Алгебра и логика, 58, № 1 (2019), 84—107

DOI: 10.33048/alglog.2019.58.106 УДК 512.54

О ПОРОЖДАЮЩИХ ТРОЙКАХ ИНВОЛЮЦИЙ ГРУПП ЛИЕВА ТИПА РАНГА 2 НАД КОНЕЧНЫМИ ПОЛЯМИ*)

Я. Н. НУЖИН

В работах автора [1–4] даётся ответ для знакопеременных групп и групп лиева типа на следующий вопрос В. Д. Мазурова:

Какие конечные простые неабелевы группы порождаются тремя инволюциями, две из которых перестановочны?

Группы, обладающие таким свойством, будем называть $(2\times 2,2)$-*группами*. Для спорадических групп окончательную точку поставил сам автор вопроса, предложив общий метод решения данной задачи, используя только таблицы характеров и известную информацию о максимальных подгруппах спорадических групп [5]. Из [1–5] следует, что среди конечных простых групп $(2\times 2,2)$-группами не являются только группы, изоморфные одной из групп

$$A_6, A_7, A_8, L_3(q), U_3(q), L_4(2^n), U_4(2^n), S_4(3), M_{11}, M_{22}, M_{23}, McL.$$

Здесь используются обозначения конечных простых групп из [6].

Основанием для этой работы послужило сообщение Г. А. Джонса в конце 2016 г. о том, что к этому списку необходимо добавить две унитарные группы $U_4(3)$ и $U_5(2)$. То, что эти группы не являются $(2\times 2,2)$-группами, впервые установил М. Мачай, исследуя группы автоморфизмов регулярных карт, и независимо проверили М. Зив-Ав и М. Д. Е. Кондёр с

*)Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект № 16-01-00707.

использованием компьютерных систем GAP и MAGMA. В связи с этим сообщением автор проанализировал доказательства из работ [2, 4] для групп $U_4(q)$ и $U_5(q)$, а также для других групп лиева типа ранга 2. Оказалось, что указанные в [2] порождающие тройки инволюций группы $U_5(2^n)$ порождают её только при $n > 1$, а в [4] при нечётном q и $q-1 \neq 0 \,(\mathrm{mod}\, 4)$ один из порождающих элементов группы $U_4(q)$ не является инволюцией. В этой статье для нечётного q и $q-1 \neq 0 \,(\mathrm{mod}\, 4)$ при $q > 3$ указаны новые порождающие инволюции группы $U_4(q)$. Основным результатом является

ТЕОРЕМА 1. *Пусть q — степень простого числа $p > 2$, $q - 1 \neq \neq 0 \,(\mathrm{mod}\, 4)$ и $q \neq 3$. Тогда группы $S_4(q)$, $U_4(q)$ и $U_5(2^n)$, $n > 1$, порождаются тремя инволюциями α, β, γ, первые две из которых перестановочны. Более того, все четыре инволюции α, β, γ и $\alpha\beta$ сопряжены.*

Новизна данного результата заключается в том, что все порождающие инволюции и произведение двух перестановочных инволюций лежат в одном классе сопряжённых элементов. Поэтому теорема 1 представляет интерес в связи со следующей записанной автором в 1999 г. задачей [7, вопр. 14.69в)]:

Для каждой конечной простой неабелевой группы G найти $i(G)$ — минимум числа порождающих сопряжённых инволюций, произведение которых равно 1.

Значительного прогресса в решении этой задачи добился Дж. М. Уорд [8]. Он нашёл числа $i(G)$ для знакопеременных и спорадических групп и для $G = L_n(q)$ при нечётном q, а для $n \geq 4$ — при дополнительном ограничении $q \neq 9$, кроме того, — для $n = 6$ при $q-1 \neq 0 \,(\mathrm{mod}\, 4)$. Из теоремы 1 вытекает

СЛЕДСТВИЕ. *Пусть G — это одна из групп $S_4(q)$, $U_4(q)$ или $U_5(2^n)$. Тогда $i(G) = 5$.*

Отметим, что $(2 \times 2, 2)$-группы нашли применение в доказательстве существования гамильтоновых путей в графах Кэли [9, 10], в построении экспандеров (графов с определёнными топологическими свойствами) [10] и в описание групп автоморфизмов карт — графов с односвязными гранями [11, 12].

§ 1. Обозначения

Всюду далее Φ — приведённая неразложимая система корней, $\Phi(K)$ — присоединённая группа Шевалле типа Φ над полем K. Группа $\Phi(K)$ порождается корневыми подгруппами

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

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, соответствуют [13]. Используем также такие сокращения: $\langle M \rangle$ — подгруппа, порождённая подмножеством M из некоторой группы G,

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

§ 2. Свойства структурных констант $N_{r,s}$ и чисел $\eta_{r,s}$

Далее нам потребуются некоторые свойства структурных констант $N_{r,s}$, $r, s \in \Phi$, и чисел $\eta_{r,s}$, зависящих от $N_{r,s}$.

ЛЕММА 1 [13, с. 55]. *Пусть $r, s, r+s \in \Phi$, и p — максимальное целое неотрицательное число, такое что $s - pr \in \Phi$. Тогда*

$$N_{r,s} = \pm(p+1), \tag{1}$$

$$N_{r,s} = -N_{-r,-s}, \tag{2}$$

$$N_{r,s} = -N_{s,r}. \tag{3}$$

ЛЕММА 2 [13, с. 55]. *Пусть корни* $r_1, r_2, r_3 \in \Phi$, *такие что* $r_1 + r_2 + r_3 = 0$. *Тогда*

$$\frac{N_{r_1,r_2}}{(r_3,r_3)} = \frac{N_{r_2,r_3}}{(r_1,r_1)} = \frac{N_{r_3,r_1}}{(r_2,r_2)}. \tag{4}$$

Числа $\eta_{r,s} = \pm 1$ определяются равенствами

$$n_r x_s(t) n_r^{-1} = x_{w_r(s)}(\eta_{r,s} t), \ r, s \in \Phi. \tag{5}$$

ЛЕММА 3 [13, с. 95]. *Для любых корней* $r, s \in \Phi$ *справедливы равенства*

$$\eta_{r,\pm r} = -1, \tag{6}$$

$$\eta_{r,s} = \eta_{r,-s}, \tag{7}$$

$$\eta_{r,s}\eta_{r,w_r(s)} = (-1)^{A_{rs}}, \tag{8}$$

где $A_{rs} = 2(r,s)/(r,r)$.

На связь между структурными константами $N_{r,s}$ и числами $\eta_{r,s}$ указывает следующая

ЛЕММА 4 [13, с. 95]. *Пусть* r, s — *линейно независимые корни, а* p *и* q — *максимальные целые неотрицательные числа, такие что* $s - pr, s + qr \in \Phi$. *Тогда*

$$\eta_{r,s} = (-1)^p \frac{\varepsilon_0 \varepsilon_1 \dots \varepsilon_{p-1}}{\varepsilon_0 \varepsilon_1 \dots \varepsilon_{q-1}}, \tag{9}$$

где $\varepsilon_i = \pm 1$ *и* $N_{r,(i-p)r+s} = \varepsilon_i (i+1)$.

Используя лемму 4, в некоторых случаях укажем явно зависимость чисел $\eta_{r,s}$ от структурных констант$N_{r,s}$.

ЛЕММА 5. *Пусть* r, s, p *и* q — *такие, как в лемме* 4. *Тогда*

$$\eta_{r,s} = 1 \ \textit{при} \ p = 0 \ \textit{и} \ q = 0, \tag{10}$$

$$\eta_{r,s} = N_{r,s} \ \textit{при} \ p = 0 \ \textit{и} \ q = 1, \tag{11}$$

$$\eta_{r,s} = N_{r,s} N_{r,r+s}/|N_{r,r+s}| \ \textit{при} \ p = 0 \ \textit{и} \ q = 2, \tag{12}$$

$$\eta_{r,s} = -1 \ \textit{при} \ p = 1 \ \textit{и} \ q = 1. \tag{13}$$

ДОКАЗАТЕЛЬСТВО. При $p = q = 0$ числитель и знаменатель дроби из правой части равенства (9) равны 1 по определению. Поэтому $\eta_{r,s} = 1$.

При $p = 0$ и $q = 1$ корни r и s составляют базу системы корней типа A_2. В этом случае числитель дроби из правой части равенства (9) равен 1 по определению, а её знаменатель — структурной константе $N_{r,s}$, которая равна ± 1. Следовательно, $\eta_{r,s} = N_{r,s}$ по лемме 4.

При $p = 0$ и $q = 2$ корни r и s составляют базу системы корней типа B_2, причём r — короткий корень. В этом случае числитель дроби из правой части равенства (9) также равен 1 по определению, а её знаменатель — дроби $N_{r,s}N_{r,r+s}/|N_{r,r+s}|$, которая равна ± 1. Следовательно, справедливо равенство (12).

При $p = 1$ и $q = 1$ корни r и s являются ортогональными короткими корнями системы корней типа B_2. В этом случае числитель и знаменатель дроби из правой части равенства (9) совпадают, и следовательно $\eta_{r,s} = -1$. Лемма доказана.

Знаки у констант $N_{r,s}$ для экстраспециальных пар (r, s) можно выбирать произвольным образом, и они определяют знаки остальных структурных констант [13, предлож. 4.2.2]. По лемме 4 числа $\eta_{r,s}$ однозначно определяются константами $N_{r,s}$ для экстраспециальных пар (r, s). Для системы корней типа B_2 такое явное представление чисел $\eta_{r,s}$ для линейно независимых корней r, s даёт

ЛЕММА 6. *Пусть Φ — система корней типа B_2 с базой $\{a, b\}$, где корень a короткий. Тогда множество экстремальных пар состоит из двух пар (a, b), $(a, a + b)$ и справедливы следующие 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) $\eta_{a+b,b} = \eta_{a+b,2a+b} = -N_{a,b}N_{a,a+b}/|N_{a,a+b}|$.

ДОКАЗАТЕЛЬСТВО. Для любой системы корней число её экстраспециальных пар совпадает с числом положительных нефундаментальных корней. Для системы корней типа B_2 существуют две экстраспециальные пары (a, b) и $(a, a+b)$.

(1) Требуемое следуют из равенства (13).

(2) Пусть r, s — длинные линейно независимые корни. Тогда $p = q = 0$ и в силу равенства (10) получаем $\eta_{r,s} = 1$. Данное утверждение следует также из того, что в это случае корневые подгруппы X_r и X_{-r} централизуют корневую подгруппу X_s.

(3) Во-первых,

$$\eta_{b,a}\eta_{b,a+b} = \eta_{b,a}\eta_{b,w_b(a)} = (-1)^{\frac{2(b,a)}{(b,b)}} = (-1)^{-1} = -1$$

в силу равенства (8). Далее, по лемме 4 и равенству (3) имеем

$$\eta_{b,a} = (-1)^0 \frac{1}{N_{b,a}} = -N_{a,b}.$$

Отсюда следует требуемое.

(4) По лемме 4 имеем

$$\eta_{2a+b,a} = (-1)^1 \frac{N_{2a+b,-a-b}}{1} = -N_{2a+b,-a-b},$$
$$\eta_{2a+b,a+b} = (-1)^1 \frac{N_{2a+b,-a}}{1} = -N_{2a+b,-a}.$$

Выразим $N_{2a+b,-a-b}$ и $N_{2a+b,-a}$ через $N_{a,b}$ и $N_{a,a+b}$. (В действительности, только через $N_{a,a+b}$.) Применяя лемму 2 при $r_1 = 2a+b$, $r_2 = -a-b$, $r_3 = -a$, получаем

$$\frac{N_{2a+b,-a-b}}{(-a,-a)} = \frac{N_{-a-b,-a}}{(2a+b, 2a+b)} = \frac{N_{-a,2a+b}}{(-a-b,-a-b)}.$$

Отсюда $2N_{2a+b,-a-b} = N_{-a-b,-a} = 2N_{-a,2a+b}$. По лемме 1 справедливы равенства $N_{-a-b,-a} = -N_{a+b,a} = N_{a,a+b}$ и $N_{-a,2a+b} = -N_{2a+b,-a}$. Суммируя эти равенства, получаем п. (4). Более того, $N_{2a+b,-a-b} = -N_{-2a-b,a+b} = N_{a+b,-2a-b}$ по лемме 1. Аналогично $N_{-a-b,-a} = -N_{a+b,a} = N_{a,a+b}$. Одновременно мы доказали, что знаки у структурных констант $N_{a+b,-2a-b}$ и $N_{a,a+b}$ совпадают.

(5) В силу равенства (8) имеем

$$\eta_{a,b}\eta_{a,2a+b} = \eta_{a,b}\eta_{a,w_a(b)} = (-1)^{\frac{2(a,b)}{(a,a)}} = (-1)^{-2} = 1.$$

Поэтому $\eta_{a,b} = \eta_{a,2a+b}$. Равенство $\eta_{a,b} = N_{a,b}N_{a,a+b}/|N_{a,a+b}|$ устанавливает лемма 5.

(6) Во-первых,

$$\eta_{a+b,-b}\eta_{a+b,2a+b} = \eta_{a+b,-b}\eta_{a+b,w_{a+b}(-b)} = (-1)^{\frac{2(a+b,-b)}{(a+b,a+b)}} = (-1)^{-2} = 1$$

в силу равенства (8). Во-вторых, $\eta_{a+b,b} = \eta_{a+b,-b}$ в силу равенства (7). Поэтому $\eta_{a+b,b} = \eta_{a+b,2a+b}$. По лемме 4

$$\eta_{a+b,b} = (-1)^2 \frac{N_{a+b,-2a-b}N_{a+b,-a}}{1} = N_{a+b,-2a-b}N_{a+b,-a}.$$

Выразим $N_{a+b,-2a-b}$ и $N_{a+b,-a}$ через $N_{a,b}$ и $N_{a,a+b}$. Применяя лемму 2 при $r_1 = a+b$, $r_2 = -a$, $r_3 = -b$, получаем

$$\frac{N_{a+b,-a}}{(-b,-b)} = \frac{N_{-a,-b}}{(a+b,a+b)} = \frac{N_{-b,a+b}}{(-a,-a)}.$$

Отсюда $N_{a+b,-a} = 2N_{-a,-b} = -2N_{a,b}$. При доказательстве п. (4) было установлено, что знаки у структурных констант $N_{a+b,-2a-b}$ и $N_{a,a+b}$ совпадают. Таким образом, $\eta_{a+b,b} = \eta_{a+b,2a+b} = -N_{a,b}N_{a,a+b}/|N_{a,a+b}|$. Лемма доказана.

Из леммы 6 и равенства (8) вытекает

ЛЕММА 7. *Пусть корни a, b такие же, как в лемме 6. Тогда справедливы следующие равенства*:

(1) $\eta_{a,a}\eta_{a+b,w_a(a)} = \eta_{a,a}\eta_{a+b,-a} = 1$,

(2) $\eta_{a,a+b}\eta_{a+b,w_a(a+b)} = \eta_{a,a+b}\eta_{a+b,a+a} = 1$,

(3) $\eta_{a,b}\eta_{a+b,w_a(b)} = \eta_{a,b}\eta_{a+b,2a+b} = -1$,

(4) $\eta_{a,2a+b}\eta_{a+b,w_a(2a+b)} = \eta_{a,2a+b}\eta_{a+b,b} = -1$,

(5) $\eta_{b,b}\eta_{2a+b,w_b(b)} = \eta_{b,b}\eta_{2a+b,-b} = -1$,

(6) $\eta_{b,2a+b}\eta_{2a+b,w_b(2a+b)} = \eta_{b,2a+b}\eta_{2a+b,2a+b} = -1$,

(7) $\eta_{b,a}\eta_{2a+b,w_b(a)} = \eta_{b,a}\eta_{2a+b,a+b} = -N_{a,b}N_{a,a+b}/|N_{a,a+b}|$,

(8) $\eta_{b,a+b}\eta_{2a+b,w_b(a+b)} = \eta_{b,a+b}\eta_{2a+b,a} = -N_{a,b}N_{a,a+b}/|N_{a,a+b}|$.

§ 3. Свойства мономиальных и диагональных элементов группы Шевалле типа B_2

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

N на группу Вейля W. По [13, теор. 7.2.2] верно

$$n_w h(\chi) n_w^{-1} = h(\chi'), \tag{14}$$

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

$$n_r h_s(t) n_r^{-1} = h_{w_r(s)}(t),\ r, s \in \Phi. \tag{15}$$

Диагональные элементы действуют на корневых элементах следующим образом:

$$h(\chi) x_s(u) h^{-1}(\chi) = x_s(u\chi(s)),\ s \in \Phi, \tag{16}$$

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

$$h_r(t) x_s(u) h_r^{-1}(t) = x_s\left(ut^{\frac{2(r,s)}{(r,r)}}\right),\ r, s \in \Phi. \tag{17}$$

ЛЕММА 8. *Пусть Φ — система корней типа B_2 с базой $\{a, b\}$, где корень a короткий. Тогда для мономиальных элементов*

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

из присоединённой 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 корни 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 $N_{a,b} = -N_{a,a+b}/|N_{a,a+b}|$.*

ДОКАЗАТЕЛЬСТВО. В общем случае, для универсальной или присоединённой группы Шевалле, $n_r^2 = h_r(-1)$ и справедлива формула

$$h_r(-1) x_s(t) h_r(-1) = x_s\left(t(-1)^{\frac{2(r,s)}{(r,r)}}\right),\ r, s \in \Phi.$$

Для системы корней Φ типа B_2

$$\frac{2(r,s)}{(r,r)} = \begin{cases} 0,\ \pm 2, & \text{если корень } r \text{ короткий или оба корня } r, s \text{ длинные}, \\ \pm 1, & \text{если корень } r \text{ длинный, а корень } s \text{ короткий}. \end{cases}$$

Следовательно, диагональные элементы $h_r(-1)$ для коротких корней r лежат в центре универсальной группы Шевалле типа B_2 и равны единице для присоединённой группы Шевалле этого же типа. Таким образом, свойства (1) и (2) справедливы. По этим же соображениям выполняются свойства (3) и (4).

(5) Пусть $N_{a,b} = -N_{a,a+b}/|N_{a,a+b}|$. Применяя формулу (5) и лемму 6, получаем равенства

$$n_a n_{a+b} x_r(t)(n_a n_{a+b})^{-1} = n_b n_{2a+b} x_r(t)(n_b n_{2a+b})^{-1}, \ r \in \Phi^+, \ t \in K. \qquad (18)$$

Действительно, пусть $r = a$. Тогда

$$\begin{aligned} n_a n_{a+b} x_a(t)(n_a n_{a+b})^{-1} &= n_a n_{a+b} x_a(t) n_{a+b} n_a \\ &= n_a x_a(\eta_{a+b,a} t) n_a = x_{-a}(\eta_{a,a}\eta_{a+b,a} t) = x_{-a}(t). \end{aligned}$$

Последнее равенство выполняется в силу леммы 3 и леммы 6(1), по которым $\eta_{a,a} = \eta_{a+b,a} = -1$. С другой стороны,

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

В силу леммы 6(3),(5) имеем $\eta_{b,-a-b} = N_{a,b}$ и соответственно $\eta_{2a+b,a} = -N_{a,a+b}/|N_{a,a+b}|$. Поэтому при $N_{a,b} = -N_{a,a+b}/|N_{a,a+b}|$ равенство (18) для $r = a$ выполняется. Подобным способом равенство (18) устанавливается и для $r = b, a+b, 2a+b$.

Используя свойство $\eta_{r,s} = \eta_{r,-s}$, получаем равенство (18) и для всех отрицательных корней r. Таким образом, элементы $n_a n_{a+b}$ и $n_b n_{2a+b}$ действуют сопряжениями одинаково на порождающих элементах группы $B_2(K)$. Центр группы $B_2(K)$ единичен, поэтому $n_a n_{a+b} = n_b n_{2a+b}$. Лемма доказана.

Следующая лемма справедлива для любой системы корней Φ, где Φ^+ — множество её положительных корней.

ЛЕММА 9. *Пусть χ — K-характер, $r_1, \ldots, r_k \in \Phi^+$, $r_i + r_j \notin \Phi$ 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.*

ДОКАЗАТЕЛЬСТВО. Положим $g = h(\chi)x_{r_1}(t_1)\cdots x_{r_k}(t_k)$. В силу (16) получаем

$$x_{r_1}(t)gx_{r_1}(-t) = h(\chi)x_{r_1}(t_1 - t(1-\chi(r_1)^{-1}))x_{r_2}(t_2)\cdots x_{r_k}(t_k).$$

Полагая $t = t_1/(1-\chi(r_1)^{-1})$, получаем, что g сопряжён с

$$h(\chi)x_{r_2}(t_2)\cdots x_{r_k}(t_k).$$

Индукция по k завершает доказательство леммы.

§ 4. Теорема Диксона и её вариации

Далее $SL_2(p^n)$ — специальная линейная группа степени 2 над полем $GF(p^n)$, где p — простое число. Пусть

$$t_{21}(u) = \begin{pmatrix} 1 & 0 \\ u & 1 \end{pmatrix},\ t_{12}(u) = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}.$$

Утверждение следующей леммы обычно называют теоремой Диксона [14; 15, теор. 2.8.4].

ЛЕММА 10. *Если u — собственный элемент поля $GF(p^n)$ при $p > 2$ и $p^n \neq 9$, то*

$$\langle t_{21}(u),\ t_{12}(1)\rangle = SL_2(p^n).$$

В различных ситуациях (см., напр., [16]) возникала необходимость в следующей вариации теоремы Диксона.

ЛЕММА 11. *Если u, u^2 — собственные элементы поля $GF(p^n)$, $p > 2$ и $p^n \neq 9$, то*

$$\langle t_{21}(u),\ t_{12}(u)\rangle = SL_2(p^n).$$

Лемма 11 вытекает из леммы 10. Действительно, сопрягая трансвекции из леммы 11 диагональной матрицей $\mathrm{diag}(1, u)$, получаем две трансвекции $t_{21}(u^2)$, $t_{12}(1)$, которые в силу леммы 10 порождают всю группу $SL_2(p^n)$.

Частным случаем при $p = 2$ для [17, теор. 1] является следующая

ЛЕММА 12. *Пусть* $V \subseteq GF(2^n)$, $|V| > 2$ *и некоторый собственный элемент* t *поля* $GF(2^n)$ *лежит в* V. *Тогда*

$$\langle t_{21}(V),\ t_{12}(1)\rangle = SL_2(2^n).$$

ЛЕММА 13. *Если* u, v *— ненулевые элементы поля* $GF(p^n)$ *при* $p > 2$, *то подгруппа* $\langle t_{21}(u), t_{12}(v)\rangle$ *содержит диагональную матрицу* $\mathrm{diag}(-1,-1)$.

ДОКАЗАТЕЛЬСТВО. В силу [17, теор. 1] для некоторого ненулевого t подгруппа $\langle t_{21}(u), t_{12}(v)\rangle$ содержит мономиальную матрицу $\begin{pmatrix} 0 & t \\ -t^{-1} & 0 \end{pmatrix}$, квадрат которой равен $\mathrm{diag}(-1,-1)$. Лемма доказана.

ЛЕММА 14. *Пусть* K *— конечное поле нечётного порядка* $q^2 \neq 9$. *Тогда для любого элемента* $t \in K$, *чей мультипликативный порядок равен* $q+1$, *его квадрат* t^2 *является собственным элементом поля* K.

ДОКАЗАТЕЛЬСТВО. Пусть $q = p^n$, где p — простое нечётное число. Предположим противное, т. е. t^2 не является собственным элементом поля K. Тогда $(p^n+1)/2$ делит $p^{2n/r} - 1$ для некоторого простого делителя r числа $2n$. Если $r = 2$, то это возможно только при $q = 9$. Пусть $r > 2$. Тогда $(p^n+1)/2 \leq p^{2n/3} - 1$ и, следовательно, $p^n \leq 2p^{2n/3} - 3 < 2p^{2n/3}$. Отсюда $1 \leq 2/(p^{\frac{n}{3}})$. При $n \geq 3$ или $p \geq 11$ последнее неравенство невозможно и мы приходим к противоречию. В оставшихся шести случаях при $n = 1, 2$ и $p = 3, 5, 7$ непосредственно проверяется, что t^2 тогда и только тогда не является собственным элементом поля K, когда $n = 1$ и $p = 3$. Лемма доказана.

§ 5. Порождающие тройки инволюций группы $B_2(q)$ для нечётного q

Присоединённая группа Шевалле $B_2(q)$ изоморфна проективной симплектической группе $S_4(q)$ размерности 4.

ТЕОРЕМА 2. *Пусть* K *— конечное поле нечётного порядка* q *при* $q - 1 \neq 0 \pmod 4$ *и* $q \neq 3$. *Предположим, что* t *и* t^2 *— собственные эле-*

менты поля K, а мультипликативный порядок элемента $u \in K$ равен $(q-1)/2$. Тогда группа $B_2(q)$ порождается тремя инволюциями α, β, γ, первые две из которых перестановочны, где

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

Более того, все четыре инволюции α, β, γ и $\alpha\beta$ сопряжены.

ДОКАЗАТЕЛЬСТВО. В силу леммы 8(1),(4) мономиальные элементы n_a, n_{a+b} являются перестановочными инволюциями и 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, т. к. порядок элемента u нечётен. Используя равенство $\eta_{a,a+b} = -1$ из леммы 6(1), получаем

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

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

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

По лемме 6, $\eta_{a,b} = \eta_{a,2a+b} = N_{a,b}N_{a,a+b}/|N_{a,a+b}|$. 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 леммы 6(1), получаем

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

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 $h_a(u)$. В силу леммы 8 справедливо

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

Отсюда

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

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 11 совпадает с подгруппой $\langle X_{a+b}, X_{-a-b}\rangle$. 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

$$h_{a+b}(v)(\alpha\gamma)^{(q+1)/2}h_{a+b}^{-1}(v) = h_a(u)x_{2a+b}(-u^{-2}v^2)x_b(-v^2),$$
$$(\alpha\gamma)^{-(q+1)/2}h_{a+b}(v)(\alpha\gamma)^{(q+1)/2}h_{a+b}^{-1}(v) = x_{2a+b}((1-v^2)u^{-2})x_b(1-v^2).$$

В силу предположения $N_{a,b}N_{a,a+b}/|N_{a,a+b}| = -1$ и леммы 6(5) 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 $v = u^{-1}$, $k = u^{-2}-1$. Здесь и далее используется тот факт, что в силу предположения теоремы мультипликативный порядок элемента u^2 равен нечётному числу $(q-1)/2$. В частности, $u^{\pm 2}, u^{\pm 4} \neq \pm 1$. Таким образом, в M лежат элементы

$$h_{a+b}^{-1}(k)x_{2a+b}(-k^2)x_b(k^2)h_{a+b}(k) = x_{2a+b}(-1)x_b(1),$$
$$(\alpha\gamma)^{(q+1)/2}x_{2a+b}(-1)x_b(1) = h_a(u)x_{2a+b}(-u^{-2}-1),$$
$$[(h_a(u)x_{2a+b}(-u^{-2}-1))^{-1}, h_{a+b}^{-1}(u)] = x_{2a+b}(1-u^{-4}),$$
$$\alpha\beta x_{2a+b}(1-u^{-4})\beta\alpha = x_{-2a-b}(-1+u^{-4}).$$

В силу предположения теоремы $(1-u^{-4})$, $(1-u^{-4})^2$ — собственные элементы некоторого подполя F поля K, причём $|F| \neq 9$. По лемме 11

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

В частности, подгруппа M содержит мономиальный элемент n_b. Итак, подгруппа M содержит мономиальные элементы n_a, n_b и корневой элемент $x_{a+b}(t)$. В силу [16, предлож. 3], $M = B_2(q)$. Теорема доказана.

§ 6. Порождающие тройки инволюций группы $^2A_3(q)$ для нечётного q

Пусть $\{e_0, e_1, e_2, e_3\}$ — ортонормированный базис четырёхмерного евклидова пространства. Тогда векторы $r_1 = e_0 - e_1, r_2 = e_1 - e_2, r_3 = e_2 - e_3$ составляют фундаментальную систему системы корней Φ типа A_3, причём $r_1 + r_2, r_2 + r_3 \in \Phi$. Положим $t^q = \bar{t}$. Группа $^2A_3(q^2) \simeq U_4(q)$ порождается своими корневыми элементами

$$\begin{aligned}
x_a(t) &= x_{r_1}(t)x_{r_3}(\bar{t}),\ t \in GF(q^2),\\
x_b(u) &= x_{r_2}(u),\ u \in GF(q),\\
x_{a+b}(t) &= x_{r_1+r_2}(t)x_{r_2+r_3}(\bar{t}),\ t \in GF(q^2),\\
x_{2a+b}(u) &= x_{r_1+r_2+r_3}(u),\ u \in GF(q),\\
x_{-a}(t) &= x_{-r_1}(t)x_{-r_3}(\bar{t}),\ t \in GF(q^2),\\
x_{-b}(u) &= x_{-r_2}(u),\ u \in GF(q),\\
x_{-a-b}(t) &= x_{-r_1-r_2}(t)x_{-r_2-r_3}(\bar{t}),\ t \in GF(q^2),\\
x_{-2a-b}(u) &= x_{-r_1-r_2-r_3}(u),\ u \in GF(q)
\end{aligned}$$

(см. [13, леммы 13.6.2, 13.6.3 и предлож. 13.6.5]). В группе $^2A_3(q^2)$ лежат следующие диагональные элементы:

$$\begin{aligned}
h_a(t) &= h_{r_1}(t)h_{r_3}(\bar{t}),\ t \in GF(q^2)^*,\\
h_b(u) &= h_{r_2}(u),\ u \in GF(q)^*,\\
h_{a+b}(t) &= h_{r_1+r_2}(t)h_{r_2+r_3}(\bar{t}),\ t \in GF(q^2)^*,
\end{aligned}$$

$$h_{2a+b}(u) = h_{r_1+r_2+r_3}(u),\ u \in GF(q)^*.$$

Используя действие сопряжением диагональных элементов в группах Шевалле типа A_3 по формуле

$$h_r(t)x_s(u)h_r^{-1}(t) = x_s(ut^{\frac{2(r,s)}{(r,r)}}),\ r, s \in \Phi, \tag{19}$$

получаем действие сопряжением диагональных элементов в скрученной группе Шевалле ${}^2A_3(q^2)$

$$\begin{aligned} h_a(t)x_{a+b}(v)h_a^{-1}(t) &= h_{r_1}(t)h_{r_3}(\overline{t})x_{r_1+r_2}(v)x_{r_2+r_3}(\overline{v})h_{r_1}^{-1}(t)h_{r_3}^{-1}(\overline{t}) \\ &= x_{r_1+r_2}(vt\overline{t}^{-1})x_{r_2+r_3}(\overline{v}t^{-1}\overline{t}) = x_{a+b}(vt\overline{t}^{-1}) \\ &= x_{a+b}(vt^{1-q}), \\ h_{a+b}(t)x_a(v)h_{a+b}^{-1}(t) &= x_a(vt\overline{t}^{-1}) = x_a(vt^{1-q}), \\ h_a(t)x_{2a+b}(u)h_a^{-1}(t) &= h_{r_1}(t)h_{r_3}(\overline{t})x_{r_1+r_2+r_3}(u)h_{r_1}^{-1}(t)h_{r_3}^{-1}(\overline{t}) \\ &= x_{r_1+r_2+r_3}(ut\overline{t}) = x_{r_1+r_2+r_3}(ut^{1+q}) = x_{2a+b}(ut^{1+q}), \\ h_a(t)x_b(u)h_a^{-1}(t) &= x_b(ut^{-1-q}). \end{aligned}$$

ЗАМЕЧАНИЕ. Пусть i — элемент порядка 4 поля нечётного порядка q^2. Последнее равенство показывает, что элемент $\gamma = n_b h_a(i)$ является инволюцией тогда и только тогда, когда $q - 1 = 0 \,(\mathrm{mod}\, 4)$. Поэтому элемент $\gamma = n_b h_a(i)$ из [4, предлож. 10] не является инволюцией при $q - 1 \neq \neq 0 \,(\mathrm{mod}\, 4)$. В этом случае при $q \neq 3$ теорема 3 даёт новые порождающие тройки инволюций.

Применяя коммутаторную формулу Шевалле, получаем коммутаторные формулы для корневых элементов группы ${}^2A_3(q^2)$, т. е. справедлива

ЛЕММА 15. *В группе ${}^2A_3(q^2)$ справедливы следующие коммутаторные формулы*

$$[x_a(t), x_b(u)] = x_{a+b}(\pm tu)x_{2a+b}(\pm t\overline{t}u), \tag{20}$$

$$[x_a(t), x_{a+b}(v)] = x_{2a+b}(\pm(\overline{t}v + t\overline{v})). \tag{21}$$

В доказательстве теоремы 3 лемма 15 используется без упоминаний. Ясно, что она применяется там, где меняются местами соседние корневые элементы.

ТЕОРЕМА 3. *Пусть K — конечное поле нечётного порядка q^2 при $q-1 \neq 0 \,(\mathrm{mod}\, 4)$ и $q \neq 3$. Пусть мультипликативные порядки элементов t и u из K равны $q+1$ и соответственно $(q-1)/2$. Тогда группа ${}^2A_3(q^2)$ порождается тремя инволюциями α, β, γ, первые две из которых перестановочны, где*

$$\alpha = n_a h_a(t),\ \ \beta = n_a n_{a+b},\ \ \gamma = (n_a h_a(ut))^{x_{a+b}(\bar{t}) x_b(1)}.$$

Более того, все четыре инволюции α, β, γ и $\alpha\beta$ сопряжены.

ДОКАЗАТЕЛЬСТВО. В силу леммы 8(1),(4) мономиальные элементы n_a, n_{a+b} являются перестановочными инволюциями и инвертируют диагональные элементы $h_a(s)$ и $h_{a+b}(s)$ соответственно. Поэтому α, β, γ — инволюции. Равенство $\alpha\beta = \beta\alpha$ следует из соотношения

$$n_{a+b} h_a(t) n_{a+b} = h_a(\bar{t})$$

и того, что $t\bar{t} = 1$.

Покажем, что инволюции α, β, γ и $\alpha\beta$ лежат в одном классе сопряжённых элементов, т. е. каждая из них сопряжена с мономиальным элементом n_a. Действительно, используя равенство $\eta_{a,a+b} = -1$, получаем

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

Уравнение $s^{q-1} = t$ разрешимо в поле K, т. к. $|t| = q+1$. Поэтому при $s^{q-1} = t$

$$\begin{aligned} h_{a+b}^{-1}(s)\alpha h_{a+b}(s) &= h_{a+b}^{-1}(s) x_a(t^{-1}) x_{-a}(-t) x_a(t^{-1}) h_{a+b}(s) \\ &= x_a(s^{q-1}t^{-1}) x_{-a}(-s^{1-q}t) x_a(s^{q-1}t^{-1}) = n_a. \end{aligned}$$

Очевидно, инволюция γ сопряжена с $n_a h_a(ut)$. Далее,

$$h_a(k) n_a h_a(ut) h_a^{-1}(k) = n_a h_a(k^2 ut).$$

По условию теоремы мультипликативный порядок элемента u нечётен. Поэтому в поле K уравнение $k^2 = u^{-1}$ разрешимо. Отсюда инволюция γ сопряжена с α. Снова из разрешимости уравнения $s^{q-1} = t$ в поле K при $s^{q-1} = t$ получаем

$$h_a^{-1}(s)\alpha\beta h_a(s) = h_a(s^{q-1})h_a^{-1}(t)n_{a+b} = n_{a+b}.$$

Равенство $n_b n_{a+b} n_b^{-1} = n_a$ завершает доказательство сопряжённости четвёрки инволюций α, β, γ и $\alpha\beta$.

Покажем, что инволюции α, β, γ порождают группу ${}^2A_3(q^2)$. Пусть

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

Подгруппа группы ${}^2A_3(q^2)$, порождённая корневыми элементами, коэффициенты которых лежат в подполе $GF(q)$, изоморфна группе $B_2(q)$. Поэтому здесь мы можем также использовать леммы 6–8. По лемме 6, $\eta_{a,b} = \eta_{a,2a+b} = N_{a,b}N_{a,a+b}/|N_{a,a+b}|$. 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 леммы 6(1), получаем

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

Так как $\overline{u} = u$, $t\overline{t} = 1$, то

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

Элемент $x_{a+b}(-2\overline{t})$ перестановочен с тремя другими сомножителями элемента $\alpha\gamma$. В силу леммы 9

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

Отсюда

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

Далее,

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

Таким образом, в M лежит подгруппа

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

которая в силу леммы 11 совпадает с подгруппой $\langle X_{a+b}, X_{-a-b}\rangle$. В частности, в M лежат все диагональные элементы $h_{a+b}(v)$, $v \in K^*$. Сейчас при любом ненулевом v из подполя неподвижных элементов $GF(q)$ относительно автоморфизма $-$, так же как и при доказательстве теоремы 2 для типа $B_2(q)$, последовательно получаем, что в M лежат элементы

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

Далее дословно повторяем доказательство теоремы 2. Теорема доказана.

§ 7. Порождающие тройки инволюций группы $^2A_4(2^{2n})$

Пусть r_1, r_2, r_3, r_4 — фундаментальная система системы корней Φ типа A_4, причём $r_1+r_2, r_2+r_3, r_3+r_4 \in \Phi$. Положим $q^2 = 2^{2n}$, $t^q = \overline{t}$. Группа $^2A_4(q^2) \simeq U_5(q)$ порождается своими корневыми элементами

$$\begin{aligned} x_a(t,u) &= x_{r_2}(t)x_{r_3}(\overline{t})x_{r_2+r_3}(u),\ t\overline{t} = u+\overline{u}, \\ x_b(t) &= x_{r_1}(t)x_{r_4}(\overline{t}), \\ x_{a+b}(t,u) &= x_{r_1+r_2}(t)x_{r_3+r_4}(\overline{t})x_{r_1+r_2+r_3+r_4}(u),\ t\overline{t} = u+\overline{u}, \\ x_{2a+b}(t) &= x_{r_1+r_2+r_3}(t)x_{r_2+r_3+r_4}(\overline{t}), \\ x_{-a}(t,u) &= x_{-r_2}(t)x_{-r_3}(\overline{t})x_{-r_2-r_3}(u),\ t\overline{t} = u+\overline{u}, \\ x_{-b}(t) &= x_{-r_1}(t)x_{-r_4}(\overline{t}), \\ x_{-a-b}(t,u) &= x_{-r_1-r_2}(t)x_{-r_3-r_4}(\overline{t})x_{-r_1-r_2-r_3-r_4}(u),\ t\overline{t} = u+\overline{u}, \\ x_{-2a-b}(t) &= x_{-r_1-r_2-r_3}(t)x_{-r_2-r_3-r_4}(\overline{t}). \end{aligned}$$

Здесь с группой ${}^2A_4(q^2)$ мы связываем систему корней типа B_2. Мономиальный элемент

$$n_0 = n_b n_{2a+b} = n_{r_1} n_{r_4} n_{r_1+r_2+r_3} n_{r_2+r_3+r_4}$$

является инволюцией и, в частности,

$$n_0 x_a(t,u) n_0 = x_{-a}(\bar{t}, u),$$
$$n_0 x_b(t) n_0 = x_{-b}(\bar{t}).$$

ЛЕММА 16. *В группе ${}^2A_3(2^{2n})$ справедливы следующие коммутаторные формулы:*

$$[x_a(t,u), x_b(v)] = x_{a+b}(tv, v\overline{vu}) x_{2a+b}(vu), \tag{22}$$

$$[x_a(t,u), x_{a+b}(v,w)] = x_{2a+b}(\bar{t}v), \tag{23}$$

$$[x_b(t), x_{2a+b}(v)] = x_{a+b}(0, t\bar{v} + \bar{t}v). \tag{24}$$

ДОКАЗАТЕЛЬСТВО. Прямые вычисления в группе $A_4(2^{2^n})$ дают указанные ниже равенства, в которых сокращающиеся переносимые справа налево друг ко другу элементы берутся в фигурные скобки. При этом могут появляться новые корневые элементы. На заключительных этапах из корневых элементов группы Шевалле нормального типа A_4 собираются корневые элементы скрученной группы ${}^2A_4(2^{2^n})$.

Установим первое соотношение. Последовательно получаем равенства

$$
\begin{aligned}
&[x_a(t,u), x_b(v)] = \\
&= x_{r_2}(t)x_{r_3}(\bar{t})\{x_{r_2+r_3}(u)\}x_{r_1}(v)x_{r_4}(\bar{v})\{x_{r_2+r_3}(u)\}x_{r_3}(\bar{t})x_{r_2}(t)x_{r_4}(\bar{v})x_{r_1}(v) \\
&= x_{r_2}(t)\{x_{r_3}(\bar{t})\}x_{r_1}(v)x_{r_1+r_2+r_3}(uv)x_{r_4}(\bar{v})x_{r_2+r_3+r_4}(u\bar{v})\{x_{r_3}(\bar{t})\}x_{r_2}(t)x_{r_4}(\bar{v})x_{r_1}(v) \\
&= x_{r_2}(t)x_{r_1}(v)x_{r_1+r_2+r_3}(uv)\{x_{r_4}(\bar{v})\}x_{r_3+r_4}(\bar{t}\bar{v})x_{r_2+r_3+r_4}(u\bar{v})x_{r_2}(t)\{x_{r_4}(\bar{v})\}x_{r_1}(v) \\
&= \{x_{r_2}(t)\}x_{r_1}(v)x_{r_1+r_2+r_3}(uv)x_{r_3+r_4}(\bar{t}\bar{v})x_{r_2+r_3+r_4}(u\bar{v})\{x_{r_2}(t)\}x_{r_1}(v) \\
&= x_{r_1}(v)x_{r_1+r_2}(tv)x_{r_1+r_2+r_3}(uv)x_{r_3+r_4}(\bar{t}\bar{v})x_{r_2+r_3+r_4}(t\bar{t}\bar{v})x_{r_2+r_3+r_4}(u\bar{v})x_{r_1}(v) \\
&= \{x_{r_1}(v)\}x_{r_1+r_2}(tv)x_{r_1+r_2+r_3}(uv)x_{r_3+r_4}(\bar{t}\bar{v})x_{r_2+r_3+r_4}(\overline{uv})\{x_{r_1}(v)\} \\
&= x_{r_1+r_2}(tv)x_{r_1+r_2+r_3}(uv)x_{r_3+r_4}(\bar{t}\bar{v})x_{r_2+r_3+r_4}(\overline{uv})x_{r_1+r_2+r_3+r_4}(v\overline{vu}) \\
&= x_{r_1+r_2}(tv)x_{r_3+r_4}(\bar{t}\bar{v})x_{r_1+r_2+r_3+r_4}(v\overline{vu})x_{r_1+r_2+r_3}(uv)x_{r_2+r_3+r_4}(\overline{uv})
\end{aligned}
$$

$= x_{a+b}(tv, v\overline{vu})x_{2a+b}(vu)$.

Докажем второе соотношение. Вычисления показывают, что

$$[x_a(t,u), x_{a+b}(v,w)] =$$
$$= x_{r_2}(t)x_{r_3}(\bar{t})x_{r_2+r_3}(u)x_{r_1+r_2}(v)x_{r_3+r_4}(\overline{v})\{x_{r_1+r_2+r_3+r_4}(w)\}\times$$
$$\times\, x_{r_2+r_3}(u)x_{r_3}(\bar{t})x_{r_2}(t)\{x_{r_1+r_2+r_3+r_4}(w)\}x_{r_3+r_4}(\overline{v})x_{r_1+r_2}(v)$$
$$= x_{r_2}(t)x_{r_3}(\bar{t})\{x_{r_2+r_3}(u)\}x_{r_1+r_2}(v)x_{r_3+r_4}(\overline{v})\{x_{r_2+r_3}(u)\}x_{r_3}(\bar{t})x_{r_2}(t)\times$$
$$\times\, x_{r_3+r_4}(\overline{v})x_{r_1+r_2}(v)$$
$$= x_{r_2}(t)\{x_{r_3}(\bar{t})\}x_{r_1+r_2}(v)x_{r_3+r_4}(\overline{v})\{x_{r_3}(\bar{t})\}x_{r_2}(t)x_{r_3+r_4}(\overline{v})x_{r_1+r_2}(v)$$
$$= \{x_{r_2}(t)\}x_{r_1+r_2}(v)x_{r_1+r_2+r_3}(\bar{t}v)x_{r_3+r_4}(\overline{v})\{x_{r_2}(t)\}x_{r_3+r_4}(\overline{v})x_{r_1+r_2}(v)$$
$$= \{x_{r_1+r_2}(v)\}x_{r_1+r_2+r_3}(\bar{t}v)\{x_{r_3+r_4}(\overline{v})\}x_{r_2+r_3+r_4}(t\overline{v})\{x_{r_3+r_4}(\overline{v})\}\{x_{r_1+r_2}(v)\}$$
$$= x_{r_1+r_2+r_3}(\bar{t}v)x_{r_2+r_3+r_4}(t\overline{v}) = x_{2a+b}(\bar{t}v).$$

Наконец, установим третье соотношение. Имеем

$$[x_b(t), x_{2a+b}(v)] =$$
$$= x_{r_1}(t)\{x_{r_4}(\bar{t})\}x_{r_1+r_2+r_3}(v)x_{r_2+r_3+r_4}(\overline{v})\{x_{r_4}(\bar{t})\}x_{r_1}(t)x_{r_2+r_3+r_4}(\overline{v})x_{r_1+r_2+r_3}(v)$$
$$= \{x_{r_1}(t)\}x_{r_1+r_2+r_3}(v)x_{r_1+r_2+r_3+r_4}(\bar{t}v)x_{r_2+r_3+r_4}(\overline{v})\{x_{r_1}(t)\}x_{r_2+r_3+r_4}(\overline{v})\times$$
$$\times\, x_{r_1+r_2+r_3}(v)$$
$$= x_{r_1+r_2+r_3}(v)x_{r_1+r_2+r_3+r_4}(\bar{t}v)x_{r_2+r_3+r_4}(\overline{v})x_{r_1+r_2+r_3+r_4}(t\overline{v})x_{r_2+r_3+r_4}(\overline{v})\times$$
$$\times\, x_{r_1+r_2+r_3}(v)$$
$$= x_{r_1+r_2+r_3+r_4}(\bar{t}v)x_{r_1+r_2+r_3+r_4}(t\overline{v}) = x_{a+b}(0, t\overline{v}+\bar{t}v).$$

Лемма доказана.

Частным случаем для [18, теор. 3], когда основное поле конечно, является

ЛЕММА 17. *Пусть подгруппа M группы ${}^2A_{2l}(q^2)$, $l \geq 2$, имеет неединичные пересечения со всеми её корневыми подгруппами, причём $x_r(k,m) \in M$ для некоторого корня $r \in {}^2A_{2l}$ и некоторых ненулевых k и m. Тогда существуют диагональный элемент $h \in {}^2\hat{A}_{2l}(q^2)$ и число q', делящее q, такие что $hMh^{-1} = {}^2A_{2l}(q'^2)$.*

ТЕОРЕМА 4. *Пусть u — собственный элемент поля $GF(q^2)$, $q^2 = 2^{2n}$, $n \geq 2$, а v — собственный элемент подполя $GF(q)$. Тогда группа*

$^2A_4(q^2)$ порождается тремя сопряжёнными инволюциями α, β, γ, первые две из которых перестановочны, где

$$\alpha = x_{2a+b}(v),\ \ \beta = x_b(1)^{x_a(1,u)},\ \ \gamma = n_b n_{2a+b}.$$

Более того, все четыре инволюции α, β, γ и $\alpha\beta$ сопряжены.

ДОКАЗАТЕЛЬСТВО. Очевидно, α, β — инволюции. Корневые элементы $x_a(1,u)$ и $x_b(1)$ централизуют корневой элемент $x_{2a+b}(v)$, т. к. $v \in GF(q)$, поэтому $\alpha\beta = \beta\alpha$. Мономиальные элементы n_b и n_{2a+b} являются перестановочными инволюциями, следовательно γ — инволюция.

Покажем, что инволюции α, β, γ и $\alpha\beta$ лежат в одном классе сопряжённых элементов, т. е. каждая из них сопряжена с корневым элементом $x_b(1)$. Очевидно,

$$\beta^{x_a^{-1}(1,u)} = x_b(1).$$

Уравнение $us^2 = 1$ разрешимо в поле $GF(q^2)$ относительно s. Следовательно, при $us^2 = 1$ получаем

$$\alpha^{h_b(s)n_a} = x_b(us^2) = x_b(1).$$

Уравнение $s + \overline{s} = 1$ разрешимо в поле $GF(q^2)$ относительно s. Поэтому при $s + \overline{s} = 1$ с использованием формул (22) и (24) получаем соотношения

$$\begin{aligned}
\gamma^{x_{-b}(1)x_{-2a-b}(1)} &= x_b(1)x_{2a+b}(1),\\
(x_b(1)x_{2a+b}(1))^{x_a(0,1)} &= x_b(1)x_{a+b}(0,1),\\
x_b(1)x_{a+b}(0,1)^{x_{2a+b}(s)} &= x_b(1)x_{a+b}(0, s+\overline{s}+1) = x_b(1).
\end{aligned}$$

Заметим, что мы одновременно установили сопряжённость инволюций α и $\alpha\beta$, т. к. $\alpha\beta = (x_b(1)x_{2a+b}(1))^{x_a(1,u)}$.

Положим $M = \langle \alpha, \beta, \gamma \rangle$ и покажем, что $M = {}^2A_4(q^2)$. Имеют место

$$\begin{aligned}
\beta &= x_b(1)x_{a+b}(1,u)x_{2a+b}(u),\\
\gamma\alpha\gamma &= x_{-2a-b}(v).
\end{aligned}$$

Подгруппа $\langle x_{2a+b}(v), x_{-2a-b}(v) \rangle$ содержит мономиальный элемент n_{2a+b}. Отсюда

$$\gamma n_{2a+b} = n_b \in M.$$

Далее,

$$\begin{aligned}\beta n_b\beta n_b &= x_b(1)x_{a+b}(1,u)x_{2a+b}(u)x_{-b}(1)x_a(1,u)x_{2a+b}(\overline{u})\\ &= x_b(1)x_{a+b}(1,u)x_{-b}(1)x_{2a+b}(u)x_a(0,u+\overline{u})x_a(1,u)x_{2a+b}(\overline{u})\\ &= x_b(1)x_{-b}(1)x_{a+b}(1,u)(1)x_a(1,\overline{u})x_{2a+b}(\overline{u})x_{2a+b}(u)x_a(0,u+\overline{u})\times\\ &\quad\times x_a(1,u)x_{2a+b}(\overline{u})\\ &= x_b(1)x_{-b}(1)x_{a+b}(1,u)(1)x_{2a+b}(u)x_a(0,1),\end{aligned}$$

$$n_b\beta n_b\beta n_b = x_b(1)x_{a+b}(1,u)(1)x_{2a+b}(u)x_a(0,1),$$

$$\beta n_b\beta n_b\beta n_b = x_a(0,1),$$

$$x_a(0,1)\gamma x_a(0,1)\gamma x_a(0,1) = n_a,$$

$$n_a\alpha n_a = x_b(v),$$

$$[x_b(v),\beta] = x_{a+b}(0,v).$$

$$n_b x_{a+b}(0,v)n_b = x_a(0,v).$$

По условию теоремы v — собственный элемент поля $GF(q)$. В силу леммы 12 подгруппа $\langle x_a(0,v),x_a(0,1),n_a\rangle$ изоморфна группе $SL_2(q)$ и совпадает с подгруппой $\langle x_a(0,t),x_{-a}(0,t)\mid t\in GF(q)\rangle$. В этой подгруппе существует такой элемент h, что $hx_b(v)h^{-1}=x_b(1)$. Очевидно,

$$x_b(1)\beta = x_{a+b}(1,u)x_{2a+b}(u).$$

Подгруппа $\langle x_b(1),x_b(v),n_b\rangle$ также изоморфна группе $SL_2(q)$ и обладает таким диагональным элементом h, что

$$[h,x_{a+b}(1,u)x_{2a+b}(u)] = x_{a+b}(k,m)$$

для некоторых ненулевых элементов k,m.

Итак, подгруппа $M=\langle\alpha,\beta,\gamma\rangle$ группы ${}^2A_4(q^2)$ имеет неединичные пересечения со всеми её корневыми подгруппами, содержит подгруппу $\langle x_a(0,t),x_{-a}(0,t)\mid t\in GF(q)\rangle$ и элемент $x_{a+b}(k,m)\in M$ для некоторых ненулевых элементов k,m. По лемме 17

$$M={}^2A_4(q^2).$$

Теорема доказана.

§ 8. Заключительные замечания

Объединяя теоремы 2–4, получаем теорему 1, сформулированную во введении. Пусть G — одна из групп в формулировке теоремы 1. По этой теореме она порождается тремя сопряжёнными инволюциями α, β, γ, первые две из которых перестановочны, причём инволюции α и $\alpha\beta$ также сопряжены. Поэтому G порождается пятёркой сопряжённых инволюций α, β, $\alpha\beta$, γ, γ, произведение которых равно 1. Из простоты группы G легко получить, что $i(G) > 4$. Отсюда $i(G) = 5$. Таким образом, следствие из теоремы 1 доказано.

ЛИТЕРАТУРА

1. *Я. Н. Нужин*, Порождающие тройки инволюций знакопеременных групп, Матем. заметки, **51**, № 4 (1992), 91—95.
2. *Я. Н. Нужин*, Порождающие тройки инволюций групп Шевалле над конечным полем характеристики 2, Алгебра и логика, **29**, № 2 (1990), 192—206.
3. *Я. Н. Нужин*, Порождающие тройки инволюций групп лиева типа над конечным полем нечетной характеристики. I, Алгебра и логика, **36**, № 1 (1997), 77—96.
4. *Я. Н. Нужин*, Порождающие тройки инволюций групп лиева типа над конечным полем нечетной характеристики. II, Алгебра и логика, **36**, № 4 (1997), 422—440.
5. *В. Д. Мазуров*, О порождении спорадических простых групп тремя инволюциями, две из которых перестановочны, Сиб. матем. ж., **44**, № 1 (2003), 193—198.
6. *J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson*, Atlas of finite groups, Oxford, Clarendon Press, 1985.
7. Unsolved problems in group theory. The Kourovka notebook, No. 19, Novosibirsk, Sobolev Institute of Mathematics, 2018;

   http://www.math.nsc.ru/~alglog/19tkt.pdf
8. *J. M. Ward*, Generation of simple groups by conjugate involutions, PhD Thesis, Queen Mary college, Univ. London, 2009.

9. *E. S. Rapaport*, Cayley color groups and Hamilton lines, Scripta Math., **24** (1959), 51—58.
10. *I. Pak, R. Radoičić*, Hamiltonian paths in Cayley graphs, Discrete Math., **309**, No. 17 (2009), 5501—5508.
11. *G. A. Jones*, Automorphism groups of edge-transitive maps, arXiv:1605.09461 [math.CO]
12. *M. Mačaj*, On minimal kaleidoscopic regular maps with trinity symmetry, The seventh workshop Graph Embeddings and Maps on Surfaces, Abstracts (Podbanske, Slovakia, 30 July - 4 August, 2017), 2017.
13. *R. W. Carter*, Simple groups of Lie type (Pure and Appl. Math., **28**), London a.o., John Wiley & Sons, a Wiley Intersci. Publ., 1972.
14. *L. E. Dickson*, Linear groups with an exposition of the Galois field theory, Leipzig, B. G. Teubner, 1901.
15. *D. Gorenstein*, Finite groups (Harper's Ser. Modern Math.), New York a.o., Harper & Row Publ., 1968.
16. *Я. Н. Нужин*, Порождающие множества элементов групп Шевалле над конечным полем, Алгебра и логика, **28**, № 6 (1989), 670—686.
17. *В. М. Левчук*, Замечание к теореме Л. Диксона, Алгебра и логика, **22**, № 4 (1983), 421—434.
18. *Я. Н. Нужин*, О группах, заключенных между группами лиева типа над различными полями, Алгебра и логика, **22**, № 5 (1983), 526—541.

Поступило 30 августа 2017 г.

Окончательный вариант 7 мая 2019 г.

Адрес автора:

НУЖИН Яков Нифантьевич, Сиб. федерал. ун-т, Ин-т матем. фундам. информ., пр. Свободный, 79, г. Красноярск, 660041, РОССИЯ. e-mail: nuzhin2008@rambler.ru