УДК 512.542

Строгая вещественность конечных простых групп *

Е. П. Вдовин, А. А. Гальт

Аннотация

В настоящей работе завершается классификация конечных простых строго вещественных групп. Как несложно понять, для каждой конечной простой группы свойство строгой вещественности эквивалентно тому, что каждый элемент представим в виде произведения двух инволюций. Таким образом, как следствие из классификации конечных простых строго вещественных групп получено вопроса 14.82 из «Коуровской тетради».

Введение

В настоящей работе получено решение вопроса 14.82 из «Коуровской тетради» [1].

Проблема 1 (1, 14.82)**.** Описать конечные простые группы, в которых каждый элемент является произведением двух инволюций.

Поскольку в любой неабелевой конечной простой группе любая инволюция вкладывается в элементарную абелеву группу порядка 4, т.е. для любой инволюции t существует перестановочная с ней инволюция $s \neq t$, проблема 14.82 эквивалентна проблеме классификации строго вещественных конечных простых групп. Напомним, что элемент x группы G называется *вещественным* (соответственно, *строго вещественным*), если элементы x и x^{-1} сопряжены в группе G (соответственно, сопряжены инволюцией в группе G). Группа G называется *вещественной* (соответственно, *строго вещественной*), если все элементы группы G являются вещественными (соответственно, строго вещественными). Таким образом, если элемент x имеет порядок отличный от 1 и 2, то x представим в виде произведения двух инволюций s, t в том и только в том случае, если x является строго вещественным. Действительно, если t — инволюция, инвертирующая элемент x, и $|x| > 2$, то элементы t, tx являются инволюциями и $x = t \cdot tx$. Обратно, если существуют инволюции s, t, для которых справедливо равенство $x = st$, то $x^t = ts = x^{-1}$, т.е. x является строго вещественным.

*Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (коды проектов 08–01–00322, 10–01–00391 и 10-01-90007), АВЦП Рособразования «Развитие научного потенциала высшей школы» (проект 2.1.1.419), ФЦП "Научные и научно-педагогические кадры инновационной России" на 2009-2013 гг. (гос. контракт No. 02.740.11.5191), Совета по грантам Президента РФ для поддержки ведущих научных школ(проект НШ-3669.2010.1). Первый автор поддержан также премией фонда Бальзана, присужденной Пьеру Делиню в 2004 году и Лаврентьевским грантом СО РАН для коллективов молодых учёных, постановление Президиума СО РАН N 43 от 04.02.2010.

В конечных простых группах представимость элементов порядка 1 и 2 в виде произведения двух инволюций следует из теоремы Фейта-Томпсона о разрешимости конечных групп нечетного порядка и замечания, сделанного выше.

Проблема вещественности и строгой вещественности конечных простых групп и конечных групп в том или ином смысле близких к простым изучалась различными авторами, см. [2–13]. В частности, в [2] получена классификация конечных простых вещественных групп. Таким образом, для решения вопроса 14.82 достаточно выяснить какие из конечных простых вещественных групп являются строго вещественными. Вопрос о строгой вещественности знакопеременных и спорадических групп решен в [3] и [4] соответственно. В [5–7] доказано, что симплектические группы $\mathrm{PSp}_{2n}(q)$ являются строго вещественными тогда и только тогда, когда $q \not\equiv 3 \pmod 4$. В [8] доказана строгая вещественность групп $\Omega^{\varepsilon}_{4n}(q)$ при четном q. Строгая вещественность групп $\mathrm{P}\Omega^{-}_{4n}(q)$ в случае нечетного q доказана в [9]. Более того, если q нечетно, то [10, Теорема 8.5] влечет, что наряду с группами $\mathrm{P}\Omega^{-}_{4n}(q)$ строго вещественными являются группы $\mathrm{P}\Omega^{+}_{4n}(q)$ и $\Omega_{2n+1}(q)$ при $q \equiv 1 \pmod 4$, а также группы $\Omega_9(q)$ при $q \equiv 3 \pmod 4$ и $\mathrm{P}\Omega^{+}_{8}(q)$ при любом q. В настоящей работе доказана

Теорема 1. (Основная теорема) *Группа $G = {}^3D_4(q)$ является строго вещественной.*

В качестве следствия данной теоремы и работ [2–10] справедливы следующие теоремы.

Теорема 2. *Любая конечная простая вещественная группа является строго вещественной.*

Теорема 3. *В конечной простой группе G любой элемент представим в виде произведения двух инволюций в том и только в том случае, если G изоморфна одной из следующих групп:*

(1) $\mathrm{PSp}_{2n}(q)$ *при* $q \not\equiv 3 \pmod 4$, $n \geqslant 1$;

(2) $\Omega_{2n+1}(q)$ *при* $q \equiv 1 \pmod 4$, $n \geqslant 3$;

(3) $\Omega_9(q)$ *при* $q \equiv 3 \pmod 4$;

(4) $\mathrm{P}\Omega^{-}_{4n}(q)$ *при* $n \geqslant 2$;

(5) $\mathrm{P}\Omega^{+}_{4n}(q)$ *при* $q \not\equiv 3 \pmod 4$, $n \geqslant 3$;

(6) $\mathrm{P}\Omega^{+}_{8}(q)$;

(7) ${}^3D_4(q)$;

(8) A_{10}, A_{14}, J_1, J_2.

Теорема 3 дает исчерпывающее решение вопроса 14.82 из «Коуровской тетради».

1 Предварительные результаты

Наши обозначения для конечных групп согласуются с [14]. Обозначения и основные результаты для конечных групп лиева типа и для линейных алгебраических групп можно найти в [15]. Будем говорить, что группа G является центральным произведением подгрупп A и B (обозначается $A \circ B$), если $G = AB$ и взаимный коммутант $[A, B]$ тривиален.

Через $|G|$ и $|g|$ обозначены порядок группы G и элемента $g \in G$ соответственно. Если X — подмножество и H — подгруппа группы G, то через $C_G(X)$ и $N_G(H)$ обозначены централизатор подмножества X и нормализатор подгруппы H в группе G. Для любого подмножества X группы G символом $\langle X\rangle$ обозначена подгруппа, порожденная множеством X. Символом $\mathbb{F}_q$ обозначено конечное поле порядка q, а p всегда обозначает его характеристику, т.е. $q = p^\alpha$ для подходящего натурального α. Единичный элемент группы обозначается символом e, а 1 обозначает единицу поля.

Пусть $\overline{G}$ — простая связная алгебраическая группа над алгебраическим замыканием $\overline{\mathbb{F}}_p$ конечного поля $\mathbb{F}_p$. Сюръективный эндоморфизм σ группы $\overline{G}$ называется *эндоморфизмом Стейнберга* (см. [15, определение 1.15.1]), если множество его неподвижных точек $\overline{G}_\sigma$ конечно. Хорошо известно, что группа $O^{p'}(\overline{G}_\sigma)$ является конечной группой лиева типа и любая конечная группа лиева типа может быть получена таким образом (отметим, что для конечной группы лиева типа соответствующая алгебраическая группа и эндоморфизм Стейнберга, вообще говоря, могут быть выбраны неединственным способом). Более подробно эти и другие определения и результаты можно найти в [15, разделы 1.5 и 2.2]. Если группа $\overline{G}$ односвязна, то в силу [15, теорема 2.2.6(f)] справедливо равенство $\overline{G}_\sigma = O^{p'}(\overline{G}_\sigma)$. Более того, [15, предложение 2.10] влечет, что в этом случае централизатор любого полупростого элемента связен и является редуктивной подгруппой максимального ранга группы $\overline{G}$.

Если группа G изоморфна ${}^3D_4(q)$, то соответствующая алгебраическая группа $\overline{G}$ может быть выбрана односвязной и мы всегда будем предполагать, что группа $\overline{G}$ односвязна в этом случае, т.е. мы считаем, что для любой группы $G = {}^3D_4(q)$ выбраны односвязная связная простая линейная алгебраическая группа $\overline{G} = D_4(\overline{\mathbb{F}}_q)$, где $\overline{\mathbb{F}}_q$ — алгебраическое замыкание поля $\mathbb{F}_q$, и эндоморфизм Стейнберга σ так, чтобы выполнялось равенство $G = \overline{G}_\sigma$. В частности, централизатор любого полупростого элемента из $\overline{G}$ связен. Если $\overline{T}$ — σ-инвариантный максимальный тор группы $\overline{G}$, то $T = \overline{T} \cap G$ называется *максимальным тором* группы лиева типа G. Если $\overline{R} \leq \overline{S}$ — σ-инвариантные подгруппы группы $\overline{G}$, $R = \overline{R} \cap G$ и $S = \overline{S} \cap G$, то группа $N_{\overline{S}}(\overline{R}) \cap G$ обозначается через $N(S, R)$. Отметим, что справедливо включение $N(S, R) \leq N_S(R)$, но равенство, вообще говоря, может нарушаться. Для любого элемента $x \in G$ существуют единственные элементы $s, u \in G$ такие, что $x = su = us$, s полупрост и u унипотентен. При этом s — это p'-часть элемента x, а u — это p-часть элемента x. Это разложение называется *разложением Жордана.*

В силу [9, лемма 10] все полупростые элементы группы ${}^3D_4(q)$ являются строго вещественными. Более того, сопрягающая инволюция, построенная в доказательстве [9, лемма 10], обладает следующим свойством.

Лемма 1. *Для любого максимального тора T группы ${}^3D_4(q)$ существует инволюция $x \in N(G, T)$ такая, что $t^x = t^{-1}$ для любого $t \in T$. В частности, для любого $t \in T$ элементы xt и tx являются инволюциями и инвертируют любой элемент из T.*

Утверждения, собранные в следующей лемме, известны и легко следуют из хорошо известного строения проективных линейных групп степени 2.

Лемма 2. *Справедливы следующие утверждения.*

(1) *Группа $\mathrm{PSL}_2(q)$ является строго вещественной тогда и только тогда, когда $q \not\equiv 3 \pmod 4$.*

(2) *Группа $\mathrm{PGL}_2(q)$ является строго вещественной.*

(3) *Если q нечетно, u — неединичный унипотентный элемент из* $\mathrm{PGL}_2(q)$ *и элемент* $t \in \mathrm{PGL}_2(q)$ *выбран так, что справедливо равенство* $u^t = u^k$ *для некоторого* $k \in \mathbb{N}$, *то t лежит в подгруппе Картана (являющейся циклической группой порядка* $q-1$*) группы* $\mathrm{PGL}_2(q)$, *нормализующей единственную максимальную унипотентную подгруппу, содержащую элемент u, группы* $\mathrm{PGL}_2(q)$.

2 Доказательство основной теоремы

Пусть $G = {}^3D_4(q)$ и $g \in G$. Если g полупрост, то его строгая вещественность следует из [9, лемма 10]. Если элемент g унипотентен и q четно, то строгая вещественность элемента g следует из [12, теорема 1]. Предположим, что элемент g унипотентен, число q нечетно, и $C_G(g)$ не содержит неединичных полупростых элементов, т.е. $C_G(g)$ является p-группой. В силу [2, лемма 5.9] существует элемент $x \in G$, такой что $g^x = g^{-1}$. Очевидно, можно считать, что $|x| = 2^k$ для некоторого $k \in \mathbb{N}$. Тогда $x^2 \in C_G(g)$ и $|x^2|$ является степенью 2. Значит, элемент x^2 полупрост, откуда $x^2 = e$. Если элемент g унипотентен, число q нечетно, и $C_G(g)$ содержит неединичный полупростой элемент s, то можно рассмотреть элемент $g_1 = sg$. Для элемента g_1 разложение sg является разложением Жордана. Если мы покажем, что существует инволюция x, инвертирующая элемент g_1, то в силу единственности разложения Жордана справедливы равенства $s^x = s^{-1}$ и $g^x = g^{-1}$. Таким образом, можно считать, что элемент g имеет «смешанный порядок», т.е. в разложении Жордана $g = su$ элементы s и u оба неединичны.

Пусть $C = C_G(s)$, тогда $u \in C$. Более того, $\overline{C} = C_{\overline{G}}(s)$ — связная редуктивная подгруппа максимального ранга группы $\overline{G}$ и $C = \overline{C}_\sigma$. Ясно, что любой максимальный тор T группы G, содержащий s, содержится в C. Строение централизаторов полупростых элементов описано в [17, предложение 2.2]. Основным техническим инструментом в дальнейших рассуждениях являются [17, таблицы 2.2a и 2.2b], в которых приведено строение централизаторов неединичных полупростых элементов, что порядок централизаторов делится на p. Если q четно, то с точностью до сопряжения в G существует 8 централизаторов, порядок которых делится на p, неединичных полупростых элементов. Если q нечетно, то существует 9 таких централизаторов. Рассмотрим каждый из этих централизаторов отдельно. Отметим, что $\overline{C} = \overline{M} \circ \overline{S}$, где $\overline{M} = [\overline{C}, \overline{C}]$ связна и полупроста, а $\overline{S} = Z(\overline{C})^0$ — тор. При этом C содержит нормальную подгруппу $M \circ S$, где $S = \overline{S}_\sigma \leq Z(C)$, а $M = \overline{M}_\sigma = O^{p'}(C)$, и в [17, таблицы 2.2a и 2.2b] приведено строение подгрупп M ($= M_\sigma$ в обозначениях из [17] и S ($= S_\sigma$ в обозначениях из [17]), а также указаны строение или порядок факторгруппы $C/(M \circ S)$. Далее индексы в обозначениях элементов у нас будут выбраны также, как в [17, таблицы 2.2a и 2.2b]. Кроме того, подгруппы и факторгруппы группы C естественным образом изоморфны некоторым классическим группам и мы будем отождествлять подгруппы и факторгруппы группы C с соответствующими классическими группами.

Предположим, что элемент s таков, что его централизатор сопряжен с централизатором элемента s_2 (в этом случае s — это инволюция и такой случай возможен лишь для нечетного q). Тогда $M \simeq \mathrm{SL}_2(q^3) \circ \mathrm{SL}_2(q)$, $|Z(M)| = 2$ и $S = \{e\}$. Более того, $|C : M| = 2$ и в силу [18, теорема 2]VdoGalt справедливы изоморфизмы $C/\mathrm{SL}_2(q) \simeq \mathrm{PGL}_2(q^3)$ и $C/\mathrm{SL}_2(q^3) \simeq \mathrm{PGL}_2(q)$. Запишем u в виде $u_1 \cdot u_2$, где $u_1 \in \mathrm{SL}_2(q^3)$, $u_2 \in \mathrm{SL}_2(q)$, и пусть v_1, v_2 — образы элементов u_1, u_2 в группах $C/\mathrm{SL}_2(q)$ и $C/\mathrm{SL}_2(q^3)$ соответственно. Предположим сначала, что $q \equiv 1 \pmod 4$. Тогда группы $\mathrm{PSL}_2(q)$ и $\mathrm{PSL}_2(q^3)$ являются строго вещественными. Следовательно, найдутся инволюции $t_1 \in \mathrm{PSL}_2(q^3)$, $t_2 \in \mathrm{PSL}_2(q)$, такие что $v_1^{t_1} = v_1^{-1}$ и $v_2^{t_2} = v_2^{-1}$. Пусть z_1, z_2 — прообразы элементов t_1, t_2 в $\mathrm{SL}_2(q^3)$ и $\mathrm{SL}_2(q)$ соответственно. Тогда $|z_1| = 4 = |z_2|$ и $z_1^2 \in Z(\mathrm{SL}_2(q^3))$, $z_2^2 \in Z(\mathrm{SL}_2(q))$. Следовательно, $z_1^2 = z_2^2$ в группе M, откуда $(z_1z_2)^2 = e$. Таким образом, z_1z_2 — инвертирующая инволюция для элемента u. Предположим теперь, что $q \equiv 3 \pmod 4$. В этом случае существуют такие инволюции $t_1 \in \mathrm{PGL}_2(q^3) \setminus \mathrm{PSL}_2(q^3)$, $t_2 \in \mathrm{PGL}_2(q) \setminus \mathrm{PSL}_2(q)$, что $v_1^{t_1} = v_1^{-1}$ и $v_2^{t_2} = v_2^{-1}$. Кроме того, t_1 лежит в подгруппе Картана группы $\mathrm{PGL}_2(q^3)$, т.е. в максимальном торе группы $\mathrm{PGL}_2(q^3)$ порядка q^3-1, а t_2 — в подгруппе Картана группы $\mathrm{PGL}_2(q)$, т.е. в максимальном торе группы $\mathrm{PGL}_2(q)$ порядка $q-1$. Пусть T — максимальный тор группы C, образы которого относительно естественных гомоморфизмов $C \to C/\mathrm{SL}_2(q)$ и $C/\mathrm{SL}_2(q^3)$ содержат элементы t_1 и t_2 соответственно. Тогда $|T| = (q^3-1)(q-1)$ и в силу [17, таблица 1.1], мы имеем $T \simeq \mathbb{Z}_{q^3-1} \times \mathbb{Z}_{q-1}$. В частности, T не содержит элементов порядка 4. Пусть z — прообраз для t_1 в T. Можно считать, что z является 2-элементом, следовательно, $z^2 = e$. Кроме того, поскольку t_1 не лежит в $\mathrm{PSL}_2(q^3)$, мы получаем, что z не лежит в M. Рассмотрим естественный гомоморфизм $\widetilde{\ } : C \to C/\mathrm{SL}_2(q^3)$. Поскольку $z \notin M$, получаем $\tilde{z} \notin \mathrm{PSL}_2(q)$, значит $t_2\,\mathrm{PSL}_2(q) = \tilde{z}\,\mathrm{PSL}_2(q)$. Кроме того, $t_2, \tilde{z} \in \widetilde{T} \simeq \mathbb{Z}_{q-1}$, следовательно, $t_2 = \tilde{z}$. Таким образом, z является прообразом и для t_2. Следовательно, z является инвертирующей инволюцией для элемента u.

Предположим, что элемент s таков, что его централизатор либо сопряжен с централизатором элемента s_5, либо сопряжен с централизатором элемента s_{10}. Тогда $|C : (M \circ S)| = (2, q-1)$, $M \simeq \mathrm{SL}_2(q)$, $S \simeq \mathbb{Z}_{q^3-\varepsilon}$, где $\varepsilon = 1$, если $C_G(s)$ сопряжен с $C_G(s_5)$, и $\varepsilon = -1$, если $C_G(s)$ сопряжен с $C_G(s_{10})$. Более того, $C/S \simeq \mathrm{PGL}_2(q)$. Выберем максимальный тор T в C таким образом, чтобы подгруппа $T \cap M$ была подгруппой Картана группы M. Поскольку $M \simeq \mathrm{SL}_2(q)$, мы будем записывать элементы из M матрицами из $\mathrm{SL}_2(q)$, полагая при этом, что $T \cap M$ — группа диагональных матриц. По лемме 1 найдется инволюция $x \in N(G,T)$, инвертирующая любой элемент $t \in T$. В частности, x инвертирует элемент s, следовательно, нормализует $C_{\overline{G}}(s)$, т.е. $x \in N(G,C)$. Значит, x нормализует $\overline{S}$, а значит и S. Пусть $C_0 = \langle C, x\rangle$ и $\widetilde{\ } : C_0 \to C_0/S$ — естественный гомоморфизм. Так как $M = O^{p'}(C)$ является характеристической подгруппой в C, элемент x индуцирует автоморфизм порядка 2 на M. В силу [19, лемма 2.3], группа $N(G,C)$ не индуцирует полевых автоморфизмов на M. Кроме того, $x \notin \widehat{M}$, где $\widehat{M}$ — группа внутреннедиагональных автоморфизмов группы M, поскольку $C/S \simeq \mathrm{PGL}_2(q) \simeq \widehat{M}$. Поэтому $C_0/S = \widetilde{C}_0 \simeq \mathrm{PGL}_2(q) \times \mathbb{Z}_2$. Далее элементы из $\widetilde{C}$ мы будем записывать проективными образами матриц из $GL_2(q)$. С точностью до сопряжения в $\widetilde{C}_0$ можно считать, что

$$\tilde{u} = \begin{bmatrix} 1 & \alpha \\ 0 & 1 \end{bmatrix}$$

для некоторого $\alpha \in \mathbb{F}_q$. Пусть $\overline{T} \in \overline{G}$ таков, что $T = \overline{T}_\sigma$. Элемент x нормализует $\overline{T}$, следовательно, действуя сопряжением, x оставляет инвариантным множество максимальных унипотентных подгрупп группы $\overline{M}$, нормализуемых тором $\overline{T} \cap \overline{M}$. Кроме того, поскольку x неподвижен относительно σ, элемент x нормализует подгруппы σ-неподвижных точек этих унипотентных подгрупп. Поскольку $\overline{M} = [\overline{C}, \overline{C}] \simeq \mathrm{SL}_2(\overline{\mathbb{F}_q})$, существуют ровно две максимальные унипотентные подгруппы группы $\overline{M}$, нормализуемые тором $\overline{T}$: одна из них состоит из верхнетреугольных матриц, а другая — из нижнетреугульных. Поэтому элемент x либо оставляет их неподвижными, либо переставляет их. Таким образом, для некоторого $\beta \in \mathbb{F}_q$,

$$\text{либо } \tilde{u}^{\tilde{x}} = \begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}, \text{ либо } \tilde{u}^{\tilde{x}} = \begin{bmatrix} 1 & 0 \\ \beta & 1 \end{bmatrix}.$$

Возвращаясь к элементам u, x в C_0 и пользуясь тем, что p взаимно просто с $|S|$, получаем, что

$$u = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \text{ и либо } u^x = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}, \text{ либо } u^x = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}.$$

Пусть $u^x = \begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix}$, тогда существует $\tilde{t} \in \mathrm{PGL}_2(q) \cap \widetilde{T}$ такой, что

$$\begin{bmatrix} 1 & \beta \\ 0 & 1 \end{bmatrix}^{\tilde{t}} = \begin{bmatrix} 1 & -\alpha \\ 0 & 1 \end{bmatrix}.$$

Следовательно, $u^{xt} = \begin{pmatrix} 1 & -\alpha \\ 0 & 1 \end{pmatrix} = u^{-1}$ и $(xt)^2 = t^x t = t^{-1}t = e$.

Пусть $u^x = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$, тогда существует $\tilde{t} \in \mathrm{PGL}_2(q) \cap \widetilde{T}$ такой, что

$$\begin{bmatrix} 1 & 0 \\ \beta & 1 \end{bmatrix}^{\tilde{t}} = \begin{bmatrix} 1 & 0 \\ \alpha & 1 \end{bmatrix}$$

Следовательно, $u^{xt} = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} = (u)^T$, где ^{T} обозначает транспонирование матриц и $(xt)^2 = t^x t = t^{-1}t = e$. Заменяя x на xt, можно считать, что $u^x = \begin{pmatrix} 1 & 0 \\ \alpha & 1 \end{pmatrix} = u^T$. Поскольку $|x| = 2$, получаем также, что $(u^T)^x = u$. Положим $z = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \in \mathrm{SL}_2(q) \cap N(C_0, T)$, тогда

$$u^{xz} = u^{-1} = u^{zx}.$$

Поскольку $|N(C_0, T)/T| = 4$, группа $N(C_0, T)/T$ является абелевой. Кроме того, элементы x, z лежат в $N(C_0, T)$ и их образы в $N(C_0, T)/T$ являются инволюциями, следовательно $N(C_0, T)/T \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ и x нормализует $z(T \cap M)$, т.е. $z^x = zt$ для некоторого $t \in T \cap M$. Значит, $xzt = zx$. Как отмечалось выше, элементы xz и zx инвертируют u, значит, $t \in Z(M)$. Если q четно, то $Z(M) = \{e\}$, откуда следует, что x централизует $\langle z \rangle$. Поэтому $|xz| = 2$, следовательно, xz — искомая инвертирующая инволюция. Предположим, что q нечетно. Тогда $|z| = 4$, $|Z(M)| = 2$, и для $t \in Z(M) \setminus \{e\}$ справедливо равенство $zt = z^{-1}$. Таким образом, либо $z^x = z$, либо $z^x = z^{-1}$. Покажем, что $z^x = z^{-1}$, откуда $(xz)^2 = z^x z = z^{-1}z = e$ и xz — искомая инволюция. Возьмем максимальный тор Q группы C, содержащий z. Отметим, что $\tilde{x}, \widetilde{Q}$ содержатся в $C_{\widetilde{C}_0}(\tilde{z})$ и $C_{\widetilde{C}_0}(\tilde{z}) \leq N(\widetilde{C}_0, \widetilde{Q})$. Кроме того, $\widetilde{C}_0 = \mathrm{PGL}_2(q) \times \langle \tilde{y} \rangle$ и $\tilde{y} \in N(\widetilde{C}_0, \widetilde{Q})$. Рассмотрим два смежных класса $\tilde{y}\widetilde{Q}$ и $\tilde{x}\widetilde{Q}$. Допустим, что они совпадают, тогда $\tilde{x} \in \tilde{y}\widetilde{Q}$. Так как $\widetilde{Q}$ является циклической группой, в ней содержится единственная инволюция $\tilde{z}$. Следовательно, в смежном классе $\tilde{y}\widetilde{Q}$ содержится две инволюции: $\tilde{y}$, $\tilde{y}\tilde{z}$ и, либо $\tilde{x} = \tilde{y}$, либо $\tilde{x} = \tilde{y}\tilde{z}$. Но первое равенство невозможно так как $\tilde{y}$ централизует $\mathrm{PGL}_2(q)$, если же $\tilde{x} = \tilde{y}\tilde{z}$, то $\tilde{u}^{-1} = \tilde{u}^{\tilde{x}\tilde{z}} = \tilde{u}^{\tilde{y}\tilde{z}^2} = \tilde{u}^{\tilde{z}^2} = \tilde{u}$, что невозможно. Следовательно, $\tilde{y}\widetilde{Q} \neq \tilde{x}\widetilde{Q}$. По лемме 1 существует инволюция $x' \in N(G, Q)$ инвертирующая любой элемент из Q. Но $s \in Q$, следовательно $x' \in C_0$ и $x, x' \in N(G, Q) \cap C_0$. Поскольку $\tilde{y}\widetilde{Q} \neq \tilde{x}\widetilde{Q}$, $N(G, Q)/Q \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$ и $x, x' \notin C$, мы получаем что $\tilde{x}'\widetilde{Q} = \tilde{x}\widetilde{Q}$ и $xQ = x'Q$. Следовательно, элемент x инвертирует любой элемент из Q, в частности, $z^x = z^{-1}$.

Предположим, что элемент s таков, что его централизатор либо сопряжен с централизатором элемента s_3, либо сопряжен с централизатором элемента s_7. Тогда $|C : (M \circ S)| =$

$(2, q-1)$, $M \simeq \mathrm{SL}_2(q^3)$, $S \simeq \mathbb{Z}_{q-\varepsilon}$, где $\varepsilon = 1$, если $C_G(s)$ сопряжен с $C_G(s_3)$, и $\varepsilon = -1$, если $C_G(s)$ сопряжен с $C_G(s_7)$. Более того, $C/S \simeq \mathrm{PGL}_2(q)$. Этот случай разбирается точно также, как только что разобранный выше случай.

Предположим, что $C_G(s)$ сопряжен с $C_G(s_4)$. Тогда $M \simeq \mathrm{SL}_3(q)$, $S \simeq \mathbb{Z}_{q^2+q+1}$. Более того, если 3 делит $(q-1)$, то $|C : M \circ S| = 3$ и $C/S \simeq \mathrm{PGL}_3(q)$, а если 3 не делит $(q-1)$, то $C = M \times S$ и $\mathrm{SL}_3(q) \simeq \mathrm{PGL}_3(q)$. Доказательство в обоих случаях одинаково. Выберем такой максимальный тор T в C, что $T \cap M$ — подгруппа Картана группы M. Мы будем отождествлять элементы из M с матрицами из $\mathrm{SL}_3(q)$ и считать, что при таком отождествлении $T \cap M$ — это подгруппа диагональных матриц. По лемме 1 существует элемент $x \in N(G,T)$ такой, что $x^2 = e$ и $t^x = t^{-1}$ для любого $t \in T$. Рассмотрим группу $C_0 = \langle C, x\rangle$. В силу [19, лемма 2.3], группа $N(G,C)$ не индуцирует полевых автоморфизмов на M. Поскольку x инвертирует любой элемент подгруппы Картана $T \cap M$ группы M, получаем, что x индуцирует графовый автоморфизм на M. Пусть ι — графовый автоморфизм группы $\mathrm{SL}_3(q)$, действующий по правилу $y \mapsto (y^{-1})^T$, где ^{T} обозначает транспонирование матриц. Тогда ι нормализует тор $T \cap M$ и инвертирует любой элемент из $T \cap M$, следовательно, умножая элемент x на подходящий элемент из тора $T \cap M$, можно считать, что x действует на M также, как ι. Элемент u сопряжен со своей жордановой формой в C, поэтому можно считать, что $u = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & \alpha \\ 0 & 0 & 1 \end{pmatrix}$, где $\alpha \in \{0,1\}$. Пусть $u = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$, положим $z = \begin{pmatrix} 0 & 0 & -1 \\ 0 & -1 & 0 \\ -1 & 0 & 0 \end{pmatrix} \in \mathrm{SL}_3(q)$. Имеем

$$u^{xz} = ((u^{-1})^T)^z = \left(\begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}^T\right)^z = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 1 & -1 & 1 \end{pmatrix}^z = \begin{pmatrix} 1 & -1 & 1 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = u^{-1}.$$

Следовательно, xz — искомая инволюция, так как $(xz)^2 = z^x z = (z^{-1})^T z = e$. Пусть $u = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$, положим $z = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & -1 \end{pmatrix} \in \mathrm{SL}_3(q)$. Имеем

$$u^{xz} = ((u^{-1})^T)^z = \left(\begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^T\right)^z = \begin{pmatrix} 1 & 0 & 0 \\ -1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}^z = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = u^{-1}.$$

Следовательно, xz — искомая инволюция, так как $(xz)^2 = z^x z = (z^{-1})^T z = e$.

Предположим, что $C_G(s)$ сопряжен с $C_G(s_9)$. Тогда $M \simeq \mathrm{SU}_3(q)$, $S \simeq \mathbb{Z}_{q^2-q+1}$. Более того, если 3 делит $(q+1)$, то $|C : M \circ S| = 3$ и $C/S \simeq \mathrm{PGU}_3(q)$, а если 3 не делит $(q+1)$, то $C = M \times S$ и $\mathrm{SU}_3(q) \simeq \mathrm{PGU}_3(q)$. Доказательство в обоих случаях одинаково. Выберем такой максимальный тор T в C, что $T \cap M$ — подгруппа Картана группы M. По лемме 1 существует элемент $x \in N(G,T)$ такой, что $x^2 = e$ и $t^x = t^{-1}$ для любого $t \in T$. Вновь [19, лемма 2.3] влечет, что группа $N(G,C)$ не индуцирует полевых автоморфизмов на M. Пусть $A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ и ι — автоморфизм группы $\mathrm{SL}_3(q^2)$, действующий по правилу $y \mapsto A(y^{-1})^T A$, где ^{T} обозначает транспонирование матриц. Обозначим через f автоморфизм группы $\mathrm{SL}_3(q^2)$, возводящий каждый элемент матрицы из $\mathrm{SL}_3(q^2)$ в степень q. Ввиду [20, с. 268-270] можно считать, что $\mathrm{SU}_3(q)$ совпадает с множеством неподвижных точек автоморфизма $\iota \circ f$. Мы будем отождествлять элементы из M с множеством неподвижных точек группы $\mathrm{SL}_3(q^2)$ относительно автоморфизма $\iota \circ f$ и считать, что при таком отождествлении $T \cap M$ — это подгруппа диагональных матриц. Обозначим тем же символом ι ограничение ι на $\mathrm{SU}_3(q)$. Тогда ι нормализует $T \cap M$, поэтому, умножая элемент x на подходящий элемент из тора T, можно считать, что x действует на M также, как ι. С точностью до сопряжения в C любой унипотентный элемент u из M имеет вид $u = \begin{pmatrix} 1 & \alpha & \beta \\ 0 & 1 & \alpha^q \\ 0 & 0 & 1 \end{pmatrix}$, где $\alpha, \beta \in F_{q^2}$ и $\beta + \beta^q = \alpha^{q+1}$. Если $\alpha \neq 0$, то найдется элемент $t \in T$, такой что $u^t = \begin{pmatrix} 1 & 1 & \gamma \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ для некоторого $\gamma \in F_{q^2}$. Поэтому можно считать, что $u = \begin{pmatrix} 1 & 1 & \gamma \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$ и $u^{-1} = \begin{pmatrix} 1 & -1 & \gamma' \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$ для некоторого $\gamma' \in F_{q^2}$. Положим $z = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix} \in \mathrm{SU}_3(q)$, тогда

$$u^{xz} = (A(u^{-1})^T A)^z = \begin{pmatrix} 1 & 1 & \gamma' \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}^z = \begin{pmatrix} 1 & -1 & \gamma' \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix} = u^{-1}.$$

При $\alpha = 0$ равенство $u^{xz} = u^{-1}$ также справедливо. Следовательно, xz — искомая инволюция, так как $(xz)^2 = z^x z = (z^{-1})^T z = e$.

Теорема 1, а значит, и теоремы 2 и 3 доказаны.

Список литературы

[1] *Мазуров В.Д., Хухро Е.И.*, Коуровская тетрадь. Нерешенные вопросы теории групп, издание 17-е, Новосибирск, 2010.

[2] *Tiep P.H., Zalesski A.E.*, Real conjugacy classes in algebraic groups and finite groups of Lie type // J. Group Theory. 2005. V. 8, N 3. P. 291-315.

[3] *Baginski C.*, On sets of elements of the same order in the alternating group A_n // Publ. Math. 1987. V. 34, N 1. P. 13–15. (1987).

[4] *Kolesnikov S.G., Nuzhin Ja.N.*, On strong reality of finite simple groups // Acta Appl. Math. 2005. V. 85, N 1-3. P. 195–203.

[5] *Gow R.*, Commutators in the symplectic group // Arch. Math. (Basel). 1988. V. 50, N 3. P 204–209.

[6] *Gow R.*, Products of two involutions in classical groups of characteristic 2 // J. Algebra. 1981. V. 71, N 2. P. 583–591.

[7] *Ellers E.W., Nolte W.*, Bireflectionality of orthogonal and symplectic groups // Arch. Math. 1982. V. 39, N 1. P. 113–118.

[8] *Rämö J.*, Strongly real elements of orthogonal groups in even characteristic // Принята к печати в J.Group Theory.

[9] *Гальт А.А.*, Строго вещественные элементы в конечных простых ортогональных группах // СМЖ. 2010. Т. 51, №2. С. 241–248.

[10] *Knüppel F., Thomsen G.*, Involutions and commutators in orthogonal groups // J. Austral. Math. Soc. 1998. V. 65, N 1. P. 1-36.

[11] *Tiep P.H., Zalesski A.E.*, Unipotent elements of finite groups of Lie tipe and realization fields of their complex representations // J. Algebra. 2004. V. 271, N 1. P. 327–390.

[12] *Газданова М.А., Нужин Я.Н.*, О строгой вещественности унипотентных подгрупп групп лиева типа над полем характеристики 2 // СМЖ. 2006. Т.47, № 5. С. 1031-1051.

[13] *Wonenburger M.J.*, Transformations which are products of two involutions // J. Math. Mech. 1966. V. 16, N 327-338.

[14] *Conway J.H., Curtis R.T., Norton S.P., Parker R.A., Wilson R.A.*, Atlas of Finite Groups, Clarendon Press, Oxford, 1985.

[15] *Gorenstein D., Lyons R., Solomon R.*, The classification of the finite simple groups. Number 3. Part I. Chapter A. Almost simple K-groups. Mathematical Surveys and Monographs, **40**, № 3, American Mathematical Society, Providence, RI, 1998.

[16] *Humphreys J.E.*, *Conjugacy classes in semisimple algebraic groups*, American Mathematical Society, Providence, Rhode Island, Mathematical Survey and Monographs, **43**, 1995.

[17] *Deriziotis D.I., Michler G.O.*, Character table and blocks of finite simple triality groups ${}^3D_4(q)$ // Transactions of the AMS. 1987. V.1, N 1. P. 39–70.

[18] *Вдовин Е.П., Гальт А.А.*, Нормализаторы подсистемных подгрупп в конечных группах лиева типа // Алгебра и логика. 2008. Т. 47, № 1. С. 3–30.

[19] *Tamburini M.C., Vdovin E.P.*, Carter subgroups of finite groups // J. Algebra. 2002. V. 255, N 1. P. 148–163.

[20] *Carter R.W.*, Simple groups of Lie type. Wiley and sons, 1972.

Адреса авторов:

Вдовин Евгений Петрович
РОССИЯ, 630090, Новосибирск,
пр. акад. Коптюга, 4,
Институт математики СО РАН,
e-mail: vdovin@math.nsc.ru

ГАЛЬТ Алексей Альбертович
РОССИЯ, 630090, Новосибирск,
ул. Пирогова, 2,
Новосибирский госуниверситет,
e-mail: galt84@gmail.com