сопряжены.

При сопряжении корневых элементов мономиальными элементами в случае нечетной характеристики основного поля, нам потребуются некоторые свойства чисел $\eta_{r,s}$, зависящих от знаков (+ или −) структурных констант $N_{r,s}$, $r, s \in \Phi$, простой комплексной алгебры Ли типа B_2 . Числа $\eta_{r,s}$ равны ± 1 и определяются равенствами

$$n_r x_s(t) n_r^{-1} = x_{w_r(s)}(\eta_{r,s} t), \quad r, s \in \Phi, \quad (7)$$

причем

$$\eta_{r,\pm r} = -1, \quad (8)$$

(см., например, [12, стр. 95]). В свою очередь, знаки у структурных констант $N_{r,s}$ можно выбирать произвольным образом для экстраспециальных пар (r, s) [12, предложение 4.2.2].

Лемма 2. [7, лемма 6] Пусть Φ — система корней типа B_2 , а $\{a, b\}$ — множество её фундаментальных корней, где корень a короткий. Тогда множество экстраспециальных пар состоит из двух пар (a, b) и $(a, a+b)$ и справедливы равенства:

- 1) $\eta_{r,s} = -1$, если r, s — короткие линейно независимые корни;
- 2) $\eta_{r,s} = 1$, если r, s — длинные линейно независимые корни;
- 3) $\eta_{b,a} = -\eta_{b,a+b} = -N_{a,b}$;
- 4) $\eta_{2a+b,a} = -\eta_{2a+b,a+b} = -N_{a,a+b}/|N_{a,a+b}|$;
- 5) $\eta_{a,b} = \eta_{a,2a+b} = N_{a,b}N_{a,a+b}/|N_{a,a+b}|$;
- 6) $\eta_{a+b,b} = \eta_{a+b,2a+b} = -N_{a,b}N_{a,a+b}/|N_{a,a+b}|$.

Лемма 3. [7, лемма 8] Пусть Φ и корни a, b такие же как в лемме 2. Тогда для мономиальных элементов

$$n_r = x_r(1) x_{-r}(-1) x_r(1), \quad r \in \Phi,$$

из присоединенной группы Шевалле $B_2(K)$ над полем K характеристики p справедливы следующие свойства:

- 1) $n_r^2 = 1$, в частности, $h_r(-1) = 1$, если корень r короткий;
- 2) если корень r длинный, то $|n_r| = 2$ для $p = 2$ и $|n_r| = 4$ для $p \neq 2$;
- 3) если оба корня r, s длинные, то $h_r(-1) = h_s(-1)$;
- 4) произведения $n_a n_{a+b}$ и $n_b n_{2a+b}$ являются инволюциями;
- 5) $n_a n_{a+b} = n_b n_{2a+b}$, если знаки у структурных констант $N_{a,b}$ и $N_{a,a+b}$ выбраны так, что $N_{a,b} = -N_{a,a+b}/|N_{a,a+b}|$.

Элемент t конечного поля $GF(q)$ мощности q называется *собственным* (соответственно *примитивным*) элементом, если он не лежит ни в каком его собственном подполе (соответственно если он порождает его мультипликативную группу).

Л. Диксон [13] описал с точностью до изоморфизма подгрупповое строение группы $PSL_2(q)$. Из результатов [13] вытекает следующее утверждение, называемое теоремой Диксона (впервые такая формулировка теоремы появилась в монографии Д. Горенштейна [14, теорема 2.8.4]).

Лемма 4. Если t, t^2 — собственные элементы поля $GF(p^n)$, $p > 2$ и $p^n \neq 9$, то

$$\left\langle \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}, \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \right\rangle = SL_2(p^n).$$

Теорема Диксона оказывается весьма полезным инструментом в теории групп лиева типа, поскольку группа, порожденная двумя корневыми подгруппами X_r и X_{-r} , изоморфна $SL_2(K)$ или $PSL_2(K)$ [12, теорема 6.3.1]. Однако, формулировку леммы 4 нельзя распространить на исключительные случаи $p = 2$ и $p^n = 9$. Следующие две леммы являются следствием основной теоремы из статьи В. М. Левчука [15], и они позволяют успешно работать с порождающими множествами из трех корневых элементов и в этих исключительных случаях.

Лемма 5. Пусть $V \subseteq GF(p^n)$, $|V| > 2$ и некоторый примитивный элемент t поля $GF(p^n)$ лежит в V . Тогда

$$\left\langle \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & V \\ 0 & 1 \end{pmatrix} \right\rangle = SL_2(p^n).$$

Лемма 6. Если u, v — ненулевые элементы поля $GF(p^n)$, то для некоторого ненулевого $t \in GF(p^n)$ подгруппа $\langle t_{21}(u), t_{12}(v) \rangle$ содержит номинальную матрицу

$$\delta = \begin{pmatrix} 0 & -t^{-1} \\ t & 0 \end{pmatrix}.$$

Частным случаем предложения 2 из [16] при $G = B_2(q)$ является

Лемма 7. Пусть t и t^2 — собственные элементы поля $GF(p^n)$, Φ — система корней типа B_2 , Π — множество её фундаментальных корней, M — подгруппа группы $B_2(q)$. Тогда, если $M \cap X_r \neq 1$, $r \in \Pi \cup -\Pi$, и $x_s(t), x_{-s}(t) \in M$ для некоторого $s \in \Phi$, то $M = B_2(q)$.

Далее в доказательствах равенства (3)–(8) мы будем использовать без упоминания, и всюду $\{a, b\}$ — множество фундаментальных корней для системы типа B_2 , причем корень a короткий как на рис. 1.

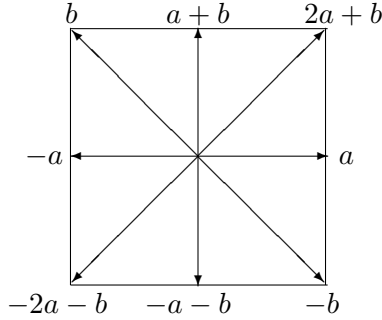


Рис. 1

Для группы $B_2(K)$ коммутаторная формула Шевалле имеет один из следующих двух видов:

$$\begin{aligned}[x_a(t), x_b(u)] &= x_{a+b}(\pm tu)x_{2a+b}(\pm t^2u), \\ [x_a(t), x_{a+b}(u)] &= x_{2a+b}(\pm 2tu).\end{aligned}$$

Укажем также наиболее часто применяемые далее случаи формулы (6). Пусть $\varepsilon = \pm 1$. Тогда

$$\begin{aligned}h_a(u)x_{\varepsilon a}(1)h_a^{-1}(u) &= x_{\varepsilon a}(u^{\varepsilon^2}), \\ h_a(u)x_{\varepsilon(2a+b)}(1)h_a^{-1}(u) &= x_{\varepsilon(2a+b)}(u^{\varepsilon^2}), \\ h_a(u)x_{\varepsilon b}(1)h_a^{-1}(u) &= x_{\varepsilon b}(u^{-\varepsilon^2}).\end{aligned}$$

В компьютерных вычислениях мы используем точное 4-мерное матричное представление универсальной группы Шевалле типа B_2 над полем K , изоморфной симплектической группе $Sp_4(K)$. Группу $B_2(K)$ можно рассматривать как централизатор графового автоморфизма универсальной группы Шевалле типа A_3 , которая, в свою очередь, изоморфна специальной линейной группе $SL_4(K)$. Поэтому универсальная группа $B_2(K)$ изоморфна группе, порожденной матрицами

$$\begin{aligned}x_a(t) &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ t & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & t & 1 \end{pmatrix}, \quad x_{-a}(t) = \begin{pmatrix} 1 & t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & t \\ 0 & 0 & 0 & 1 \end{pmatrix}, \\ x_b(t) &= \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & t & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad x_{-b}(t) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & t & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},\end{aligned}$$

$$x_{a+b}(t) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ t & 0 & 1 & 0 \\ 0 & -t & 0 & 1 \end{pmatrix}, \quad x_{-a-b}(t) = \begin{pmatrix} 1 & 0 & t & 0 \\ 0 & 1 & 0 & -t \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$x_{2a+b}(t) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ t & 0 & 0 & 1 \end{pmatrix}, \quad x_{-2a-b}(t) = \begin{pmatrix} 1 & 0 & 0 & t \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Это согласуется с леммой 13.6.2 из [12]. Применяя данное представление, можно проверить на матричном языке все наши, иногда не очень короткие, вычисления.

3 Доказательство теоремы 2 для $q = 2^n$, $q > 2$

В группе $B_2(2^n)$ имеется три класса сопряженных инволюций, с представителями

$$\begin{aligned} \sigma_1 &= x_{-a}(1), \\ \sigma_2 &= x_{-b}(1), \\ \sigma_3 &= x_{-a}(1)x_{-a-b}(1). \end{aligned}$$

Обозначим через H класс с представителем σ_3 . Выделим в нем следующие три элемента

$$\begin{aligned} \alpha &= n_a x_{-b}(1) x_{-a-b}(1) x_{-2a-b}(1) = \sigma_3^{x_{-b}(1)x_a(1)}, \\ \beta &= x_b(1) x_{a+b}(1) x_{2a+b}(1) n_a = \alpha^{n_b n_a n_b}, \\ \gamma &= x_{-a}(1) x_{-a-b}(1) x_{-2a-b}(t) = \sigma_3^{x_{-b}(t)h_{-a-b}(\sqrt{t+1})}, \end{aligned}$$

где t — примитивный элемент конечного поля $\mathbb{F}_{2^n}$. Так как

$$\begin{aligned} \sigma_3^{x_{-a}(1)x_{-a-b}(1)x_b(1)n_a n_{a+b}} &= (x_a(1)x_{a+b}(1))^{x_{-a}(1)x_{-a-b}(1)x_b(1)} = \\ &= (x_a(1)x_{2a+b}(1))^{x_{-a}(1)x_{-a-b}(1)} = (x_a(1)x_{2a+b}(1)x_a(1)x_{-b}(1))^{x_{-a}(1)} = \\ &= x_b(1)x_{a+b}(1)x_{2a+b}(1)x_{-b}(1)x_{-a-b}(1)x_{-2a-b}(1) = \beta\alpha, \end{aligned}$$

то произведение $\beta\alpha$ также лежит в H , в частности, инволюции α и β перестановочны.

Для доказательства теоремы 2 достаточно показать, что подгруппа

$$M = \langle \alpha, \beta, \gamma \rangle$$

совпадает с группой $B_2(2^n)$. Вычисления показывают, что

$$(\alpha\gamma)^3 = x_{-a-b}(t).$$

Действительно,

$$(\alpha\gamma)^3 = (n_a x_{-b}(1) x_{-a}(1) x_{-2a-b}(t+1))^3 =$$

$$= n_a(x_{-b}(1)x_{-a}(1)x_{-2a-b}(t+1)n_ax_{-b}(1)x_{-a}(1)x_{-2a-b}(t+1))n_a \times \\ \times x_{-b}(1)x_{-a}(1)x_{-2a-b}(t+1).$$

Вычислим отдельно сомножитель

$$n_a(x_{-b}(1)x_{-a}(1)x_{-2a-b}(t+1)n_ax_{-b}(1)x_{-a}(1)x_{-2a-b}(t+1))n_a.$$

Он равен

$$\begin{aligned} & x_{-2a-b}(1)x_a(1)x_{-b}(t+1)n_ax_{-2a-b}(1)x_a(1)x_{-b}(t+1) = \\ & = x_{-2a-b}(1)x_{-b}(t+1)x_{-a}(1)x_a(1)x_{-2a-b}(1)x_a(1)x_{-b}(t+1) = \\ & = x_{-2a-b}(1)x_{-b}(t+1)x_{-a}(1)x_{-2a-b}(1)\{[x_{-2a-b}(1), x_a(1)]\}x_{-b}(t+1) = \\ & = x_{-2a-b}(1)x_{-b}(t+1)x_{-a}(1)x_{-2a-b}(1)\{x_{-a-b}(1)x_{-b}(1)\}x_{-b}(t+1) = \\ & = x_{-b}(t+1)x_{-a}(1)x_{-b}(t+1)x_{-a-b}(1)x_{-b}(1) = \\ & = x_{-a}(1)\{[x_{-a}(1), x_{-b}(t+1)]\}x_{-a-b}(1)x_{-b}(1) = \\ & = x_{-a}(1)\{x_{-a-b}(t+1)x_{-2a-b}(t+1)\}x_{-a-b}(1)x_{-b}(1) = \\ & = x_{-a-b}(t)x_{-a}(1)x_{-2a-b}(t+1)x_{-b}(1). \end{aligned}$$

Сейчас равенство $(\alpha\gamma)^3 = x_{-a-b}(t)$ становится очевидным. Отметим, что это равенство, как и порождающие инволюции, изначально были найдены для $q = 4, 8$ с помощью компьютера в матричном представлении, указанном в параграфе 2. Далее,

$$\begin{aligned} \gamma^\alpha &= x_a(1)x_{-b}(t+1), \\ \eta &= \gamma^\alpha\beta\gamma^\alpha = x_{-b}(t+1)(x_b(1)x_{-a}(1))x_{-b}(t+1), \\ ((\alpha\gamma)^3)^\eta &= (x_{-a-b}(t)x_{-a}(t)x_{-2a-b}(t^2))^{x_{-b}(t+1)} = x_{-a}(t)x_{-a-b}(t^2)x_{-2a-b}(t^3), \\ \theta &= (((\alpha\gamma)^3)^\eta)^\alpha = (x_{-a}(t)x_{-a-b}(t^2+t)x_{-2a-b}(t^3+t^2))^{n_a} = \\ &= x_a(t)x_{-a-b}(t^2+t)x_{-b}(t^3+t^2). \end{aligned}$$

Корневые подгруппы X_a и X_{-a} нормализуют группу $X_{-b}X_{-a-b}X_{-2a-b}$. Поэтому, в силу леммы 5 для любого $u \in F^*$ и некоторых $u_i \in F$ в группе $\langle \gamma, \gamma^\alpha, \theta \rangle$ имеется элемент

$$h_a(u)x_{-b}(u_1)x_{-a-b}(u_2)x_{-2a-b}(u_3),$$

квадрат которого для подходящих $v_i \in F$ равен

$$h_a(u^2)x_{-b}(v_1)x_{-2a-b}(v_2).$$

Таким образом, для некоторых $y, z \in F$ в подгруппе M лежит элемент

$$\mu = h_a(\sqrt{t^{-1}})x_{-b}(y)x_{-2a-b}(z).$$

Вычисления показывают, что

$$\begin{aligned} \gamma^\mu &= (x_{-a}(1)x_{-a-b}(y+1)x_{-2a-b}(y+t))^{h_a(\sqrt{t^{-1}})} = \\ &= x_{-a}(t)x_{-a-b}(y+1)x_{-2a-b}((y+t)t), \\ \gamma^\mu((\alpha\gamma)^3)^\eta &= x_{-a-b}(y+1+t^2)x_{-2a-b}((y+t)t+t^3). \end{aligned}$$

Далее доказательство разбивается на два случая, в зависимости от того равняется нулю сумма $(y+t)t+t^3$ или нет.

Случай 1. Пусть $(y + t)t + t^3 \neq 0$. Тогда

$$[\mu, \gamma^\mu((\alpha\gamma)^3)^\eta] = x_{-2a-b}(((y + t)t + t^3)(t + 1)),$$

а учитывая, что $t \neq 1$, получаем включение $x_{-2a-b}(v) \in M$ для некоторого ненулевого $v \in F$. Сопрягая корневой элемент $x_{-2a-b}(v)$ всевозможными элементами $h_a(u^2)x_{-b}(v_1)x_{-2a-b}(v_2)$, получим включение $X_{-2a-b} < M$. Отсюда $X_{-2a-b}^\alpha = X_{-b} < M$. Следовательно, диагональная подгруппа $H_a = \{h_a(u) \mid u \in F^*\}$ лежит в M . Коммутируя γ и $x_{-b}(1)$, получаем $x_{a+b}(1)x_{2a+b}(1)$. Отсюда $x_{-a}(1) \in M$. Сопрягая последний элемент всевозможными элементами из H_a , получим включение $X_{-a} < M$. Подгруппы $X_{-a}, X_{-b}, X_{-2a-b}$ порождают всю (верхнюю) унипотентную подгруппу V . Сейчас, используя вид инволюции α , имеем $n_a \in M$ и, следовательно,

$$\begin{aligned} \beta n_a &= x_b(1)x_{a+b}(1)x_{2a+b}(1) \in M, \\ (\beta n_a)^{x_{-a}(1)} &= x_{2a+b}(1). \end{aligned}$$

Подгруппа, порожденная элементом $x_{2a+b}(1)$ и подгруппой H_a , содержит корневую подгруппу X_{2a+b} . Наконец, $X_{-a}^{n_a} = X_a$ и $X_{2a+b}^{n_a} = X_b$. Остается заметить, что подгруппы X_a, X_b, V порождают всю группу Шевалле $B_2(q)$.

Случай 2. Пусть $(y + t)t + t^3 = 0$. Тогда $y = t^2 + t$ и, следовательно,

$$\gamma^\mu((\alpha\gamma)^3)^\eta = x_{-a-b}(t + 1).$$

Сейчас, учитывая ранее полученное включение $x_{-a-b}(t) \in M$, получаем, что

$$\begin{aligned} x_{-a-b}(1) &\in M, \\ \alpha x_{-a-b}(1) &= n_a x_{-b}(1)x_{-2a-b}(1) \in M, \\ \gamma x_{-a-b}(1) &= x_{-a}(1)x_{-2a-b}(t) \in M. \end{aligned}$$

В этом случае

$$\mu = h_a(\sqrt{t^{-1}})x_{-b}(t^2 + t)x_{-2a-b}(z)$$

и вычисления показывают, что

$$\begin{aligned} (x_a(1)x_{-b}(t + 1))^{\mu^{-1}} &= (x_a(t)x_{-b}(t^2 + t))^{x_{-2a-b}(z)} = \\ &= x_a(t)x_{-a-b}(tz)x_{-b}(t^2z + t^2 + t), \\ ((x_a(1)x_{-b}(t + 1))^{\mu^{-1}})^\alpha &= (x_{-a}(t)x_{-a-b}(tz)x_{-2a-b}(t^2z + t^2 + t))^{x_{-b}(1)} = \\ &= x_{-a}(t)x_{-a-b}(tz + t)x_{-2a-b}(t^2z + t), \\ ((x_a(1)x_{-b}(t + 1))^{\mu^{-1}})^\alpha((\alpha\gamma)^3)^\eta &= x_{-a-b}(tz + t + t^2)x_{-2a-b}(t^2z + t + t^3). \end{aligned}$$

Если $t^2z + t + t^3 \neq 0$, то мы попадаем в уже рассмотренный случай 1.

Пусть $t^2z + t + t^3 = 0$. Тогда $z = t + t^{-1}$ и $z \neq 0$, поскольку $t \neq 1$. В этом случае

$$\mu = h_a(\sqrt{t^{-1}})x_{-b}(t^2 + t)x_{-2a-b}(t + t^{-1}).$$

Далее,

$$\beta n_a x_{-b}(1)x_{-2a-b}(1) = x_b(1)x_{a+b}(1)x_{2a+b}(1)x_{-b}(1)x_{-2a-b}(1) =$$

$$\begin{aligned}
&= x_b(1)x_{-b}(1)x_{a+b}(1)x_a(1)x_{-2a-b}(1) = \\
&= n_b x_b(1)x_{a+b}(1)x_{-a-b}(1)x_{-b}(1)x_{-2a-b}(1)x_a(1).
\end{aligned}$$

Сопрягая последний элемент элементом $x_{-b}(t+1)x_a(1)$, получаем

$$\begin{aligned}
&x_{-b}(t+1)n_b x_b(1)x_{-a-b}(1)x_{-b}(1)x_{-2a-b}(1)x_{-b}(t+1) = \\
&= x_{-b}(t)n_b x_{-a-b}(1)x_{-2a-b}(1)x_{-b}(t).
\end{aligned}$$

Так как $x_{-a-b}(1) \in M$, то в M лежит элемент

$$\delta = x_{-b}(t)n_b x_{-2a-b}(1)x_{-b}(t).$$

Далее,

$$\mu^2 = h_a(t^{-1})x_{-b}(t^3 + t)x_{-2a-b}(t + 1 + t^{-1} + t^{-2}).$$

Пусть $g = x_{-b}(t)$, $M' = M^g$. Тогда в M' лежат элементы

$$\begin{aligned}
&\delta^g = n_b x_{-2a-b}(1), \\
&(x_a(1)x_{-b}(t+1))^g = x_a(1)x_{-b}(t+1), \\
&x_{-a-b}(1)^g = x_{-a-b}(1), \\
&(\mu^2)^g = h_a(t^{-1})x_{-2a-b}(t + 1 + t^{-1} + t^{-2}), \\
&((\mu^2)^g)^{\delta^g} = h_{a+b}(t^{-1})x_{-2a-b}(t + t^{-1}), \\
&x_{-a-b}(1)^{\delta^g} = x_{-a}(1).
\end{aligned}$$

Сопрягая многократно корневой элемент $x_{-a}(1)$ элементом $(\mu^2)^g$, получим включение $X_{-a} < M'$, а следовательно, и $X_{-a-b} = X_{-a}^{\delta^g} < M'$. Пусть $f = x_{-2a-b}(t)$, $M'' = (M')^f$. Тогда в M'' лежат следующие элементы

$$\begin{aligned}
&(n_b x_{-2a-b}(1))^f = n_b x_{-2a-b}(1), \\
&X_{-a-b}^f = X_{-a-b}, \\
&X_{-a}^f = X_{-a}, \\
&(x_a(1)x_{-b}(t+1))^f = x_a(1)x_{-a-b}(t)x_{-b}(1), \\
&(h_{a+b}(t^{-1})x_{-2a-b}(t + t^{-1}))^f = h_{a+b}(t^{-1}).
\end{aligned}$$

Элемент t примитивный, поэтому диагональная подгруппа H_{a+b} лежит в M'' . Так как $x_{-a-b}(t) \in M''$, то $x_a(1)x_{-b}(1) \in M''$. Далее,

$$[h_{a+b}(t^{-1}), x_a(1)x_{-b}(1)] = x_{-b}(t^2 + 1).$$

Поскольку $q \neq 2$, то $t^2 + 1 \neq 0$ и поэтому

$$(x_{-b}(t^2 + 1))^{H_{a+b}} = X_{-b} \setminus x_{-b}(0).$$

Следовательно, $x_a(1) \in M''$. Так как $x_{-a}(1) \in M''$, то $n_a \in M''$. Далее, $X_{-b} \in M''$, значит $x_{-b}(1) \in M''$. Тогда

$$\begin{aligned}
&(n_b x_{-2a-b}(1))^{x_{-b}(1)} = x_b(1)x_{-2a-b}(1), \\
&(n_b x_{-2a-b}(1))^{x_b(1)x_{-2a-b}(1)} = x_{-b}(1)x_{-2a-b}(1).
\end{aligned}$$

Перемножая последние два элемента и учитывая включение $x_a(1) \in M''$, получаем $n_b \in M''$. Подгруппа $\langle n_a, n_b \rangle$ изоморфна группе Вейля типа

B_2 и действует сопряжениями транзитивно на множестве корневых подгрупп, индексированных корнями одинаковой длины. Таким образом, в M'' лежат все корневые подгруппы. Поэтому $M'' = B_2(q)$.

Теорема доказана.

4 Доказательство теоремы 2 для $q \equiv 1 \pmod{4}$, $q > 3$

Мы укажем явно порождающие тройки инволюций с необходимыми свойствами для группы $B_2(q)$, $q \equiv 1 \pmod{4}$, $q > 3$, причем при $q > 9$ они такие же как в статье [7] при $q \equiv 3 \pmod{4}$. Наше доказательство порождаемости группы $B_2(q)$ при $q > 9$ данными инволюциями похоже на доказательство из [7], но в некоторых местах пришлось внести существенные изменения, поэтому мы приводим его без сокращений.

Случай $q > 9$. Пусть K — конечное поле порядка $q \equiv 1 \pmod{4}$. Пусть t и t^2 — собственные элементы поля K , а мультипликативный порядок элемента $u \in K$ равен $(q-1)/2$. Покажем, что инволюции

$$\begin{aligned}\alpha &= n_a, \\ \beta &= n_{a+b}, \\ \gamma &= (n_a h_a(u))^{x_{a+b}(t)x_b(1)}\end{aligned}$$

удовлетворяют условиям теоремы.

В силу пп. 1) и 4) леммы 3 мономиальные элементы n_a , n_{a+b} являются перестановочными инволюциями. Они инвертируют диагональные элементы $h_a(u)$ и $h_{a+b}(u)$ соответственно. Поэтому α , β , γ — инволюции и $\alpha\beta = \beta\alpha$. Инволюции α , β , γ сопряжены. Действительно, $\alpha = n_b\beta n_b^{-1}$, $\alpha = \gamma^{h_a(s)x_{a+b}(-t)x_b(-1)}$, где $s^2 = u$. Такой элемент s существует, так как порядок элемента u равен $(q-1)/2$. Используя равенство $\eta_{a,a+b} = -1$ из п. 1) леммы 2, получаем

$$\begin{aligned}(n_a n_{a+b})^{x_{a+b}(1)} &= n_a x_{-a-b}(-1), \\ (n_a x_{-a-b}(-1))^{x_{-a-b}(-1/2)} &= n_a = \alpha.\end{aligned}$$

Таким образом, инволюции $\alpha\beta = n_a n_{a+b}$ и α также сопряжены.

Положим

$$M = \langle \alpha, \beta, \gamma \rangle.$$

В силу п. 5) леммы 2 $\eta_{a,b} = \eta_{a,2a+b} = N_{a,b}N_{a,a+b}/|N_{a,a+b}|$. Пары (a,b) и $(a,a+b)$ экстраспециальные, поэтому знаки у структурных констант $N_{a,b}$ и $N_{a,a+b}$ могут быть выбраны произвольным образом. Пусть $N_{a,b}N_{a,a+b}/|N_{a,a+b}| = -1$. Тогда $\eta_{a,b} = -1$. Отсюда, учитывая также, что $\eta_{a,a+b} = -1$ в силу п. 1) леммы 2, получаем

$$\begin{aligned}\gamma &= (n_a h_a(u))^{x_{a+b}(t)x_b(1)} = x_{a+b}(t)x_b(1)n_a h_a(u)x_b(-1)x_{a+b}(-t) = \\ &= n_a x_{a+b}(\eta_{a,a+b}t)x_{2a+b}(\eta_{a,b})h_a(u)x_b(-1)x_{a+b}(-t) = \\ &= n_a h_a(u)x_{a+b}(-2t)x_{2a+b}(-u^{-2})x_b(-1), \\ \alpha\gamma &= h_a(u)x_{a+b}(-2t)x_{2a+b}(-u^{-2})x_b(-1).\end{aligned}$$

Корневой элемент $x_{a+b}(-2t)$ перестановочен с тремя другими сомножителями элемента $\alpha\gamma$, а два его последних сомножителя перестановочны между собой, но не коммутируют с $h_a(u)$. Поэтому в силу леммы 1

$$(\alpha\gamma)^{(q-1)/2} = x_{a+b}(t).$$

Отсюда

$$\alpha\gamma x_{a+b}(t)^2 = h_a(u)x_{2a+b}(-u^{-2})x_b(-1).$$

Далее,

$$\beta(\alpha\gamma)^{(q-1)/2}\beta = x_{-a-b}(-t).$$

Таким образом, в M лежит подгруппа

$$L = \langle x_{a+b}(t), x_{-a-b}(t) \rangle,$$

которая по лемме 4 совпадает с подгруппой $\langle X_{a+b}, X_{-a-b} \rangle$. (Здесь используется ограничение $q > 9$.) В частности, в M лежат все диагональные элементы $h_{a+b}(v)$, $v \in K^*$. Сейчас при $v \in K^*$ последовательно получаем, что в M лежат элементы

$$\begin{aligned} h_{a+b}(v)(h_a(u)x_{2a+b}(-u^{-2})x_b(-1))h_{a+b}^{-1}(v) &= h_a(u)x_{2a+b}(-u^{-2}v^2)x_b(-v^2), \\ (h_a(u)x_{2a+b}(-u^{-2})x_b(-1))^{-1}h_a(u)x_{2a+b}(-u^{-2}v^2)x_b(-v^2) &= \\ &= x_{2a+b}((1-v^2)u^{-2})x_b(1-v^2). \end{aligned}$$

В силу предположения $N_{a,b}N_{a,a+b}/|N_{a,a+b}| = -1$ и п. 5) леммы 2 получаем

$$\alpha x_{2a+b}((1-v^2)u^{-2})x_b(1-v^2)\alpha = x_{2a+b}(v^2-1)x_b((v^2-1)u^{-2}).$$

Произведение двух последних элементов равно $x_{2a+b}(-k^2)x_b(k^2)$ при $v = u^{-1}$, $k = u^{-2} - 1$. Таким образом, в M лежат элементы

$$\begin{aligned} h_{a+b}^{-1}(k)x_{2a+b}(-k^2)x_b(k^2)h_{a+b}(k) &= x_{2a+b}(-1)x_b(1), \\ (h_a(u)x_{2a+b}(-u^{-2})x_b(-1))x_{2a+b}(-1)x_b(1) &= h_a(u)x_{2a+b}(-u^{-2}-1), \\ [(h_a(u)x_{2a+b}(-u^{-2}-1))^{-1}, h_{a+b}^{-1}(u)] &= x_{2a+b}(1-u^{-4}), \\ \alpha\beta x_{2a+b}(1-u^{-4})\beta\alpha &= x_{-2a-b}(-1+u^{-4}). \end{aligned}$$

Так как $q > 9$, то $1 - u^{-4} \neq 0$. Поэтому в силу леммы 6 подгруппа

$$\langle x_{2a+b}(1-u^{-4}), x_{-2a-b}(1-u^{-4}) \rangle$$

содержит мономиальный элемент $n_{2a+b}(v)$ для некоторого $v \in K^*$. Таким образом,

$$n_a, n_{2a+b}(v), x_{a+b}(t), x_{-a-b}(t) \in M.$$

Следовательно, M имеет нетривиальные пересечения со всеми корневыми подгруппами и по лемме 7 совпадает с $B_2(q)$.

Случай $q=5$. Покажем, что инволюции

$$\begin{aligned} \alpha &= n_a, \\ \beta &= n_{a+b}, \\ \gamma &= h_a(2)x_{-a}(1)x_b(2) \end{aligned}$$

удовлетворяют условиям теоремы. Действительно, перестановочность инволюций α и β и сопряженность инволюций α , β , $\alpha\beta$ установлены выше, а

$$\gamma^{x_{2a+b}(-1)x_{a+b}(-2)x_b(1)x_a(-2)x_{-a}(2)} = \alpha.$$

Последнее и следующее равенства получены при помощи компьютерной системы GAP.

$$x_a(1) = \alpha(\gamma\alpha\beta\gamma\beta)^2\gamma\beta(\alpha(\beta\gamma)^2)^2\alpha(\beta\gamma)^3(\alpha\gamma\beta)^2\gamma\alpha\gamma\beta.$$

Далее,

$$\begin{aligned}(x_a(1))^\alpha &= x_{-a}(-1), \\ h_a(2) &= x_a(1)^2x_{-a}(1)^2x_a(1)^2\alpha, \\ h_a(2)\gamma x_{-a}(-1) &= x_b(2), \\ x_b(2)^{\alpha\beta} &= x_{-b}(2).\end{aligned}$$

Элементы $x_a(1), x_{-a}(1), x_b(2), x_{-b}(2)$ порождают группу $B_2(5)$ по лемме 7.

Случай $q=9$. Покажем, что инволюции

$$\begin{aligned}\alpha &= n_a, \\ \beta &= n_{a+b}, \\ \gamma &= h_{2a+b}(i)h_b(i-1)x_b(i-1)x_{2a+b}(i)x_{a+b}(1) \times \\ &\quad \times x_{-b}(i)x_{-2a-b}(-1)x_{-a-b}(1)x_a(i)x_{-a}(-i)\end{aligned}$$

удовлетворяют условиям теоремы. Действительно, перестановочность инволюций α и β и сопряженность инволюций α , β , $\alpha\beta$ установлены выше, а

$$\gamma^\eta = \beta,$$

где

$$\begin{aligned}\eta &= x_{-b}(1)n_ax_{-a-b}(-1)x_a(-i)x_{-a}(1)x_{-b}(-1) \times \\ &\quad \times x_{a+b}(i)x_b(i)x_{a+b}(-1)x_{-b}(i+1)x_a(-1)x_{2a+b}(-1).\end{aligned}$$

Последнее и следующие три равенства получены при помощи компьютерной системы GAP.

$$\begin{aligned}x_b(1-i) &= \gamma\beta\gamma(\alpha(\gamma\beta)^2)^2(\alpha\gamma)^2\alpha(\beta\gamma)^4\alpha\gamma\beta\gamma, \\ x_b(1+i) &= \gamma\beta\gamma\alpha(\gamma\beta)^7\gamma\alpha\beta\gamma\alpha(\gamma\beta)^6(\alpha\gamma)^2\alpha\beta\gamma\beta(\gamma\beta\gamma\alpha)^2(\gamma\beta)^4\gamma\alpha\beta(\gamma\alpha)^2\gamma\beta(\gamma\alpha)^3, \\ x_{a+b}(i) &= \alpha(\gamma\alpha\gamma\beta)^2\gamma\alpha\beta\gamma\beta\alpha\gamma\beta\gamma\alpha\beta\gamma\beta\alpha\beta\gamma\alpha(\beta\gamma)^4.\end{aligned}$$

Поскольку аддитивная группа поля $GF(9)$ порождается элементами $1-i$ и $1+i$, элементы $x_b(1-i)$ и $x_b(1+i)$ порождают X_b . Последовательно сопрягая X_b элементами α , β , α , получим также подгруппы X_{2a+b} , X_{-b} , X_{-2a-b} . В частности, в подгруппе $M = \langle \alpha, \beta, \gamma \rangle$ лежат элементы n_{2a+b} , n_b , $h_b(-i)$ и

$$x_{a+b}(i)^{h_b(-i)} = x_{a+b}(1).$$

Элементы $x_{a+b}(i)$ и $x_{a+b}(1)$ порождают группу X_{a+b} . Таким образом, в M лежат корневые подгруппы X_b , X_{-b} , $X_{-a} = X_{a+b}^{n_{2a+b}}$, $X_a = X_{a+b}^{n_a n_{2a+b}}$, которые порождают группу $B_2(9)$.

Теорема доказана.

5 Доказательство теоремы 1

Случай $q \neq 2, 3$. Теорема 1 следует из теоремы 2 в силу следующей леммы, доказанной Дж. Уордом [3] при решении задачи А) из введения для спорадических и знакопеременных групп и для $PSL_n(q)$ при определенных ограничениях на n и q , указанных выше.

Лемма 8. *Следующие утверждения эквивалентны.*

1) *Группа G порождается тремя инволюциями α, β, γ , первые две из которых перестановочны (соответственно инволюции $\alpha, \beta, \gamma, \alpha\beta$ сопряжены).*

2) *Группа G порождается инволюциями $\alpha, \beta, \gamma, \delta, \epsilon$, две из которых совпадают, и $\alpha\beta\gamma\delta\epsilon = 1$ (соответственно инволюции $\alpha, \beta, \gamma, \delta, \epsilon$ сопряжены).*

Случай $q = 3$. Частным случаем утверждения следствия на стр. 432 из [11] является

Лемма 9. *Пусть G — конечная неприводимая подгруппа общей линейной группы $GL_n(K)$ над полем K характеристики отличной от 2, χ — след данного представления. Тогда, если $\chi(1) < 5\chi(g)$, то G не порождается пятеркой инволюций из класса сопряженности с представителем g , произведение которых равно 1.*

Группа $B_2(3)$ изоморфна $PSU_4(2^2)$ и имеет два класса сопряженных инволюций $2A$ и $2B$ в соответствии с обозначениями из [17]. Для неё согласно [17] существуют 6-мерное и 15-мерное комплексные неприводимые представления, для которых

$$6 = \chi(1) < 5\chi(2B) = 5 \cdot 2 = 10$$

и соответственно

$$15 = \chi(1) < 5\chi(2A) = 5 \cdot 7 = 35.$$

Поэтому $n_c(B_2(3)) > 5$ по лемме 9. С другой стороны, в силу [10] группа порождается тройкой сопряженных инволюций. Следовательно, $n_c(B_2(3)) = 6$.

Случай $q = 2$. Сейчас нам нужно доказывать непорождаемость группы $B_2(2)$ любыми $k < 10$ сопряженными инволюциями, произведение которых равно единице. Для этого оказывается полезным следующий результат "о непорождаемости" транзитивных групп подстановок, полученный Р. Ри в [18]. (Другое доказательство этого результата приводят У. Фейт, Р. Линдон и Л. Скотт в статье [19].)

Лемма 10. *Пусть подстановки $x_1, \dots, x_m$ порождают транзитивную подгруппу симметрической группы S_n на n символах, с условием*

$x_1 x_2 \cdots x_m = 1$, и пусть c_i — число орбит группы $\langle x_i \rangle$, $1 \leq i \leq m$. Тогда

$$c_1 + c_2 + \cdots + c_m \leq n(m-2) + 2.$$

Группа $B_2(2)$ изоморфна симметрической группе S_6 . (Доказательство этого утверждения можно найти в монографии Р. Стейнберга [20, стр. 80].) В группе S_6 три класса сопряженных инволюций C_1, C_2, C_3 с представителями $\sigma_1 = (12)$, $\sigma_2 = (12)(34)(56)$, $\sigma_3 = (12)(34)$ соответственно. Очевидно, что класс четных подстановок с представителем σ_3 не порождает всю группу S_6 . Рассмотрим класс с представителем σ_1 . Любой его элемент имеет 5 орбит. По лемме 10 группа, порожденная $m \leq 9$ инволюциями из этого класса, произведение которых равно единице, не является транзитивной, следовательно, не может совпадать с S_6 . Неравенство в утверждении леммы 10 выполняется, начиная с $m = 10$, причём, инволюции $x_1 = (12)$, $x_2 = (23)$, $x_3 = (34)$, $x_4 = (45)$, $x_5 = (56)$, $x_6 = x_5$, $x_7 = x_4$, $x_8 = x_3$, $x_9 = x_2$, $x_{10} = x_1$ порождают группу S_6 , а их произведение равно единице. Известно также, что группа S_6 обладает внешним автоморфизмом, который переставляет классы сопряженности C_1 и C_2 . (Построение этого автоморфизма на языке групп подстановок указано в заметке В. Миллера [21], а с учетом отмеченного выше изоморфизма между группами $B_2(2)$ и S_6 можно интерпретировать данный внешний автоморфизм как графовый автоморфизм группы $B_2(2)$ [20, стр. 80].) Поэтому минимальное число порождающих инволюций из класса C_2 , произведение которых равно единице, тоже равно 10. Следовательно, $n_c(B_2(2)) = 10$.

Теорема доказана.

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

References

- [1] G. Malle, J. Saxl, T. Weigel, *Generation of classical groups*, Geom. Dedicata, **49**:1 (1994), 85–116. Zbl 0832.20029
- [2] V.D. Mazurov (ed.), E.I. Khukhro (ed.), *The Kourovka notebook: Unsolved Problems in Group Theory*, **19**, Sobolev Institute of Mathematics, Novosibirsk, 2018. MR3981599
- [3] <http://www.maths.qmul.ac.uk/~raw/JWardPhD.pdf> J.M. Ward, *Generation of simple groups by conjugate involutions*, Thesis PHD, Queen Mary college, University of London, 2009.
- [4] I.Yu. Efimov, Ya.N. Nuzhin, *Generating sets of conjugate involutions of the groups $SL_n(q)$ for $n = 4, 5, 7, 8$ and odd q* , Tr. Inst. Mat. Mekh., **27**:1 (2021), 62–69. MR4245776
- [5] R.I. Gvozdev, *Generating sets of conjugate involutions of groups $PSL_n(9)$* , Algebra Logic, **62**:4 (2023), 319–338. Zbl 1550.20017
- [6] R.I. Gvozdev, Ya.N. Nuzhin, *The minimal number of generating involutions, whose product is 1 for the groups $PSL_3(2^m)$ and $PSU_3(q^2)$* , Sib. Math. J., **64**:6 (2023), 1297–1306. Zbl 1530.20054

- [7] Ya.N. Nuzhin, *Generating triples of involutions of groups of Lie type of rank 2 over finite fields*, Algebra Logic, **58**:1 (2019), 59–76. Zbl 1468.20030
- [8] M.A. Vsemirnov, R.I. Gvozdev, Ya.N. Nuzhin, *The minimal number of generating involutions, the product of which is equal to 1, of finite simple non-Abelian groups*, International Conf. "Mal'tsev Meeting November 13–17, 2023, Abstracts, Institute of Mathematics, S.L. Sobolev RAS, Novosibirsk, 2023, 148.
- [9] Ya.N. Nuzhin, *Generating triples of involutions of groups of Lie type over a finite field of odd characteristic. II*, Algebra Logic, **36**:4 (1997), 422–440. Zbl 0936.20008
- [10] M.A. Vsemirnov, Ya.N. Nuzhin, *Generating triples of conjugate involutions for finite simple groups*, Algebra Logic, **62**:5 (2023), 379–397. Zbl 1552.20050
- [11] Ya.N. Nuzhin, *Generating sets of involutions of finite simple groups*, Algebra Logic, **58**:3 (2019), 288–293. Zbl 1485.20040
- [12] R.W. Carter, *Simple groups of Lie type*, Wiley & Sons, London etc., 1972. Zbl 0248.20015
- [13] L.E. Dickson, *Linear groups with an exposition of the Galois fields theory*, Teubner, Leipzig, 1901. JFM 32.0128.01
- [14] D. Gorenstein, *Finite groups*, Harper & Row, New York etc., 1968. Zbl 0185.05701
- [15] V.M. Levchuk, *Remark on L. Dickson's theorem*, Algebra Logic, **22** (1983), 306–316. Zbl 0542.20027
- [16] Ya.N. Nuzhin, *Generating sets of elements of Chevalley groups over a finite field*, Algebra Logic, **28**:6 (1989), 438–449. Zbl 0721.20034
- [17] J.H. Conway, et al., *Atlas of finite groups*, Clarendon Press, Oxford, 1985. Zbl 0568.20001
- [18] R. Ree, *A theorem on permutations*, J. Comb. Theory, Ser. A, **10** (1971), 174–175. Zbl 0221.05033
- [19] W. Feit, R.S. Lyndon, L.L. Scott, *A remark about permutations*, J. Comb. Theory, Ser. A, **18** (1975), 234–235. Zbl 0297.05021
- [20] R. Steinberg, *Lectures on Chevalley groups*, Yale University, New Haven, 1968. Zbl 1196.22001
- [21] D.W. Miller, *On a theorem of Hölder*, Am. Math. Mon., **65**:4 (1958), 252–254. Zbl 0083.01904

RODION IGOREVICH GVOZDEV
 SIBERIAN FEDERAL UNIVERSITY,
 PR. SVOBODNY, 79,
 660041, KRASNOYARSK, RUSSIA
Email address: gvozdev.rodion@bk.ru

YAKOV NIFANTEVICH NUZHIN
 SIBERIAN FEDERAL UNIVERSITY,
 PR. SVOBODNY, 79,
 660041, KRASNOYARSK, RUSSIA
Email address: nuzhin2008@rambler.ru

TATYANA SERGEYEVNA PETRUT
 SIBERIAN FEDERAL UNIVERSITY,
 PR. SVOBODNY, 79,
 660041, KRASNOYARSK, RUSSIA
Email address: petryt88@gmail.com

ANNA MAKSIMOVNA SOKOLOVSKAYA
 SIBERIAN FEDERAL UNIVERSITY,
 PR. SVOBODNY, 79,
 660041, KRASNOYARSK, RUSSIA
Email address: sokolovskaya-anna-24@mail.ru