Общероссийский математический портал

Л. С. Казарин, О группах, предложенных Сидельниковым, *Матем. сб.*, 1998, том 189, номер 7, 131–144

DOI: <https://doi.org/10.4213/sm339>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.209.158.208

26 апреля 2023 г., 14:04:13

УДК 512.54

Л. С. Казарин

О группах, предложенных Сидельниковым

Изучаются матричные группы, открытые В. М. Сидельниковым, близкие к симплектическим и ортогональным группам. Получены результаты о строении групп Сидельникова. Они могут быть полезны для построения некоторых орбитных кодов и решеток.

Библиография: 5 названий.

В работе Сидельникова [1] построено семейство конечных матричных групп $\Sigma_{n,p}$, связанных с орбитными кодами на евклидовой сфере, обладающих рядом замечательных свойств.

Некоторым подобием группы $\Sigma_{n,p}$ является группа автоморфизмов решетки Лича в 24-мерном пространстве. В [1] показано, что при $p = 2$ группа $\Sigma_{n,p}$ содержит подгруппу индекса 2, которая будет группой автоморфизмов некоторой 2^n -мерной решетки. В частности, при $n = 4$ такой решеткой является решетка Барнса–Уолла, повернутая на угол $\pi/2$ вокруг некоторой оси.

Способ задания указанных групп (через матричные образующие) не позволяет немедленно отождествить группы $\Sigma_{n,p}$ с известными конечными группами. Даже порядки указанных групп вычислены в [1] в аддитивной форме. Внимательное изучение групп Сидельникова обнаруживает их тесную связь с симплектическими и ортогональными группами над полем из p элементов. Не исключено, что все конечные простые группы лиевского типа могут быть реализованы подобным образом. Основанием для этого предположения служит аналогия между строением максимальных параболических подгрупп групп Шевалле [2] и описываемым ниже устройством групп Сидельникова.

Полученные результаты дают описание системы матричных образующих для ортогональных и симплектических групп, полезное в различных приложениях. Весьма неожиданным кажется появление матриц Фурье и Адамара в качестве образующих элементов. Отметим также наличие у групп $\Sigma_{n,p}$ матричного представления степени p^n над полем $\mathbb{C}$, вытекающее из определения.

Основной результат статьи – следующая

ТЕОРЕМА А. Пусть G – группа Сидельникова $\Sigma_{n,p}$, $n > 1$. Если $p > 2$ и $(p, n) \neq (3, 1)$, то $G \cong PK \times \mathbb{Z}_m$, где PK – полупрямое произведение экстраспециальной группы $P \cong O_p(G)$ порядка p^{2n+1} и группы $K = Sp(2n, p)$, действующей на P естественным образом. При $p \equiv 1 \pmod{4}$ $m = 2$ и при $p \equiv 3 \pmod{4}$ $m = 4$. Если $p = 2$, $n > 1$, то $G/O_2(G) \cong O^+(2n, 2)$ – ортогональная группа автоморфизмов экстраспециальной группы $O_2(G)$ порядка 2^{2n+1} , действующая на ней естественным образом.

Работа выполнена при частичной поддержке Российского фонда фундаментальных исследований (грант № 97-01-00547).

В §1 доказывается теорема В, описывающая строение групп $\Sigma_{1,p}$ ($p > 3$), являющихся в каком-то смысле моделью для общего случая. §2 посвящен рассмотрению вопросов вычислительного плана. Наконец, в §3 доказывается теорема А. Принятые обозначения в основном стандартны. Обозначения и результаты из [1] применяются достаточно широко, но основные определения воспроизводятся в тексте статьи. Если q – простое число, то $O_q(G)$ – наибольшая нормальная подгруппа группы G , порядок которой – степень числа q . Экстраспециальная q -группа – это группа X порядка q^{2n+1} , у которой $Z(X) = X' = \Phi(X)$ и $|X| = q$. Через $X \rtimes Y$ обозначается полупрямое произведение групп X и Y с нормальной подгруппой X .

§1. Группы $\Sigma_{1,p}$

Пусть F_p – поле из p элементов, K – поле характеристики, отличной от p , содержащее первообразный корень ω p -й степени из единицы. Определим матрицу $A(s) = p^{-1/2}(\omega^{abs})$, $a, b \in \{0, 1, \dots, p-1\}$. Если $f \in F_p[x]$ и $\deg f < 3$, то $E_f = \text{diag}(\omega^{f(0)}, \omega^{f(1)}, \dots, \omega^{f(p-1)})$ – диагональная матрица.

Группа Сидельникова $\Sigma_{1,p}$ определяется следующим образом:

$$\Sigma_{1,p} = \langle A(s), E_f; s = 1, 2, \dots, p-1, f \in F_p[x], \deg f < 3 \rangle.$$

Заметим, что $A(1)$ – нормализованная матрица Фурье степени p с коэффициентами из поля K . Основным результатом параграфа –

ТЕОРЕМА В. Пусть конечная группа G изоморфна группе Сидельникова $\Sigma_{1,p}$ для $p > 3$. Тогда $G = PM \times \mathbb{Z}_m$, где $P = O_p(G)$ – неабелева группа порядка p^3 и экспоненты p , $M \cong Sp(2, p)$ – группа автоморфизмов P , действующая на P естественным образом, и $m = 2$ при $p \equiv 1 \pmod{4}$, $m = 4$ при $p \equiv 3 \pmod{4}$.

В оригинале группы $\Sigma_{1,p}$ определены над полем $\mathbb{C}$, однако рассуждения проходят и для поля K , удовлетворяющего сформулированным выше условиям. Случай $p = 3$ не рассматривается по техническим соображениям. Доказательству теоремы В предпослано несколько вспомогательных утверждений. При этом вводимые в промежуточных леммах обозначения сохраняются до конца доказательства теоремы.

Следующая подгруппа $\mathfrak{L}$ группы $G = \Sigma_{1,p}$ играет важную роль в дальнейших рассуждениях. Пусть σ – аффинное отображение, ставящее в соответствие каждому элементу $x \in F_p$ элемент $\sigma(x) = dx + e \in F_p$, $d \neq 0$. Тогда $\Gamma(\sigma) = (\gamma_{ab}) \in \mathfrak{L}$, где $\gamma_{ab} = 1$, когда $\sigma(a) = b$, и $\gamma_{ab} = 0$ во всех остальных случаях. Нетрудно видеть, что $\mathfrak{L}$ состоит из перестановочных матриц и имеет порядок $p(p-1)$. Согласно теореме 1 из [1] всякий элемент $P \in \Sigma_{1,p}$ представим в виде $P = i^\varepsilon E_f A(s) E_g$ или $P = i^\varepsilon E_f \Gamma(\sigma)$ при $p \equiv 3 \pmod{4}$ и $P = \pm E_f A(s) E_g$ или $P = \pm E_f \Gamma(\sigma)$ при $p \equiv 1 \pmod{4}$ для подходящих $f, g \in F_p[x]$ с $\deg f < 3$, $\deg g < 3$, $s \in F_p^*$ и аффинного отображения $\sigma: F_p \rightarrow F_p$. Заметим, что

$$A(s)^2 = \begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 0 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \dots & 0 \end{pmatrix},$$

и потому

$$\det A(s) = \begin{cases} \pm 1 & \text{при } p \equiv 1 \pmod{4}, \\ \pm i & \text{при } p \equiv 3 \pmod{4}. \end{cases}$$

ЛЕММА 1. Пусть группа $G = \Sigma_{1,p}$, σ — аффинное отображение $F_p \rightarrow F_p$. Тогда для элементов G справедливы следующие соотношения:

- (1) $\Gamma(\sigma) = A(1)E_f A(s)$ для некоторых $f \in F_p[x]$, $f = bx$, $s \in \{1, 2, \dots, p-1\}$;
- (2) $\Gamma(\sigma)A(s) = A(1)\Gamma(\sigma')E_f$ для подходящих σ' и $f \in F_p[x]$;
- (3) если $P \in G$, $p > 3$, то либо $P = i^\varepsilon E_f A(1)\Gamma(\sigma)E_g$, либо $P = i^\varepsilon E_f \Gamma(\sigma)E_g$ для подходящих $f, g \in F_p[x]$, $\varepsilon \in \mathbb{Z}_4$ и некоторого $\Gamma(\sigma) \in \mathfrak{L}$.

ДОКАЗАТЕЛЬСТВО. (1) Рассмотрим $P = A(1)E_f A(s)$, где $f = bx$. Тогда $P = \Gamma(\sigma)$, где $\sigma(x) = (x+b)/s = s^{-1}x + s^{-1}b$. Пусть $\sigma(x) = dx + e$, $d \neq 0$. Система уравнений $s^{-1} = d$, $s^{-1}b = e$ относительно s и b , очевидно, имеет решение $s = d^{-1}$, $b = ed^{-1}$.

(2) В силу (1) имеем $\Gamma(\sigma)A(s) = A(1)E_g A(t)A(s)$ для подходящих g и t . Однако $A(t)A(s) = \Gamma(\sigma')$ для некоторого аффинного преобразования σ' поля F_p . Поэтому из $E_g \Gamma(\sigma') = \Gamma(\sigma')E_f$ для подходящего $f \in F_p[x]$ получаем заключение.

(3) По определению группы $G = \Sigma_{1,p}$ каждый ее элемент имеет запись вида

$$P = E_{f_0} A(s_1) E_{f_1} A(s_2) \dots A(s_k) E_{f_k}.$$

Предположим, что из всех таких записей для элемента P выбрана запись наименьшей длины. Если в разложении P имеется фрагмент вида $A(s_i)E_{f_i} A(s_{i+1})$, где $\deg f_i = 2$, то из соотношений (1) и (2), приведенных в [1], заключаем, что $A(s_i)E_{f_i} A(s_{i+1}) = i^\varepsilon E_g A(s)E_h$ для подходящих $g, h \in F_p[x]$, $s \in F_p^*$, $\varepsilon \in \mathbb{Z}_4$. Поэтому элемент P имеет запись меньшей длины, что противоречит его выбору.

Итак, можно считать, что $\deg f_i < 2$ для всех $i = 1, 2, \dots, k-1$. Согласно соотношению (3) из [1] $A(s_i)E_{f_i} A(s_{i+1}) = \lambda \Gamma(\sigma)$, где $\lambda = \omega^c$ для подходящего $c \in F_p$. Пусть $p > 3$. Тогда $\det E_{f_i} = 1$. Действительно, $\det E_{f_i} = \omega^{m_i}$, где $m_i = \sum_{x=0}^{p-1} (ax^2 + bx + c) \equiv 0 \pmod{p}$ (используется условие $p > 3$), откуда $\det E_{f_i} = 1$. Переходя в выписанном соотношении для матриц к определителям, имеем:

$$\det A(s_i) \det E_{f_i} \det A(s_{i+1}) = \pm \lambda^p.$$

Так как $\det A(s_i)$ — корень из единицы степени не выше 4, то $\lambda^p = \pm 1$ и

$$A(s_i)E_{f_i} A(s_{i+1}) = i^\varepsilon \Gamma(\sigma_i) \mu_i,$$

где μ_i — корень p -й степени из 1.

Таким образом, все фрагменты вида $A(s_i)E_{f_i} A(s_{i+1})$ можно заменить на $i^\varepsilon \Gamma(\sigma_i)E_{h_i}$ с $h_i \in F_p[x]$, $\deg h_i < 3$. Поэтому P имеет одну из следующих записей

$$P = i^\varepsilon E_{f_0} \Gamma(\sigma_1) E_{f_1} \dots \Gamma(\sigma_m) E_{f_m}$$

или

$$P = i^\varepsilon E_{f_0} \Gamma(\sigma_1) E_{f_1} \dots \Gamma(\sigma_m) E_{f_m} A(s) E_{f_{m+1}}.$$

Так как $\Gamma(\sigma)E_f = E_g\Gamma(\sigma)$ для подходящих $f \in F_p[x]$ и σ , то заключаем, что $P = i^\varepsilon E_f\Gamma(\sigma)$ или $P = i^\varepsilon E_f\Gamma(\sigma)A(s)E_h$. Согласно (2) $\Gamma(\sigma)A(s) = A(1)\Gamma(\sigma')E_h$. Поэтому $P = i^\varepsilon E_f\Gamma(\sigma)$ или $P = i^\varepsilon E_fA(1)\Gamma(\sigma)$, что и доказывает (3).

Нетрудно проверить, что подгруппа

$$\mathfrak{H} = \langle E_f, \Gamma(\sigma) \mid f \in F_p[x], \deg f < 3, \Gamma(\sigma) \in \mathfrak{L} \rangle$$

группы $\Sigma_{1,p}$ имеет порядок $p(p-1)$, и $\tilde{\mathfrak{H}} = \langle i^\varepsilon, \mathfrak{H} \rangle$, где $\varepsilon = 1$ при $p \equiv 3 \pmod{4}$, $\varepsilon = 2$ при $p \equiv 1 \pmod{4}$, имеет порядок $4p^4(p-1)$ в первом случае и $2p^4(p-1)$ во втором.

Расширенной группой $\tilde{\Sigma}_{1,p} = \tilde{G}$ будем называть группу $\langle \Sigma_{1,p}, i^m I \rangle$, где $m = 1$ при $p \equiv 3 \pmod{4}$ и $m = 2$ при $p \equiv 1 \pmod{4}$.

ЛЕММА 2. (1) $\tilde{\Sigma}_{1,p}$ – 2-транзитивная группа на смежных классах по подгруппе $\tilde{\mathfrak{H}}$.

(2) $\tilde{\Sigma}_{1,p} = \mathfrak{S} \times C$, где $\mathfrak{S} = \langle P \in \tilde{\Sigma}_{1,p} \mid \det P = 1 \rangle$, C – подгруппа $\mathbb{Z}_4$.

ДОКАЗАТЕЛЬСТВО. (1) В силу леммы 1 $\tilde{\Sigma}_{1,p} \subseteq \tilde{\mathfrak{H}} \cup \tilde{\mathfrak{H}}A(1)\tilde{\mathfrak{H}}$.

(2) Используя лемму 1, получаем, что для любого $P \in \Sigma_{1,p}$ значение $\det P$ содержится во множестве $\{\pm 1, \pm i\}$. Поэтому $\tilde{\Sigma}_{1,p}/\mathfrak{S}$ изоморфна подгруппе C группы $\mathbb{Z}_4$. Так как все матрицы из $\tilde{\Sigma}_{1,p}$ имеют нечетный размер p , то $\langle i^m I \rangle \cong C$ имеет тривиальное пересечение с подгруппой $\mathfrak{S}$. Поэтому получаем заключение (2).

ЛЕММА 3. Группа $G = \Sigma_{1,p} = \tilde{\Sigma}_{1,p}$. Коммутант G' группы G совпадает с $\mathfrak{S} = G''$.

ДОКАЗАТЕЛЬСТВО. Покажем сначала, что подгруппа $\mathfrak{E} = \langle E_f \mid \deg f < 3 \rangle$ содержится в G' , коммутанте группы G . Пусть $f(x) = ax^2 + bx + c$. В силу соотношения (7) из [1] $\Gamma(\sigma)E_f = E_g\Gamma(\sigma)$, где $g(x) = f(dx + e)$ при $\sigma(x) = dx + e$. Поэтому коммутатор $[E_f, \Gamma(\sigma)] = E_{g-f}$, где $(g-f)(x) = f(dx+e) - f(x)$. Если $\sigma(x) = x+1$, то $(g-f)(x) = 2ax + a + b$. При $a = 0$ элемент $E_{g-f} = \omega^b I \in Z(G) \cap G'$. При $b = 0$, $a = 1/2$ элемент $E_{x+1/2} \in G'$. Так как $E_{1/2} \in G'$ по только что сказанному, то $E_x \in G'$. Наконец, если $d = 2$, $p > 3$, то при $\sigma(x) = 2x$ имеем:

$$(g-f)(x) = a(2x)^2 + b(2x) + c - ax^2 - bx - c = 3ax^2 + bx.$$

Так как в этом случае $E_{g-f} = E_{3ax^2}E_{bx}$, то, выбрав $a = 1/3$ (напомним, что $p > 3$), заключаем, что $E_{x^2} \in G'$.

Покажем теперь, что $A(s)\det A(s)$ содержится в G' .

Рассмотрим $E_{-f}A(-1)E_fA(1) = [E_f, A(1)]$. Согласно соотношениям (1) и (2) из [1] $[E_f, A(1)] = \pm i^\varepsilon E_gA(-1/2a)E_h$, если $f = ax^2 + bx + c$, $a \neq 0$, $g, h \in F_p[x]$ и $\varepsilon = 2$ при $p \equiv 3 \pmod{4}$, $\varepsilon = 1$ при $p \equiv 1 \pmod{4}$. По доказанному выше $E_f, E_h \in G'$. Поэтому $\lambda A(-1/2a)$ содержится в G' для подходящего $\lambda \in F_p^*$. Уравнение $s = -1/2a$ разрешимо при любом $a \in F_p^*$. Поэтому $\lambda A(s)$ содержится в G' . По лемме 1 элемент $\lambda A(s)$ может содержаться в G лишь в случае, когда $\lambda^p \in \{\pm 1, \pm i\}$. Поэтому можно считать, что $\lambda^2 = 1$ или $\lambda^4 = 1$. Но $G' \subseteq \mathfrak{S}$ ввиду леммы 2. Поэтому $A(s)\det A(s)$ содержится в G' .

Пусть теперь группа $G = \langle x_1, x_2, \dots, x_n \rangle$ и для любого i существует такой элемент $z_i \in Z(G)$, что $z_i x_i \in G'$. Тогда $G' = G''$. Действительно, G' – нормальное замыкание в G множества $R = \{[x_i, x_j] \mid 1 \leq i, j \leq n\}$. Так как $[x_i z_i, x_j z_j] = [x_i, x_j]$ для любых i и j , то $R \subseteq G''$. Поэтому и нормальное замыкание R содержится в G'' . Отсюда $G' = G''$.

Так как $E_f \in G' = \Sigma'_{1,p}$ для любого $f \in F_p[x]$ с $\deg f < 3$ и $A(s) \det A(s) \in G'$ для любого $s \in F_p^*$, то $G' = G''$.

Пусть матрица P содержится в $Z(G)$. Так как $E_x = \text{diag}(\omega^0, \omega^1, \dots, \omega^{p-1})$ содержится в G , то $C_G(E_x) \geq Z(G)$. Нетрудно видеть, что $C_G(E_x)$ состоит из диагональных матриц. Так как $\Gamma(\sigma)$ перестановочна с любой матрицей из $Z(G)$, то легко проверить, что $Z(G)$ состоит из скалярных матриц. В силу леммы 1 для любой $P \in \Sigma_{1,p}$ множество значений $\det(P)$ содержится в $\{\pm 1, \pm i\}$, а матрица λI с $\lambda^p = 1$, $\lambda \neq 0$, очевидно, есть матрица вида E_f , где $f = \lambda$. Поэтому, применяя лемму 1, заключаем, что $|Z(G)| = 2^m p$, где $m = 2$ при $p \equiv 3 \pmod{4}$ и $m = 1$ при $p \equiv 1 \pmod{4}$. При этом из $E_f \in G'$ для любого $f \in F_p[x]$ ($\deg f < 3$) следует, что $\Sigma_{1,p} = G' Z(G) = \tilde{\Sigma}'_{1,p} Z(\tilde{\Sigma}_{1,p}) = \tilde{\Sigma}_{1,p}$, так как $\mathfrak{S} \supseteq G' = \tilde{G}'$ и $G = \mathfrak{S} \times C$ по лемме 2.

ЛЕММА 4. $|O_p(\Sigma_{1,p})| = p^3$, $O_p(\Sigma_{1,p})$ имеет экспоненту p и является неабелевой группой.

ДОКАЗАТЕЛЬСТВО. Пусть $\mathfrak{K}$ – подгруппа из G , порожденная всеми матрицами $\Gamma(\sigma) \in \mathfrak{L}$ и всеми E_f , где $\deg f < 2$. Очевидно, что $\mathfrak{K} = \mathfrak{E}_1 \mathfrak{L}$, где $\mathfrak{E}_1 = \langle E_f \mid \deg f < 2 \rangle$, и имеет порядок $p^3(p-1)$. По лемме 1

$$\begin{aligned} A(-1)E_f \Gamma(\sigma) A(1) &= A(-1) \Gamma(\sigma) E_g A(1) \\ &= A(-1) A(1) E_h A(s) \Gamma(\sigma) E_g A(1) = E_h A(s) \Gamma(\sigma) E_g A(1) \end{aligned}$$

для подходящих h, g степени меньше 2 и $s \in F_p[x]^*$. Так как $\deg g < 2$, то по лемме 1 (1) заключаем, что $A(-1)E_f \Gamma(\sigma) A(1)$ содержится в $\mathfrak{K}$. В силу этой же леммы $A(1)A(s)$ содержится в $\mathfrak{K}$ для любого $s \in F_p^*$. Поэтому $O_p(\mathfrak{K})$ инвариантна в $\langle A(s), E_f \mid s \in F_p^*, \deg f < 3 \rangle = \Sigma_{1,p} = G$. Так как $A(-1)E_{x^2} A(1)$ не содержится в $\mathfrak{E} = \langle E_f \mid \deg f < 3 \rangle$, то $O_p(G) \neq \mathfrak{E}$. По теореме 1 из [1] порядок силовой p -подгруппы группы G равен p^4 . Отсюда $O_p(\mathfrak{K}) = O_p(G)$ и имеет порядок p^3 . Прямые вычисления показывают, что $O_p(\mathfrak{K})$ неабелева и имеет экспоненту p .

Теперь мы имеем возможность завершить доказательство теоремы В.

Обозначим через $\mathfrak{U}$ подгруппу $O_p(G)$. Так как $\mathfrak{U}$ содержит матрицу $E_x = \text{diag}(\omega^0, \omega^1, \dots, \omega^{p-1})$, то $C_G(\mathfrak{U})$ состоит из диагональных матриц, а так как матрица $\Gamma(\sigma_0)$ для $\sigma_0 = x+1$ содержится в $\mathfrak{U}$ и перестановочна лишь со скалярными диагональными матрицами, то $C_G(\mathfrak{U}) = Z(\mathfrak{U}) \times C$, где $C = \langle i^m I \rangle$ и $m = 1$ при $p \equiv 3 \pmod{4}$, $m = 2$ при $p \equiv 1 \pmod{4}$.

Покажем, что $G/\mathfrak{U}C_G(\mathfrak{U})$ изоморфна $Sp(2, p)$. Пусть W – двумерное векторное пространство над полем F_p , e_1, e_2 – его базис. Определим на этом пространстве кососимметрическую билинейную форму $(\cdot, \cdot)$, положив $(e_1, e_1) = (e_2, e_2) = 0$ и $(e_1, e_2) = -(e_2, e_1) = 1$. Матрица формы

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

Если X – невырожденное линейное преобразование, сохраняющее форму $(\cdot, \cdot)$, то, переходя к его матричной записи и отождествляя X с невырожденной матрицей размера 2×2 над F_p , получаем $XTX^t = T$. Множество всех таких невырожденных матриц над F_p есть группа $Sp(2, p)$ порядка $p(p^2 - 1)$ (изоморфная группе $SL(2, p)$).

Так как $\mathfrak{U}$ порождается элементами $E_x = P_1$ и $\Gamma(\sigma_0) = P_2$ порядка p , для которых $[P_1, P_2] = Z \in Z(\mathfrak{U})^\sharp$, и для любого внешнего автоморфизма ψ группы $\mathfrak{U}$ выполнено:

- а) ψ индуцирует автоморфизм группы $\mathfrak{U}/Z(\mathfrak{U})$;
- б) $[P_1, P_2]^\psi = [P_1^\psi, P_2^\psi]$;
- в) $[P_1, P_2] = [P_2, P_1]^{-1} = Z \in Z(\mathfrak{U}) \subseteq F_p$,

то отсюда следует, что $G/O_p(G)C_G(O_p(G)) = G/\mathfrak{U}C$ вкладывается в группу $Sp(2, p)$. Учитывая теорему 1 [1], заключаем, что $G/\mathfrak{U}C \cong Sp(2, p)$. Применяя леммы 2 и 3, получаем $G/\mathfrak{U} \cong Sp(2, p) \times C$, где $C \cong \mathbb{Z}_4$ при $p \equiv 3 \pmod{4}$ и $C \cong \mathbb{Z}_2$ при $p \equiv 1 \pmod{4}$. Пусть $\bar{\tau}$ – единственная инволюция группы $G'/\mathfrak{U}$ и $\mathfrak{P}$ – полный прообраз в G подгруппы $\langle \bar{\tau} \rangle$. Применяя аргумент Фратини, заключаем, что $G = \mathfrak{P}C_G(\tau)$ для некоторой инволюции $\tau \in \mathcal{P}$. Применяя теорему Грюна о перемещении [3, с. 238], имеем $G = \mathfrak{U}\mathfrak{Y}$ для некоторой подгруппы $\mathfrak{Y}$ с $\mathfrak{Y} \cap \mathfrak{U} = 1$. Отсюда следует заключение теоремы В.

§ 2. Вспомогательные результаты

Для удобства читателя воспроизведем здесь определение группы Сидельникова $\Sigma_{n,p}$ из [1]. Пусть $D = (d_{ij})$ – матрица размера $n \times n$ с коэффициентами из поля $GF(p) = F_p$. Через $\ker(D)$ будем обозначать пространство всех векторов-строк $x \in F_p^n$, для которых $xD = 0$. Через $\text{Im}(D)$ обозначается пространство всех векторов-строк $y \in F_p^n$ вида $y = xD$. Пусть $D, R, T \in M_n(F_p)$ и $m = \dim \ker(T) = \dim \ker(R)$. Матрицу $C(D, R, T) = C_n(D, R, T) = (v_{a,b})$, $a, b \in F_p^n$, размера $p^n \times p^n$ с комплексными элементами определим соотношениями $v_{a,b} = 0$, если $aR - bT \neq 0$ и

$$v_{a,b} = p^{-m/2} \exp(2\pi i u D b^t / p), \quad \text{если } aR - bT = 0,$$

где в выражении $\exp(2\pi i a / p)$ элементы $a \in F_p$ трактуются как целые положительные числа. Пусть $U_n = \{\alpha_1, \alpha_2, \dots, \alpha_N\} = F_p^n$ ($N = p^n$) – множество всех элементов пространства F_p^n , записанное в каком-либо порядке. Нумерацию строк и столбцов матрицы $C(D, R, T)$ зададим с помощью множества U_n так, что элемент, стоящий на пересечении i -й строки и j -го столбца равен элементу v_{α_i, α_j} . Будем обозначать через $B(D, R, T)$ матрицу $C(D, R, T)$, у которой тройка матриц D, R, T удовлетворяет следующим двум условиям:

- а. $\text{Im}(R) = \text{Im}(T)$.
- б. Билинейная форма xDy^t при $m > 0$ является невырожденной на $\ker(R) \times \ker(T)$, т.е. для любого ненулевого $x_0 \in \ker(R)$ найдется такой $y_0 \in \ker(T)$, что $x_0 D y_0^t \neq 0$.

В случае выполнения указанных условий матрица $C(D, R, T)$ является унитарной (доказательство см. в [1]).

Матрица Адамара (обобщенная при $p > 2$) $A = A_n = p^{-n/2}(\exp(2\pi i \langle a, b \rangle / p))$, $a, b \in F_p^n$, совпадает с матрицей $B(I, 0, 0)$, а единичная матрица из $M_{p^n}(\mathbb{C})$ – с матрицей $B(0, I, I)$, где I – единичная матрица из $M_n(F_p)$, $\langle a, b \rangle$ – скалярное произведение в F_p^n . При $D = I$, $n > m > 0$ матрица $B(D, R, R)$ (при соответствующей нумерации ее строк и столбцов) представляет собой клеточно-диагональную матрицу, на диагонали которой расположены матрицы Адамара размера $p^m \times p^m$, умноженные на числа $\exp(2\pi i f(a)/p)$, где $f \in F_p[x]$ – многочлен второй степени от n переменных с коэффициентами из поля F_p .

ЛЕММА 5. Пусть R и T – квадратные $n \times n$ -матрицы с коэффициентами из поля F . Через $\text{Im } R$ обозначим множество векторов-строк $y \in F^n$ вида $y = xR$. Тогда $\text{Im } R = \text{Im } T$ в том и только том случае, когда существует такая невырожденная матрица S , что $T = SR$.

ДОКАЗАТЕЛЬСТВО. Пусть $T = SR$, где S – невырожденная матрица. Если $y = xR$, то из $R = S^{-1}T$ следует, что для $z = xS^{-1}$ получаем $y = xS^{-1}T = zT \in \text{Im } T$. Поэтому $\text{Im } R \subseteq \text{Im } T$. Если $u \in \text{Im } T$, то $u = vT$ для некоторого v и поэтому $u = (vS)R \in \text{Im } R$. Следовательно, $\text{Im } R = \text{Im } T$. Докажем теперь, что если $\text{Im } R = \text{Im } T$, то $T = SR$ для некоторой невырожденной матрицы S . Не ограничивая общности, можно считать, что первые k строк матриц T и R являются максимальными линейно независимыми подсистемами строк этих матриц ($k = \dim \text{Im } R = \dim \text{Im } T$). В противном случае вместо матриц R и T можно рассмотреть матрицы PR и QT , где P и Q – подходящие матрицы-перестановки. Пусть $\tilde{R}$ и $\tilde{T}$ – подматрицы матриц R и T , состоящие из первых k строк матриц R и T соответственно. Тогда строки матриц $\tilde{R}$ и $\tilde{T}$ являются базисами $\text{Im } R$ и $\text{Im } T$ соответственно. Так как $\text{Im } R = \text{Im } T$, то существует $k \times k$ -матрица A , для которой $A\tilde{R} = \tilde{T}$. Так как $k = \text{rang } \tilde{T} = \text{rang } A\tilde{R} \leq \text{rang } A$, то A – невырожденная матрица. Минор k -го порядка матрицы $\tilde{R}$, отличный от нуля, можно считать расположенным в левом углу матрицы $\tilde{R}$. В противном случае вместо матриц $\tilde{R}$ и $\tilde{T}$ можно рассмотреть матрицы $\tilde{R}P$ и $\tilde{T}P$, где P – подходящая матрица-перестановка (размера $n \times n$).

Пусть $R_1, R_2, \dots, R_k$ – первые k строк матрицы R , $T_1, T_2, \dots, T_k$ – первые k строк матрицы T . Тогда

$$T_i = \sum_{j=1}^k \alpha_{ij} R_j, \quad \text{где } (\alpha_{ij}) = A.$$

Понятно, что все остальные строки матриц T и R линейно выражаются через $R_1, \dots, R_k$:

$$\begin{aligned} \lambda_{1i} R_1 + \lambda_{2i} R_2 + \dots + \lambda_{ki} R_k &= R_{k+i}, \\ \mu_{1i} R_1 + \mu_{2i} R_2 + \dots + \mu_{ki} R_k &= T_{k+i}, \quad i = 1, \dots, n-k. \end{aligned}$$

Отсюда

$$(\lambda_{1i} + \mu_{1i}) R_1 + \dots + (\lambda_{ki} + \mu_{ki}) R_k - R_{k+i} = T_{k+i}.$$

Поэтому существует матрица

$$S = \begin{pmatrix} A & 0 \\ B & -I \end{pmatrix}, \quad B = (\lambda_{ji} + \mu_{ji}), \quad j = 1, \dots, k, \quad i = 1, \dots, n-k,$$

такая, что $SR = T$. Так как A невырожденная, то и S невырожденная.

Пусть $f(x_1, \dots, x_n)$ – линейная функция и E_f – соответствующая ей матрица, определенная в [1]. Подгруппу, порожденную всеми такими E_f и всеми матрицами Γ_α ($\alpha(x) = x + \alpha$), обозначим через $\mathfrak{U}$. Так как $\mathfrak{U}_1 = \langle \Gamma_\alpha \mid \alpha(x) = x + \alpha \rangle$ оставляет на месте подгруппу $\mathfrak{E}_1$, порожденную всеми E_f , где f – линейная функция, то из [1] следует, что $\mathfrak{U}$ – группа порядка p^{2n+1} . Подгруппа $\mathfrak{U}$ будет играть весьма важную роль в определении строения группы $G = \Sigma_{n,p}$.

ЛЕММА 6. $\mathfrak{U}$ – экстраспециальная группа, нормальная в $G = \Sigma_{n,p}$, причем $\mathfrak{U} = \mathfrak{E}_1 \rtimes \mathfrak{U}_1$ и $C_G(\mathfrak{U}) \subseteq \mathfrak{U}Z(G)$. В частности, $G/\mathfrak{U}C_G(\mathfrak{U}) \subseteq Sp(2n, p)$ при $p > 2$ и $G/\mathfrak{U} \subseteq O^+(2n, 2)$ при $p = 2$. При $p > 2$ $Z(G) \cong Z(\mathfrak{U}) \times \mathbb{Z}_m$, где $m = 2$ при $p \equiv 1 \pmod{4}$ и $m = 4$ при $p \equiv 3 \pmod{4}$.

Экстраспециальность $\mathfrak{U}$ и факторизация $\mathfrak{U} = \mathfrak{E}_1 \rtimes \mathfrak{U}_1$ проверяются непосредственно при помощи вычислений, использующих формулу (12) из [1].

Докажем нормальность $\mathfrak{U}$. В силу определения G достаточно проверить, что $AYA^{-1} \in \mathfrak{U}$ для любой матрицы A , являющейся матрицей $B(D, R, T)$ (в смысле определения из [1]), и для любой $Y \in \mathfrak{U}$. При этом из $A^{-1}Y_1Y_2A = A^{-1}Y_1AA^{-1}Y_2A$ следует, что достаточно рассмотреть по отдельности два случая

- (а) $Y \in \mathfrak{E}_1$, т.е. $Y = E_f$ для $\deg f \leq 1$,
- (б) $Y \in \mathfrak{U}_1$, т.е. $Y = \Gamma_\alpha$ для $\alpha(x) = x + \alpha$.

Обозначим через μ_{ab} элемент матрицы AYA^{-1} , отвечающий строкам a, b в пространстве $GF(p)^n$. Пусть $m = \dim \ker R = \dim \ker T$. Элементы матрицы $A = (v_{ab})$ в этом случае задаются формулами (11) из [1]. Мы перепишем их здесь, принимая полезное и в дальнейшем обозначение $\omega^x = \exp \omega(x)$.

$$\begin{aligned} v_{ab} &= 0, \quad \text{если } aR - bT \neq 0, \\ v_{ab} &= p^{-m/2} \exp \omega(aDb^t), \quad \text{если } aR - bT = 0. \end{aligned}$$

Напомним, что ω – первообразный корень p -й степени из единицы.

- (а) Пусть $Y = E_f$ с $\deg f \leq 1$,

$$\mu_{ab} = p^{-m} \sum_x \exp \omega(aDx^t + f(x) - bDx^t), \quad (1)$$

где суммирование проводится по тем x , для которых

$$aR - xT = 0, \quad bR - xT = 0. \quad (2)$$

Слегка упрощая формулу (1), получаем:

$$\mu_{ab} = p^{-m} \sum_x \exp \omega((a-b)Dx^t + f(x)). \quad (3)$$

Предположим, что $\mu_{ab} \neq 0$ для некоторого b . Тогда существует решение x_0 системы уравнений (2) и $aR - x_0T = bR - x_0T$, откуда $(a-b)R = 0$, т.е. $a-b = d \in \ker R$. Если y – любое другое решение системы (2), то $y = x_0 + w$, где $w \in \ker T = L$. По лемме 5 существует такая невырожденная матрица S , что $R = ST$. Отсюда ясно,

что $x_0 = aS$ является решением системы (2) при условии, что $a - b = d \in \ker R$. Теперь соотношение (3) можно переписать в виде

$$\begin{aligned}\mu_{ab} &= p^{-m} \sum_{x \in L} \exp \omega(dD(x_0 + w)^t + f(x_0 + w)) \\ &= p^{-m} \exp \omega(dDx_0^t + f(x_0)) \sum_{x \in L} \exp \omega(dDw^t + f(w)).\end{aligned}\quad (4)$$

Очевидно, что $\mu_{ab} \neq 0$ только в том случае, когда $dDw^t + f(w) = 0$ для всех $w \in L$. Если $d_1 \in \ker R$ такой элемент, что $d_1Dw^t + f(w) = 0$ для всех $w \in L$, то $(d - d_1)Dw^t = 0$ для всех $w \in L$. Поэтому из невырожденности на $\ker R \times \ker T$ формы xDy^t [1] следует, что $d = d_1$. Таким образом, элемент $d = a - b$ такой, что $\mu_{ab} \neq 0$, определяется однозначно из условия $0 = dDw^t + f(w)$ при всех $w \in L$. В частности, в строке, отвечающей элементу a , имеется единственный элемент $b = a - d$, для которого $\mu_{ab} \neq 0$. При этом

$$\mu_{ab} = \exp \omega(dDx_0^t + f(x_0)) = \exp \omega(dDS^t a^t + f(S^t a^t)).\quad (5)$$

Очевидно, что $\psi(a) = dDS^t a^t + f(S^t a^t)$ — линейная функция от a . Поэтому $AYA^{-1} = E_\psi \Gamma_\sigma$, где $\sigma(x) = x - d$.

(b) $Y \in \mathfrak{U}_1$, т.е. $Y = \Gamma_\alpha$, где $\alpha(x) = x + \alpha$.

Вычислим элемент β_{ab} матрицы AYA^{-1} в предположении, что матрица A задается, как и в случае (a).

$$\beta_{ab} = p^{-m} \sum_x \exp \omega(aDx^t - bD(x + \alpha)^t).\quad (6)$$

Суммирование в (6) проводится по всем x , для которых

$$aR - xT = 0, \quad bR - (x + \alpha)T = 0.\quad (7)$$

Предположим, что $\beta_{ab} \neq 0$. Тогда система (7) имеет хотя бы одно решение x_0 . По лемме 5 $T = SR$ для некоторой невырожденной матрицы S . Поэтому

$$aR - x_0T = 0, \quad bR - x_0T - \alpha SR = 0.$$

Отсюда $bR - aR - \alpha SR = 0$ и $a - b + \alpha S \in \ker R$. С другой стороны, если y — любое решение системы (7), то $y = x_0 + w$, где $w \in \ker T = L$. В качестве x_0 можно взять aS^{-1} . Пусть $d = a - b$. Тогда соотношение (6) переписывается в виде

$$\beta_{ab} = p^{-m} \exp \omega(bDa^t + (a - b)Dx_0^t) \sum_{w \in L} \exp \omega(dDw^t).\quad (8)$$

Заметим, что $\beta_{ab} \neq 0$ только в том случае, когда $dDw^t = 0$ на $w \in L$. Предположим, что также $\beta_{ac} \neq 0$. Тогда $a - c + \alpha S \in \ker R$ по тем же соображениям, что и выше. При этом $d_1 = a - c$ удовлетворяет условию $d_1Dw^t = 0$ на L . Но тогда $b - c = (a - c) + \alpha S - ((a - b) + \alpha S) \in \ker R$ и $(b - c)Dw^t = d_1Dw^t - dDw^t$ обращается в нуль на L . Так как $b - c \in \ker R$, то из условий на D (см. § 4 из [1])

следует, что $b - c = 0$, т.е. $b = c$. Таким образом, существует единственное значение $d \in GF(p)^n$, для которого функция dDw^t обращается в нуль на всех $w \in L$.

Но тогда, как и выше, $b = a - d$ и элемент

$$\beta_{ab} = \exp \omega(bD\alpha^t + (a - b)Dx_0^t).$$

Учитывая, что $b = a - d$, $x_0 = aS^{-1}$, получаем

$$\begin{aligned} \beta_{ab} &= \exp \omega((a - d)D\alpha^t + dD(aS^{-1})^t) \\ &= \exp \omega((a - d)D\alpha^t + dDS^{-t}a^t) = \exp \omega(\psi(a)), \end{aligned}$$

где $\psi(a)$ — многочлен от a степени не выше единицы. Отсюда $AY A^{-1} = E_\psi \Gamma_d$, что и доказывает нормальность подгруппы $\mathfrak{U}$.

Покажем теперь, что централизатор $C_G(\mathfrak{U})$ состоит из скалярных матриц. Для этого достаточно установить неприводимость естественного матричного представления $\mathfrak{U}$. Действительно, у экстраспециальной группы $\mathfrak{U}$ порядка p^{2n+1} имеется ровно p^{2n} неприводимых представлений степени 1, содержащих в своем ядре $Z(\mathfrak{U})$, и $p - 1$ представление степени p^n . Отсюда следует неприводимость рассматриваемого представления. Таким образом, уже множество матриц, централизующих $\mathfrak{U}$, состоит из скалярных матриц.

Так как любая матрица из $\Sigma_{n,p}$ имеет вид $\pm iE_f B E_g$, где f и g — многочлены степени ≤ 2 [1], то матрица $\lambda I \in \Sigma_{n,p}$ лишь в том случае, когда B — диагональная $B(D, R, T)$ матрица. Коэффициенты последней — корни p -ой степени из единицы. Поэтому $\lambda I \in Z(G)$ лишь в том случае, когда $\lambda = i^l \omega^k$ для подходящих l, k . При этом $\lambda = \pm i \omega^k$ для $p \equiv 3 \pmod{4}$ и $\lambda = \pm \omega^k$ для $p \equiv 1 \pmod{4}$. В случае $p = 2$ $\lambda I \in \mathfrak{E}_1 \subseteq \mathfrak{U}$. В других случаях $Z(\mathfrak{U})\mathfrak{U} = \mathfrak{U} \times \mathbb{Z}_m$, где $m = 4$ при $p \equiv 3 \pmod{4}$ и $m = 2$ при $p \equiv 1 \pmod{4}$.

Если $p > 2$, то, полагая $\langle x, y \rangle = [x, y] \in \mathbb{Z}_{p,+}$ для элементов x и y из $\mathfrak{U}/Z(\mathfrak{U})$, получаем кососимметричную билинейную форму на $\mathfrak{U}/Z(\mathfrak{U})$, и группа $G/C_G(\mathfrak{U})\mathfrak{U}$ — группа внешних автоморфизмов $\mathfrak{U}$, сохраняющая эту форму. Поэтому

$$G/C_G(\mathfrak{U})\mathfrak{U} \subseteq Sp(2n, p) \quad \text{при } p > 2.$$

Если $p = 2$, то положим $Q(x) = x^2 \in \mathbb{Z}_{2,+}$ для любого $x \in \mathfrak{U}/Z(\mathfrak{U})$. В аддитивной записи имеем $Q(x + y) = Q(x) + Q(y) + \langle x, y \rangle$, где $\langle x, y \rangle = [x, y]$ — коммутатор элементов x и y . Квадратичная форма на ортогональном пространстве $\mathfrak{U}/Z(\mathfrak{U})$ может быть записана в виде $x_1 x_{-1} + x_2 x_{-2} + \dots + x_{n-1} x_{-(n-1)} + x_n^2 + x_n x_{-n} + x_{-n}^2$, что следует из строения группы $\mathfrak{U} = \mathfrak{E}_1 \rtimes \mathfrak{U}_1$. Поэтому $G/C_G(\mathfrak{U})\mathfrak{U} = G/\mathfrak{U}$ вкладывается в $O^+(2n, n)$.

Для дальнейшего полезно следующее замечание (см. § 7 из [1]). Пусть σ — линейное преобразование $GF(p)^n$, ставящее в соответствие каждому $x \in GF(p)^n$ элемент $y = \sigma(x) = xS$, где S — невырожденная матрица из $GL(n, p)$. Понятно, что множество всех матриц Γ_σ , отвечающих преобразованиям σ указанного вида, является подгруппой группы $G = \Sigma_{n,p}$. Обозначим ее через $\mathfrak{K}$. Очевидно, что $\mathfrak{K} \cong GL(n, p)$. Пусть $\mathfrak{L} = \langle E_f \mid \deg f \leq 2 \rangle$. Тогда $\mathfrak{H} = \mathfrak{L} \rtimes \mathfrak{K}$ является p -локальной подгруппой группы $G = \Sigma_{n,p}$ (нормализатором нетривиальной p -подгруппы).

ЛЕММА 7. Если $p > 2$, то порядок силовской p -подгруппы группы G равен p^{n^2+2n+1} и порядок силовской p -подгруппы группы $G/\mathfrak{U}$ равен p^{n^2} . Если $p = 2$, то порядок силовской 2-подгруппы группы G делится на 2^{n^2+n+1} и делит 2^{n^2+n+2} .

ДОКАЗАТЕЛЬСТВО. Рассматривая формулы для порядка группы G (теорема 6 из [1]), легко усмотреть, что наивысшая степень числа p , делящая порядок группы G при $p > 2$, делится на $p^{(n+1)^2}$. Так как порядок силовской p -подгруппы группы $Sp(2n, p)$ равен p^{n^2} и $|\mathfrak{U}| = p^{2n+1}$, то отсюда получаем заключение леммы 7 для $p > 2$. Если $p = 2$, то из формул (38), (39) и леммы 6 в [1] следует только, что наивысшая степень двойки, делящая $|G|$, делится на 2^{n^2+n+1} . Так как $G/\mathfrak{U}$ — подгруппа группы $O^+(2n, 2)$, то и в этом случае получаем заключение.

§ 3. Доказательство теоремы А

Для доказательства теоремы необходима некоторая дополнительная информация о группах $Sp(2n, p)$ и $\Omega^+(2n, 2)$, связанных с описываемой ситуацией. Группа $X = Sp(2n, p)(\Omega^+(2n, 2))$ является группой лиевского типа, с которой ассоциирован граф Дынкина на n вершинах:

$$\overset{\circ}{1} - \overset{\circ}{2} - \overset{\circ}{3} - \cdots - \overset{\circ}{n-1} = \overset{\circ}{n}$$

Соответственно

$$\overset{\circ}{1} - \overset{\circ}{2} - \overset{\circ}{3} - \cdots - \overset{\circ}{n-2} - \overset{\circ}{n-1} \quad \begin{array}{c} \nearrow \\ \overset{\circ}{n} \end{array}$$

Если $X \cong \Omega^+(2n, 2)$, то $p = 2$. Силовская p -подгруппа группы X играет важную роль в объяснении строения группы X . Любая подгруппа группы X , содержащая нормализатор силовской p -подгруппы X , называется параболической подгруппой группы X . Любая p -локальная подгруппа группы X (нормализатор нетривиальной p -подгруппы группы X) содержится в максимальной параболической подгруппе [2]. Последние же легче изучать, используя информацию о них, заключенную в графе Дынкина. Имеется ровно n классов сопряженности максимальных параболических подгрупп группы X , занумерованных вершинами диаграммы Дынкина группы X . Если X_i — максимальная параболическая подгруппа группы X , то (см. лемму (2.2) из [2]) $X_i = (Q_i L_i)H$, где $Q_i = O_p(X_i)$, $Q_i L_i \triangleleft X_i$, H — абелева группа, а L_i — центральное произведение накрывающих подгрупп для групп, отвечающих связным компонентам графа Дынкина, получающегося из графа X удалением вершины i вместе с инцидентными ей ребрами. Если вспомнить, что граф Дынкина $\overset{\circ}{0} - \overset{\circ}{1} - \overset{\circ}{2} - \cdots - \overset{\circ}{n}$ на k вершинах отвечает группе $PSL(k+1, p)$, то понятно устройство “осколков”, отвечающих полученной диаграмме.

Например, для диаграммы с 6 вершинами для группы $X \cong PSp(12, p)$:

$$\overset{\circ}{1} - \overset{\circ}{2} - \overset{\circ}{3} - \overset{\circ}{4} - \overset{\circ}{5} = \overset{\circ}{6}$$

Подгруппа X_3 имеет диаграмму:

$$\begin{array}{c} \circ \\ 1 \end{array} - \begin{array}{c} \circ \\ 2 \end{array} \quad \begin{array}{c} \circ \\ 4 \end{array} - \begin{array}{c} \circ \\ 5 \end{array} = \begin{array}{c} \circ \\ 6 \end{array}$$

Отсюда $X_3 = Q_3 L_3 H$, где $Q_3 = O_p(X_3)$, а L_3 – центральное произведение накрывающих подгрупп для групп $PSL(3, p)$ и $PSp(6, p)$. При этом $X'_3 \leq Q_3 L_3$. Более подробные сведения можно найти в [2], [4].

ЛЕММА 8. Если $p > 2$, $n > 2$, то $G/\mathcal{MC}_G(\mathfrak{U}) \cong Sp(2n, p)$.

ДОКАЗАТЕЛЬСТВО. Пусть $\overline{\mathfrak{H}} = \overline{\mathfrak{L}}\overline{\mathfrak{K}}$ – образ подгруппы $\mathfrak{H}$ в $\overline{G} = G/\mathcal{MC}_G(\mathfrak{U})$. В силу лемм 6 и 7 $\overline{\mathfrak{H}}$ содержится в некоторой максимальной параболической подгруппе X_i группы $X \cong Sp(2n, p)$. Так как $X_i = Q_i(L_i H)$, где $Q_i = O_p(X_i)$, и $\overline{\mathfrak{H}}$ содержит силовскую p -подгруппу группы X , то ясно, что $Q_i \leq \overline{\mathfrak{L}} = O_p(\overline{\mathfrak{H}})$ и $\overline{\mathfrak{H}}/Q_i = \overline{\mathfrak{L}}\overline{\mathfrak{K}}/Q_i \cong (\overline{\mathfrak{L}}/Q_i)\overline{\mathfrak{K}}$ содержится в качестве подгруппы группы L_i . Группа L_i в данном случае может отвечать только одной из следующих диаграмм:

$$\begin{array}{c} 1 \\ * \end{array} - \begin{array}{c} 2 \\ \circ \end{array} - \begin{array}{c} 3 \\ \circ \end{array} - \dots - \begin{array}{c} n-1 \\ \circ \end{array} = \begin{array}{c} n \\ \circ \end{array} \quad \begin{array}{c} 1 \\ \circ \end{array} - \begin{array}{c} 2 \\ \circ \end{array} - \begin{array}{c} 3 \\ \circ \end{array} - \dots - \begin{array}{c} n-1 \\ \circ \end{array} = \begin{array}{c} n \\ * \end{array}$$

В первом случае $L_i/Z(L_i) \cong PSp(2(n-1), 2)$, а во втором $L_i/Z(L_i) \cong PSL(n, p)$. Согласно предложению (3.2) из [2], в первом случае Q_i – экстраспециальная группа порядка p^{2n-1} . Однако $\mathfrak{L}$ – абелева группа, как подгруппа, состоящая из диагональных матриц. Так как $Q_i \subseteq \overline{\mathfrak{L}}$, то она также должна быть абелевой. Последнее возможно лишь при $n = 1$.

Следовательно, $X_i = X_n = (Q_n L_n)H$. В этом случае $\overline{\mathfrak{H}} = \overline{\mathfrak{L}}\overline{\mathfrak{K}}$ является максимальной параболической подгруппой группы $Sp(2n, p)$. Так как $\mathfrak{H}$ не нормальна в $G = \Sigma_{n,p}$, то отсюда следует заключение леммы.

ЛЕММА 9. Группа $X \cong Sp(2n-2, 2)$ не содержит подгрупп, изоморфных $GL(n, 2)$ при $n \geq 5$.

Покажем сначала, что если n нечетно, то при $n \geq 3$ $|GL(n, 2)|$ не делит $|Sp(2n-2, 2)|$. Действительно, $2^n - 1$ делит $|GL(n, 2)|$ и по теореме Жигмонди [5] существует такое простое число r , что r делит $2^n - 1$ и не делит $2^k - 1$ для любого $0 < k < n$. Так как

$$|Sp(2n-2, 2)| = 2^{(n-1)^2} \prod_{i=2}^{n-1} (2^{2i} - 1),$$

то из нечетности n следует, что $(2^n - 1, 2^{2i} - 1) = 2^{(n, 2i)} - 1 = 2^{(n, i)} - 1 < 2^n - 1$ при $i \leq n-1$ и r не делит $|Sp(2n-2, 2)|$.

Покажем теперь, что если $Sp(2n-2, 2)$ содержит циклическую подгруппу порядка $2^n - 1$, то n является степенью двойки.

Как показано выше, $n = 2k$. Так как $(2^n - 1, 2^{2i} - 1) = 2^{2(i, k)} - 1$, то простое число Жигмонди r , делящее $2^n - 1$ и не делящее $2^i - 1$ при $0 < i < n$, не будет делить $2^{2i} - 1$ при $i \neq k, 0 < i < n$. Поэтому элемент порядка r содержится в $Sp(2k, 2)$ и в подходящем базисе может быть записан в виде

$$y = \begin{pmatrix} A & 0 \\ 0 & I_{2k-2} \end{pmatrix},$$

где A – симплектическая $2k \times 2k$ -матрица, а I_{2k-2} – единичная матрица. Не ограничивая общности, можно считать, что y сохраняет форму с матрицей

$$\Phi = \begin{pmatrix} 0 & I_k & 0 & 0 \\ I_k & 0 & 0 & 0 \\ 0 & 0 & 0 & I_{k-1} \\ 0 & 0 & I_{k-1} & 0 \end{pmatrix},$$

где I_m – единичная $m \times m$ -матрица. Если $H = GL(n, 2)$, то $|C_H(A)| = 2^n - 1$ (напомним, что $n = 2k$) и $|C_X(A)| = |Sp(2k - 2, 2)|(2^k + 1)$.

Так как y содержится в циклической подгруппе порядка $2^{2k} - 1 = (2^k - 1)(2^k + 1)$, то группа $Sp(2k - 2, 2)$ должна содержать подгруппу порядка $2^k - 1$. Применяя предположение индукции, замечаем, что k – степень двойки. Но тогда и $n = 2k$ – степень двойки.

Предположим теперь, что $GL(n, 2)$ содержится в $Sp(2n - 2, 2)$ для некоторого $n \geq 5$. Из доказанного выше следует, что $n \geq 8$.

Группа $GL(n, 2)$ содержит подгруппу $\mathbb{Z}_{2^{n-3}-1} \times \mathbb{Z}_7$. Пусть r – простое число, делящее $2^{n-3} - 1$ и не делящее $2^i - 1$ при $0 < i < n - 3$ (существует по теореме Жигмонди). Так как n – степень двойки, то $n - 3$ – нечетное число. Поэтому $(2^{n-3} - 1, 2^{2^i} - 1) = 2^{(i, n-3)} - 1$ и поэтому существует единственный сомножитель в разложении

$$|Sp(2n - 2, 2)| = 2^{(n-1)^2} \prod_{i=1}^{n-1} (2^{2^i} - 1),$$

для которого r делит $2^{2^i} - 1$. Этот сомножитель $2^{2^{n-6}} - 1$. Не ограничивая общности, можно считать, что в подходящем базисе элемент y порядка r может быть представлен в виде

$$y = \begin{pmatrix} B & 0 \\ 0 & I_4 \end{pmatrix},$$

где B – симплектическая матрица размера $2n - 6 \times 2n - 6$, а I_4 – единичная 4×4 -матрица. При этом для $M = Sp(2n - 6, 2)$ выполнено $|C_M(B)| = 2^{n-3} - 1$ и $|C_X(y)| = (2^{n-3} - 1)|Sp(4, 2)|$. Так как 7 не делит $|Sp(4, 2)|$, то получаем противоречие.

Заметим, что случаи $n = 2$ и $n = 4$ являются исключениями, ибо $Sp(2, 2) \cong GL(2, 2)$ и $Sp(6, 2)$ содержит $A_8 \cong GL(4, 2)$.

ЛЕММА 10. Если $n \geq 5$, то $\Sigma_{n,2}/\mathfrak{U}$ изоморфна $O^+(2n, 2)$.

Как и в доказательстве леммы 8, заключаем, что подгруппа $\overline{\mathfrak{H}} = \mathfrak{H}/\mathfrak{U}$ содержится в одной из максимальных параболических подгрупп группы $X = \Omega^+(2n, 2)$, отвечающих диаграммам для X_1, X_{n-1} или X_n .

В первом случае $X_1 = Q_1 L_1 H$, где $Q_1 \leq Q_2(X_1)$ и $L_1/Z(L_1) \cong O^+(2n - 2, 2)$. Так как $\overline{\mathfrak{H}}$ содержит подгруппу, изоморфную $GL(n, 2) = SL(n, 2)$, а $Q_1 L_1 = X'_1$ ее не содержит, то эта возможность исключена.

В оставшихся случаях $X_j = Q_j L_j H$, где $j > n - 2$, $L_j \cong GL(n, 2)$ и $\overline{\mathfrak{H}}$ – максимальная параболическая подгруппа простой группы $\Omega^+(2n, 2)$. Так как $\mathfrak{H} \neq \Sigma_{n,2}$, то в этом случае $\Sigma_{n,2}/\mathfrak{U}$ содержит подгруппу $\Omega^+(2n, 2)$, имеющую

индекс 2 в $O^+(2n, 2)$. Как показано в [1], группа $\Sigma_{n,2}/\mathfrak{U}$ содержит подгруппу индекса 2. Отсюда следует заключение леммы 10.

Теперь нетрудно закончить доказательство теоремы.

Используя рассуждения, аналогичные использованным при доказательстве теоремы В, находим, что при $p > 2$ и $n > 1$ $G = (\mathfrak{U} \rtimes Sp(2n, p)) \times \mathbb{Z}_m$, где $m = 2$ при $p \equiv 1 \pmod{4}$ и $m = 4$ при $p \equiv 3 \pmod{4}$. Если $p = 2$ и $n \geq 5$, то в силу леммы 10 получаем $G/O_2(G) \cong O^+(2n, 2)$. Если $p = 2$ и $n < 5$, то в [1] вычислены порядки групп $\Sigma_{n,2}$, откуда следует заключение теоремы и для этих случаев.

СЛЕДСТВИЕ С. Пусть $G = \Sigma_{n,p}$ — группа Сидельникова. Если $p > 2$ и $\Theta(p) = 2$ при $p \equiv 1 \pmod{4}$, $\Theta(p) = 4$ при $p \equiv 3 \pmod{4}$, то

$$|G| = \Theta(p)p^{n^2+2n+1}(p^2-1)(p^4-1)\cdots(p^{2n}-1).$$

Если $p = 2$, $n > 1$, то

$$|G| = 2^{n^2+n+2}(2^2-1)(2^4-1)\cdots(2^{2n-2}-1)(2^n-1).$$

Заметим, что в [1] вычислены аддитивные аналоги для порядков групп $\Sigma_{n,p}$. В качестве другого следствия приведем следующую комбинаторную формулу:

$$1 + \sum_{m=1}^n p^{\frac{m(m+1)}{2}} \frac{(p^n-1)\cdots(p^{n-m+1}-1)}{(p^m-1)\cdots(p-1)} = (p+1)(p^2+1)\cdots(p^n+1)$$

для нечетного p или:

$$1 + \sum_{m=1}^n \frac{(p^{n+1}-p)(p^{n+1}-p^2)\cdots(p^{n+1}-p^m)}{(p^m-1)(p^{m-1}-1)\cdots(p-1)} = (p+1)(p^2+1)\cdots(p^n+1).$$

Кажется правдоподобным, что она справедлива при замене p на любое число $x \neq 1$.

Автор выражает признательность В. М. Сидельникову и С. П. Стрункову за полезные обсуждения, способствовавшие улучшению статьи.

Список литературы

1. Сидельников В. М. Об одной матричной группе и кодах на евклидовой сфере // Проблемы передачи информации. 1997. Т. 33. № 1. С. 35–54.
2. Curtis C. W., Kantor W. M., Seitz G. M. The 2-transitive permutation representations of the finite Chevalley groups // Trans. Amer. Math. Soc. 1976. V. 218. P. 1–59.
3. Bourbaki N. Éléments de mathématique // Fasc. XXXIV. Groupes et algèbres de Lie. Chaps IV, V, VI: Groupes de Coxeter et systèmes de Tits. Groupes engendrés par des réflexions. Systèmes de racines. Paris: Hermann & Cie, 1968.
4. Холл М. Теория групп. М.: ИЛ, 1962.
5. Zsigmondy K. Zur Theorie der Potenzreste // Monatshefte Math. Phys. 1892. V. 3. P. 265–284.

Ярославский государственный
университет им. П. Г. Демидова

Поступила в редакцию
01.07.1997