Министерство науки и высшего образования РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт математики и фундаментальной информатики
Кафедра алгебры и математической логики

УТВЕРЖДАЮ
И. О. заведующего
кафедрой
/Я.Н.Нужин
«____» _____ 2023 г.

БАКАЛАВРСКАЯ РАБОТА

Направление 01.03.01 Математика

ПОРОЖДАЮЩИЕ МНОЖЕСТВА ИНВОЛЮЦИЙ ЛИНЕЙНЫХ ГРУПП МАЛЫХ РАЗМЕРНОСТЕЙ НАД КОНЕЧНЫМИ ПОЛЯМИ ХАРАКТЕРИСТИКИ 2

Руководитель	профессор, доктор физико-математических наук	Я.Н. Нужин
Выпускник		Т.С. Петруть
Нормоконтролер		Т.Н. Шипина

Красноярск 2023

РЕФЕРАТ

Дипломная работа по теме «Порождающие множества инволюций линейных групп малых размерностей над конечными полями характеристики 2» содержит 23 страницы текста, 1 приложение, 15 использованных источников.

КОНЕЧНАЯ ПРОСТАЯ ГРУППА, КЛАСС СОПРЯЖЕННОСТИ, ПОРОЖДАЮЩЕЕ МНОЖЕСТВО ИНВОЛЮЦИЙ, ЗНАКОПЕРЕМЕННАЯ И СИМПЛЕКТИЧЕСКАЯ ГРУППА.

Цель работы — для группы $GL_n(F)$ малых размерностей над полем F характеристики 2 найти нижнюю границу числа порождающих инволюций, произведение которых равно единице; для групп A_8 и $PSp_4(2^n)$ найти порождающие множества инволюций, удовлетворяющих некоторым дополнительным условиям.

В результате исследований для группы $GL_n(F)$ малых размерностей над полем F характеристики 2 указана нижняя граница числа порождающих инволюций, произведение которых равно единице. В явном виде получена четверка сопряженных инволюций, две из которых перестановочны, порождающая группу A_8. Доказана теорема о существовании тройки сопряженных инволюций, две из которых перестановочны, для группы $PSp_4(2^n)$.

СОДЕРЖАНИЕ

Введение 3
1 Обозначения и терминология 5
2 Применение теоремы Скотта 8
3 Группа A_8 11
4 Группа $PSp_4(2^n)$ 14
Заключение 21
Список использованных источников 22
Приложение 24

ВВЕДЕНИЕ

Вопрос о минимальном количестве и порядках порождающих элементов группы постоянно вызывал большой интерес и изучался для разнообразных классов групп: конечных и бесконечных, абстрактных, групп подстановок, матричных групп и других. Порождающие тройки инволюций конечных групп используются при нахождении гамильтоновых циклов в графах Кели и при описании групп автоморфизмов карт.

Хорошо известно, что классические группы порождаются своими простейшими элементами. Например, симметрические группы порождаются транспозициями, а простые классические линейные группы или более обобщенно — простые группы лиева типа — порождаются корневыми элементами. В обоих случаях мощность порождающего множества растет вместе с ростом мощности самой группы. Особый интерес вызывают порождающие множества минимальной мощности относительно некоторых свойств.

В 1999 году Я. Н. Нужин записал в Коуровскую тетрадь следующий вопрос [1, вопрос 14.69].

Для каждой конечной простой неабелевой группы найти минимум числа порождающих инволюций, удовлетворяющих дополнительному условию, в каждом из следующих случаев:

а) Произведение порождающих инволюций равно 1;

б) (Малле-Сакс-Вайгель). Все порождающие инволюции сопряжены;

в) (Малле-Сакс-Вайгель). Выполняются одновременно свойства а) и б);

г) Все порождающие инволюции сопряжены, и две из них перестановочны;

Целью бакалаврской работы является решение вопроса 14.69 для некоторых групп.

Для исследования были поставлены следующие **задачи**:

1. Для группы $GL_n(F)$ малых размерностей над полем F характеристики 2 провести вычисления, которые могут быть полезны для решения задачи 14.69в).

2. Для группы A_8 указать в явном виде четверку порождающих сопряженных инволюций, две из которых перестановочны (задача 14.69г)).

3. Для группы $PSp_4(2^n)$ найти минимальное число порождающих сопряженных инволюций, две из которых перестановочны (задача 14.69г)).

1 Обозначения и терминология

Все нижеперечисленные определения были взяты из книги А. И. Кострикина "Введение в алгебру"[2] и М. И. Каргаполова, Ю. И. Мерзлякова "Основы теории групп"[3]

Определение 1.1. Группа называется *конечной*, если она состоит из конечного числа элементов. Число элементов конечной группы называется её *порядком*.

Для порядка конечной группы G будем использовать обозначение $|G|$.

Определение 1.2. *Порядком элемента* g группы называется наименьшее натуральное число n, такое что $g^n = 1$. Элемент порядка 2 называется *инволюцией*.

Определение 1.3. Подгруппа H группы G называется *нормальной*, если $g^{-1}hg \in H$ для любых $h \in H$, $g \in G$.

Определение 1.4. *Простая группа* —это группа, не имеющая нормальных подгрупп, отличных от всей группы и единичной подгруппы.

Определение 1.5. *Коммутатор* двух элементов g и h из группы G, является элементом $[g, h] = ghg^{-1}h^{-1}$

Определение 1.6. Элементы g_1 и g_2 группы G называются *сопряженными*, если существует элемент $h \in G$, для которого $hg_1h^{-1} = g_2$. Сопряженность является отношением эквивалентности, а потому разбивает G на классы эквивалентности, это, в частности, означает, что каждый элемент группы принадлежит в точности одному классу сопряженности, и классы $[g_1]$ и $[g_2]$ совпадают тогда и только тогда, когда g_1 и g_2 сопряжены, и не пересекаются в противном случае.

Определение 1.7. *Класс сопряженности* — множество элементов группы G, образованное из элементов, сопряженных заданному $g \in G$, то есть — всех элементов вида hgh^{-1}, где h — произвольный элемент группы G.

Класс сопряженности элемента $g \in G$ может обозначаться $[g]$ или g^G.

Определение 1.8. *Инвариантное подпространство* W векторного пространства V относительно линейного отображения $T : V \longrightarrow V$ — это такое подпространство, что $T(x) \in W$ для любого $x \in W$ другими словами $T(W) \subset W$. Подпространство называется *инвариантным относительно группы* G, если оно инвариантно относительно каждого элемента этой группы, рассматриваемого как линейное преобразование.

Определение 1.9. Матричная группа называется *приводимой*, если существует собственное инвариантное подпространство. В противном случае, группа называется неприводимой.

Под представлением группы мы будем понимать вложение этой группы в общую линейную группу $GL_n(F)$ над полем F

Определение 1.10. *Характером* $\chi(g)$ элемента g данной группы G в заданном представлении называется сумма диагональных элементов матрицы, соответствующей элементу g в этом представлении.

Хорошо известно, что число неприводимых представлений данной группы равно числу её классов сопряженных элементов.

Конечное поле $GF(q)$ — поле, состоящее из конечного числа элементов q, где $q = p^m$, p — простое число.

Определение 1.11. *Примитивным элементом* конечного поля $GF(p^m)$ называется такой элемент α, что все элементы поля, за исключением нуля, могут быть представлены в виде степени элемента.

Определение 1.12. Подполе отличное от всего поля называется *собственным подполем*. Элемент называется собственным, если он не лежит в собственном подполе.

Очевидно, всякий примитивный элемент поля является собственным элементом. Обратное не верно. Например, элемент порядка 4 в поле из 9 элементов $GF(9)$, является его собственным элементом, но не является примитивным. Так как порядок примитивного элемента в этом поле равен 8.

Определение 1.13. *Трансвекция* —это матрица, содержащая единицы на главной диагонали, ненулевое число t в ячейке $(i, j), i \neq j$ и нули в остальных ячейках.

Определение 1.14. *Порождающее множество* группы —это такое её подмножество, что каждый её элемент может быть представлен в виде конечного произведения элементов из этого подмножества и их обратных.

2 Применение теоремы Скотта.

Хорошо известен следующий результат Л. Скотта, который часто применяется для получения отрицательных утверждений о порождении неприводимых матричных групп над полями, определёнными конечными множествами матриц.

Теорема 2.1. [4, Scott L.L.] *Пусть неприводимая подгруппа G общей линейной группы $GL_n(K)$ над полем K порождается элементами $g_1, g_2, \ldots, g_k$, с условием*

$$g_1 g_2 \ldots g_k = 1.$$

Через $d(g_i)$ обозначим коразмерность подпространства неподвижных элементов $V_n(g_i) = \{v \in V_n | g_i v = v\}$, где векторное пространство размерности n над полем K. Тогда

$$d(g_1) + d(g_2) + \cdots + d(g_k) \geq 2n \tag{2.1}$$

В силу теории К. Жордана в качестве представителей сопряженных классов инволюций в группе $GL_n(K)$ при $n = 2, 3, 4, 5, 6$ над полем K характеристики 2 можно взять следующие матрицы:

$$\alpha(2,1) = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix};$$

$$\alpha(3,1) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix};$$

$$\alpha(4,1) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

$$\alpha(4,2) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix};$$

$$\alpha(5,1) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix};$$

$$\alpha(5,2) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix};$$

$$\alpha(6,1) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix};$$

$$\alpha(6,2) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix};$$

$$\alpha(6,3) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

Непосредственно проверкой неравенством Скотта 2.1, получена

Теорема 2.2. *Пусть G – неприводимая подгруппа общей линейной группы $GL_n(F)$ над полем F характеристики 2, порожденная инволюциями $\alpha_1, \alpha_2, \ldots, \alpha_k$ из класса сопряженности с представителем $\alpha(n,i)$ с условием*

$$\alpha_1\alpha_2 \ldots \alpha_k = 1.$$

Тогда

$$k \geqslant c(n,i),$$

где константы $c(n,i)$ соответственно равны:

$$c(2,1) = 4;$$
$$c(3,1) = 6;$$
$$c(4,1) = 8,\ c(4,2) = 4;$$
$$c(5,1) = 10,\ c(5,2) = 5;$$
$$c(6,1) = 12,\ c(6,2) = 6,\ c(6,3) = 4.$$

Эти результаты могут быть полезны при решении задачи 14.69в) описанной в введении.

3 Группа A_8

Введем некоторые ключевые обозначения, которые будут использоваться далее.

Определение 3.1. Для любой конечной простой неабелевой группы G, порожденной инволюциями, обозначим:
1) через $n_c(G)$ минимальное число сопряженных порождающих инволюций, произведение которых равно 1;
2) через $m(G)$ обозначим минимальное число сопряженных порождающих инволюций, две из которых перестановочны.

Лемма 1. *Если группа G порождается тремя сопряжёнными инволюциями, то*

$$m(G) \leq 4.$$

Доказательство. Пусть $G = \langle a, b, c\rangle$, где a, b, c — тройка порождающих сопряжённых инволюций, тогда $G = \langle a, a, b, c\rangle$, где a, a, b, c — порождающая четвёрка сопряжённых инволюций, две из которых перестановочны. □

Очевидно, что в силу определения числа $m(G)$, если G не порождается тремя инволюциями, две из которых перестановочны, то $m(G) \geq 4$. В работах [5], [6], [7], [8], [9], [10], [11] указаны известные конечные простые группы, которые не порождаются тремя инволюциями, две из которых перестановочны. Объединяя результаты этих работ, получаем следующую теорему.

Теорема 3.1. *Конечные простые неабелевы группы, которые не порождаются тремя инволюциями, две из которых перестановочны исчерпываются*

следующими:

1) Знакопеременные группы:

$$A_6, A_7, A_8$$

2) Классические группы

$$L_3(q), U_3(q), L_4(2^n), U_4(2^n), U_4(3), S_4(3), U_5(2)$$

3) Спорадические группы:

$$M_{11}, M_{22}, M_{23}, McL.$$

Известно, что $n_c(A_8) = 7$ [12]. С другой стороны, если группа G порождается тремя сопряженными инволюциями, то получаем верхнюю оценку

$$n_c(G) \leq 6.$$

Следовательно, A_8 не порождается тремя сопряженными инволюциями. В частности,

$$m(A_8) > 3.$$

Доказательство следующей теоремы основано на том, что порождающая четверка сопряженных инволюций, две из которых перестановочны, указывается явно.

Теорема 3.2. $m(A_8) = 4$

Доказательство. Группа $A_8 \cong PSL_4(2)$, порождается четверкой трансвекций.

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

$$\gamma = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \delta = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

причем $\alpha\beta = \beta\alpha$.

Действительно, хорошо известно, что группа $SL_n(q)$ над любым конечным полем порядка q порождается своими трансвекциями. Нетрудно понять, что, коммутируя между собой трансвекции α, β, γ, получим все нижние трансвекции. Затем, коммутируя все нижние трансвекции с δ, получим все верхние трансвекции. Таким образом, инволюции $\alpha, \beta, \gamma, \delta$ порождают группу A_8. □

Существует порождающая четверка инволюций также из второго класса сопряженности:

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

$$\gamma = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \delta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix},$$

где $\alpha\beta = \beta\alpha$. Данные порождающие найдены с помощью компьютерной системы GAP (Groups, Algorithms and Programming) [Приложение А].

Заметим, что

$$A_8 = \langle \alpha, \beta, \beta\alpha, \gamma, \gamma, \sigma, \sigma \rangle$$

и

$$\alpha\beta(\beta\alpha)\gamma\gamma\sigma\sigma = 1.$$

Таким образом, справедливо следующее следствие, которое впервые отмечается в диссертации Дж. Ворда [12].

Следствие 1. $n_c(A_8) = 7$ *для любого класса сопряженных инволюций.*

4 Группа $PSp_4(2^n)$

Как и в предыдущем пункте, обозначим через $n_c(G)$ минимальное число сопряженных порождающих инволюций, произведение которых равно 1, а через $m(G)$ обозначим минимальное число сопряженных порождающих инволюций, две из которых перестановочны.

Далее, введем некоторые обозначения, которые используются в теории групп Шевалле. Они потребуются для дальнейшей работы.

$$x_a(t) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ t & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & t & 1 \end{pmatrix};$$

$$x_b(t) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & t & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

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

$$x_{2a+b}(t) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ t & 0 & 0 & 1 \end{pmatrix};$$

$$x_{-a}(t) = \begin{pmatrix} 1 & t & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & t \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

$$x_{-b}(t) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & t & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

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

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

где $t \in F$.

Для группы $PSp_4(2^n)$ ответ на вопрос из Коуровской тетради [вопрос 14.69г)] даёт следующая теорема.

Теорема 4.1. *Группа $PSp_4(2^n)$ при $n \geq 2$ порождается тремя сопряженными инволюциями, две из которых перестановочны, то есть*

$$m(PSp_4(2^n)) = 3.$$

Доказательство. В группе $PSp_4(2^n)$ три класса сопряженных инволюций, с

представителями

$$\sigma_1 = \begin{pmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\sigma_2 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

$$\sigma_3 = \begin{pmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Обозначим через H больший по размерности класс с представителем σ_3. Выделим следующие три матрицы:

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

$$\beta = \begin{pmatrix} 1 & 0 & t^3 & 1 \\ 0 & 1 & 0 & t^3 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

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

где t — примитивный (собственный) элемент конечного поля $\mathbb{F}_{2^n}$.

Матрицы β и γ лежат в H, но α не принадлежит классу H. Пусть

$$\delta = \alpha\beta = \begin{pmatrix} 1 & t & t^3 & t^4+1 \\ 0 & 1 & 0 & t^3 \\ 0 & 0 & 1 & t \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Тогда, δ тоже лежит в H. Также заметим, что инволюции δ и β перестановочны.

Для доказательства теоремы достаточно показать, что группа

$$M = \langle(\alpha\beta), \beta, \gamma\rangle = \langle\delta, \beta, \gamma\rangle$$

совпадает с $PSp_4(2^n)$.

Вычисления показывают, что:

$$\gamma\beta\gamma = \beta^\gamma = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ t^3 & 0 & 1 & 0 \\ 1 & t^3 & 0 & 1 \end{pmatrix};$$

$$[\alpha, \beta^\gamma] = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ t & t^2 & 1 & 0 \\ 0 & t & 0 & 1 \end{pmatrix};$$

$$[\alpha, \beta^\gamma]^\gamma = \begin{pmatrix} 1 & 0 & t & 0 \\ 0 & 1 & t^2 & t \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

$$[[\alpha,\beta^\gamma]^\gamma,\alpha]=\begin{pmatrix}1&0&t^3&t^4\\0&1&0&t^3\\0&0&1&0\\0&0&0&1\end{pmatrix};$$

$$\varepsilon=[[\alpha,\beta^\gamma]^\gamma,\alpha]*\beta=\begin{pmatrix}1&0&0&t^4+1\\0&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}=t_{14}(t^4+1);$$

$$\varepsilon^\gamma=\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\t^4+1&0&0&1\end{pmatrix}=t_{41}(t^4+1).$$

Далее нам потребуется следующее утверждение.

Лемма 2. [13, лемма 5] *Пусть t и t^2 — собственные элементы поля F. Если характеристика поля F равна 2, то*

$$n_r=x_r(t)x_{-r}(t)x_r(t)\in\langle x_r(t),x_{-r}(t)\rangle,$$

для любого не нулевого $t\in F$.

По лемме 2.

$$\langle\varepsilon,\varepsilon^\gamma\rangle\ni\begin{pmatrix}0&0&0&1\\0&1&0&0\\0&0&1&0\\1&0&0&0\end{pmatrix}=\eta.$$

В группе M лежит матрица

$$x_a(t) = \alpha^\gamma = \begin{pmatrix} 1 & 0 & 0 & 0 \\ t & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & t & 1 \end{pmatrix}.$$

Поэтому, снова по лемме 2 получаем включение

$$\langle \alpha, \alpha^\gamma \rangle \ni \begin{pmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} = \theta.$$

Вычисления показывают:

$$x_{-a-b}(t) = \alpha^\eta = \begin{pmatrix} 1 & 0 & t & 0 \\ 0 & 1 & 0 & t \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

$$x_{a+b}(t) = (\alpha^\eta)^\gamma = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ t & 0 & 1 & 0 \\ 0 & t & 0 & 1 \end{pmatrix};$$

$$x_b(t^2) = (\alpha^\eta)^\gamma [\alpha, \beta^\gamma]^\gamma = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & t^2 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

$$x_{-b}(t^2) = (x_b(t^2))^\eta = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & t^2 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

$$x_{-2a-b}(t^2) = (x_b(t^2))^\theta = \begin{pmatrix} 1 & 0 & 0 & t^2 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix};$$

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

Предложение 2 из статьи Я. Н. Нужина [13] в нашем частном случае для группы $PSp_4(F)$ выглядит следующим образом.

Предложение 1. *Пусть M — подгруппа $PSp_4(F)$, t и t^2 — собственные элементы поля F. Тогда, если*

$$x_r(t), x_{-r}(t) \in M,$$

для некоторого $r = a, b, a+b, 2a+b$ и

$$M \cap x_s(F) \neq 1,$$

для $s = a, -a, 2a+b, -2a-b$, то $M = PSp_4(F)$.

Все матрицы $x_{\pm a}(t), x_{\pm b}(t^2), x_{\pm a \pm b}(t), x_{\pm 2a \pm b}(t^2)$ содержатся в M. Поэтому в силу предложения 1, получается, что $M = PSp_4(2^n)$ при $n \geq 2$.

□

Из теоремы 5 вытекает, что $n_c(G) \leq 6$. Однако, какой будет ответ на вопрос 14.69в), пятерка или шестерка еще не известно.

ЗАКЛЮЧЕНИЕ

Все поставленные задачи выполнены. В работе получены следующие результаты.

1) С помощью теоремы Скотта для группы $GL_n(F)$ над полем F характеристики 2 при $n \leq 6$ найдено минимальное число сопряженных порождающих инволюций, произведение которых равно 1. Этот результат может быть полезен при решении задачи 14.69в).

2) Для группы A_8 явно указана четверка сопряженных порождающих инволюций, две из которых перестановочны, тем самым решена задача 14.69г).

3) Для группы $PSp_4(2^n)$ явно указана тройка сопряженных порождающих инволюций, две из которых перестановочны, тем самым решена задача 14.69г).

Следует отметить, что при решении данных задач, а также при нахождении порождающих инволюций существенно использовалась система GAP и имеющиеся результаты в Атласе конечных простых групп [15]. Некоторые из полученных результатов были представлены на конференциях «Проспект Свободный — 2022» и «Проспект Свободный — 2023 »

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Коуровская тетрадь. Нерешенные вопросы теории групп —- Изд. 17-е, доп. —- Ин-т математики СО РАН, Новосибирск, 2010. —- URL: http:/math.nsc.ru/alglog/17kt.pdf. (дата обращения: 10.06.2023).

2. Кострикин, А. И. Введение в алгебру / А. И. Кострикин; — М.: Наука, 1977. — 496 с.

3. Каргаполов, М. И. Основы теории групп / М. И. Каргаполов, Ю. И. Мерзляков; — 2-е изд. — М.: Наука, 1977. — 240 с.

4. Scott, L. L. Matrices and cohomology / L. L. Scott // Ann. Math. (2). — 1977. — №3. — С. 473-492.

5. Нужин, Я. Н. Порождающие тройки инволюций групп Шевалле над конечным полем характеристики 2 / Я. Н. Нужин // Алгебра и логика. — 1990. — №2. — С. 192–206.

6. Нужин, Я. Н. Порождающие тройки инволюций знакопеременных групп / Я. Н. Нужин // Математические заметки. — 1990. — №4. — С. 91-95.

7. Нужин, Я. Н. Порождающие элементы групп лиева типа над конечным полем нечетной характеристики. I / Я. Н. Нужин // Алгебра и логика. — 1997. — №1. — С. 77–96.

8. Нужин, Я. Н. Порождающие элементы групп лиева типа над конечным полем нечетной характеристики. II / Я. Н. Нужин // Алгебра и логика. — 1997. — №4. — С. 422–440.

9. Мазуров, В. Д. О порождении спорадических простых групп тремя инволюциями, две из которых перестановочны / В. Д. Мазуров// Алгебра и логика.— 2003. — №1. — С. 193–198.

10. Тимофеенко, А. В. О порождающих тройках инволюций больших спорадических групп / А. В. Тимофеенко // Дискретная математика. — 2003. — №2. — С. 103–112.

11. Нужин, Я. Н. О порождающих тройках инволюций групп лиева типа ранга 2 над конечными полями /Я. Н. Нужин // Алгебра и логика. — 2019. — №1. — С. 84–107.

12. Ward, J. M. Generation of simple groups by conjugate involutions: Thesis of Doctor of Philosophi / Jonathan Mark Ward ; Queen Mary college, University of London, 2009. — 193p

13. Нужин, Я. Н. Порождающие множества элементов групп Шевалле над конечным полем / Я. Н. Нужин // Алгебра и логика. — 1989. — №6. — С. 670-686.

14. Нужин, Я. Н. О порождающих множествах инволюций простых конечных групп / Я. Н. Нужин // Алгебра и логика. — 2019. — №3. — С. 426-434.

15. Wilson, R. A. The Atlas of Finite Groups / R. A.Wilson, R. A.Parker , J. N.Bray; — University Press. — 1985. — 252c.

ПРИЛОЖЕНИЕ А

Нахождение порождающих инволюций в системе GAP.

```
gap> G:=SL(4,2);
SL(4,2)

gap> a:=Random(G);
<an immutable 4x4 matrix over GF2>

gap> Order(a);
2

gap> PrintArray(a);
[ [  0*Z(2),  0*Z(2),  0*Z(2),  Z(2)^0 ],
[  0*Z(2),  0*Z(2),  Z(2)^0,  0*Z(2) ],
[  0*Z(2),  Z(2)^0,  0*Z(2),  0*Z(2) ],
[  Z(2)^0,  0*Z(2),  0*Z(2),  0*Z(2) ] ]

gap> I:=Set([]);
[  ]

gap> H:=ConjugacyClass(G,a);
[ [ 0*Z(2), 0*Z(2), 0*Z(2), Z(2)^0 ],
[ 0*Z(2), 0*Z(2), Z(2)^0, 0*Z(2) ],
[ 0*Z(2), Z(2)^0, 0*Z(2), 0*Z(2) ],
[ Z(2)^0, 0*Z(2), 0*Z(2), 0*Z(2) ] ]^G

gap> for i in H do
> if a*i=i*a then
```

```
> AddSet(I,i); fi;od;

gap> b:=Random(I);

gap> PrintArray(b);

[ [  0*Z(2),  Z(2)^0,  0*Z(2),  0*Z(2) ],
  [  Z(2)^0,  0*Z(2),  0*Z(2),  0*Z(2) ],
  [  0*Z(2),  0*Z(2),  0*Z(2),  Z(2)^0 ],
  [  0*Z(2),  0*Z(2),  Z(2)^0,  0*Z(2) ] ]

gap> a*b=b*a;
true

gap> for i in [1..10] do
> c:=Random(H);
> d:=Random(H);
> if Group(a,b,c,d) = G then
> PrintArray(c);
> Print("\n");
> PrintArray(d);
> Print("\n"); fi;od;od;

[ [  0*Z(2),  0*Z(2),  0*Z(2),  Z(2)^0 ],
  [  0*Z(2),  Z(2)^0,  Z(2)^0,  0*Z(2) ],
  [  0*Z(2),  0*Z(2),  Z(2)^0,  0*Z(2) ],
  [  Z(2)^0,  0*Z(2),  0*Z(2),  0*Z(2) ] ]
```

```
[ [  Z(2)^0,  0*Z(2),  0*Z(2),  0*Z(2) ],
  [  Z(2)^0, Z(2)^0,  0*Z(2),  0*Z(2) ],
  [  0*Z(2),  0*Z(2),  0*Z(2),  Z(2)^0 ],
  [  0*Z(2),  0*Z(2),  Z(2)^0,  0*Z(2) ] ]

gap> c:= [ [  0*Z(2),  0*Z(2),  0*Z(2),  Z(2)^0 ],
  [  0*Z(2),  Z(2)^0,  Z(2)^0,  0*Z(2) ],
  [  0*Z(2),  0*Z(2),  Z(2)^0,  0*Z(2) ],
  [  Z(2)^0,  0*Z(2),  0*Z(2),  0*Z(2) ] ];

gap> d:= [ [  Z(2)^0,  0*Z(2),  0*Z(2),  0*Z(2) ],
  [  Z(2)^0, Z(2)^0,  0*Z(2),  0*Z(2) ],
  [  0*Z(2),  0*Z(2),  0*Z(2),  Z(2)^0 ],
  [  0*Z(2),  0*Z(2),  Z(2)^0,  0*Z(2) ] ];

gap> Group(a,b,c,d) = SL(4,2);
true
```

Министерство науки и высшего образования РФ
Федеральное государственное автономное
образовательное учреждение высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Институт математики и фундаментальной информатики
Кафедра алгебры и математической логики

УТВЕРЖДАЮ
И. О. заведующего
кафедрой
/Я.Н.Нужин
«23» 06 2023 г.

БАКАЛАВРСКАЯ РАБОТА

Направление 01.03.01 Математика

ПОРОЖДАЮЩИЕ МНОЖЕСТВА ИНВОЛЮЦИЙ ЛИНЕЙНЫХ ГРУПП МАЛЫХ РАЗМЕРНОСТЕЙ НАД КОНЕЧНЫМИ ПОЛЯМИ ХАРАКТЕРИСТИКИ 2

Руководитель 23.06.2023 профессор, доктор физико-математических наук Я.Н. Нужин

Выпускник 23.06.2023 Т.С. Петруть

Нормоконтролер Т.Н. Шипина

Красноярск 2023