

## SR-группы порядка $2^n p^m$ с диэдральной 2-силовской подгруппой

Янишевский В.В.

Ярославский государственный университет,  
150 000, Ярославль, Советская, 14  
e-mail: yvitaliy@rambler.ru,

получена 22 мая 2007

### Аннотация

Устанавливается строение SR-групп порядка  $2^n p^m$  с диэдральной 2-силовской подгруппой по модулю подгруппы Фраттини. Доказано, что если такая группа несверхразрешима, то  $p$  — простое число Мерсенна и данная группа имеет факторгруппу специального вида.

Рассматриваются только конечные группы. Обозначения, нуждающиеся в пояснении: через  $A \rtimes B$  обозначается полупрямое произведение подгрупп  $A$  и  $B$  с нормальной подгруппой  $A$ ;  $D_{2n}$  — диэдральная группа порядка  $2n$ ,  $n \geq 3$ ; через  $C_n$  и  $\langle x \rangle_n$  обозначается циклическая подгруппа порядка  $n$  (во втором обозначении  $x$  — образующая);  $E_{p^n}$  — элементарная абелева группа порядка  $p^n$ ;  $O_p(G)$  — наибольшая нормальная  $p$ -подгруппа в  $G$ ;  $O(G)$  — наибольшая нормальная подгруппа нечетного порядка в  $G$ ;  $S_n$  — симметрическая группа степени  $n$ ;  $C_G^*(g) := \{x \in G \mid g^x = g^{\pm 1}\}$  — расширенный централизатор элемента  $g$ ;  $G^\# := G \setminus \{1\}$ .

**Определение 1.** Конечная группа называется SR-группой, если она обладает следующими свойствами: 1) Любой элемент сопряжен со своим обратным и 2) В разложении тензорного произведения любых двух неприводимых представлений каждое неприводимое представление входит не более одного раза.

**Определение 2.** Пусть группа  $G$  изоморфна группе вида  $V \rtimes D_{2^n}$ , где  $V \cong E_{p^m}$  — минимальная нормальная подгруппа группы  $G$ , причем  $Z(G) = 1$ ,  $p > 2$ ,  $n \geq 3$ ,  $m \geq 1$ . Такую группу мы будем называть атомарной группой.

Главный результат настоящей работы:

**Теорема 1.** Пусть  $G$  — конечная несверхразрешимая SR-группа порядка  $2^n p^m$  с диэдральной 2-силовской подгруппой. Если  $\Phi(G) = 1$ , то либо  $G \cong E_{p^2} \rtimes D_{2^{q+1}}$  — атомарная SR-группа,  $p = 2^q - 1$  — простое число Мерсенна, либо  $G \cong S_4$  и  $p = 3$ .

Доказательство этой теоремы разбивается на несколько лемм. Сначала мы установим, что либо  $G \cong S_4$ , либо  $G$  является 2-нильпотентной. Далее, в случае 2-нильпотентности, доказывается существование у SR-группы  $G$  атомарной факторгруппы. В лемме 3 доказывается, что атомарная группа  $E_{p^m} \rtimes D_{2^n}$  является несверхразрешимой SR-группой, если и только если  $m = 2$ ,  $n = q + 1$ , где  $p = 2^q - 1$  — простое число Мерсенна. В лемме 4 доказывается, что группа  $(E_1 \times E_2) \rtimes D_{2^n}$ , где  $E_1 \times D_{2^n} \cong E_2 \times D_{2^n}$  — изоморфные атомарные SR-группы, не является SR-группой. Таким образом, минимального контрпримера к утверждению теоремы не существует, что завершает ее доказательство.

**Предложение 1.** Любая конечная SR-группа обладает следующими свойствами: 1) Факторгруппа SR-группы является SR-группой, 2) Центр SR-группы есть элементарная абелева 2-группа.

Доказательство. См. [1]. □

**Лемма 1.** Пусть  $G$  — SR-группа порядка  $2m$ , где  $m$  — нечетное число. Тогда она изоморфна обобщенно диэдральной группе.

Доказательство. Как известно, любая группа порядка  $|G| = 2m$  имеет вид  $A \rtimes \langle \tau \rangle$ , где  $|A| = m$ . По определению SR-группы любой ее элемент сопряжен с обратным, поэтому любой элемент из  $A$  инвертируется  $\tau$ . Пусть  $a \in C_A(\tau)$ , тогда  $\langle a \rangle \times \langle \tau \rangle$  является подгруппой в  $G$ . Из того что  $a$  сопряжено с  $a^{-1}$ , следует, что существует такой элемент  $y$ , что  $a^y = a^{-1}$ . Рассмотрим теперь множество  $C_G^*(a)$ . Очевидно, что  $C_G^*(a)$  — группа, и при этом  $|C_G^*(a) : C_G(a)| = 2$ . Но так как  $|C_G(a)|$  делится на 2, то тогда  $|C_G^*(a)|$  делится на 4. Откуда следует, что и  $|G|$  делится на 4. Значит,  $C_A(\tau) = \langle 1 \rangle$ . Учитывая, что  $A \cong [A, \tau] \times C_A(\tau)$ , получаем  $A \cong [A, \tau]$ . Итак,  $G \cong D(A)$  — обобщенно диэдральная группа. □

**Лемма 2.** Если  $G/O_3(G) \cong S_4$  и  $G$  — SR-группа, то  $O_3(G) = 1$ .

*Доказательство.* Предположим, что  $G$  — минимальный контрпример. В таком случае  $O_3(G)/\Phi(O_3(G))$  является элементарной абелевой группой. Если  $\Phi(O_3(G)) \neq 1$ , то по предположению о минимальности  $G/\Phi(O_3(G))$  не является  $SR$ -группой. Значит,  $\Phi(O_3(G)) = 1$ , откуда  $O_3(G)$  — элементарная абелева.

Покажем, что  $G = O_3(G) \rtimes S_4$ . Пусть  $T \triangleleft S_4$  — четверная группа Клейна,  $T \cong C_2 \times C_2$ . Обозначим через  $\bar{T}$  полный прообраз  $T \triangleleft S_4$ . По аргументу Фраттини  $G = \bar{T}N_G(S) = O_3(G)N_G(S)$ , где  $S \cong T$  — силовская 2-подгруппа группы  $\bar{T}$ . Отсюда  $N(S)/N(S) \cap O_3(G) \cong G/O_3(G) \cong S_4$ . Так как  $O_3(G)$  — абелева, то  $D = N(S) \cap O_3(G) \triangleleft N(S)$  и  $N(S) \cap O_3(G) \triangleleft O_3(G)$ , откуда  $D \triangleleft G$ . Если  $D \neq O_3(G)$ , то  $O_3(G)/D \neq 1$  и  $G/D$  не является  $SR$ -группой по предположению о минимальности. Значит,  $D = 1$  или  $D = O_3(G)$ . В первом случае  $G = O_3(G) \rtimes N_G(S)$ , где  $N_G(S) \cong S_4$ , а  $O_3(G)$  — элементарная абелева.

Рассмотрим случай, когда  $O_3(G) \leq N_G(S)$ . Группа  $G/O_2(G)$  имеет 2-силовскую подгруппу порядка 2 и является  $SR$ -группой порядка  $2 \cdot 3^l$ . Поэтому по лемме 1 она является обобщенно диэдральной группой и, стало быть, любая циклическая подгруппа порядка 3 из  $O_3(G)$  нормальна в  $G$ . Если  $|O_3(G)| \geq 9$ , то по минимальности контрпримера для  $x \in O_3(G) \setminus 1$ ,  $\langle x \rangle \triangleleft G$ ,  $G/\langle x \rangle$  имеем  $O_3(G) \neq \langle x \rangle$  и поэтому не является  $SR$ -группой. Значит,  $|O_3(G)| = 3$ . Итак,  $|G| = 3 \cdot 24 = 72$ .

Для поиска возможных контрпримеров использовалась система компьютерной алгебры GAP [2]. GAP содержит библиотеку `SmallGroups`, которая состоит из небольших, отсортированных по порядку конечных групп. Команда обращения к группе в этой библиотеке выглядит так: `G:=SmallGroup(m,n);`, где  $m$  — порядок группы, а  $n$  — ее номер среди групп порядка  $m$ . Команда `IdSmallGroup(G)`; возвращает порядок и номер группы  $G$  в виде  $[m,n]$ . Далее, группа  $G_{[m,n]}$  обозначает группу `SmallGroup(m,n)`.

Возвращаясь к возможному строению групп контрпримеров, замечаем, что имеются две возможности. Либо  $G = (\langle c \rangle_3 \times A_4) \rtimes \langle \tau \rangle_2$ , где  $\tau c \tau = c^{-1}$ ,  $A_4 \rtimes \langle \tau \rangle \cong S_4$ . В таком случае группа  $G$  имеет представление в виде

$$G_{[72,43]} = \langle a, b, c \mid a^3 = b^3 = c^4 = (ac)^2 = (bc)^2 = [a, b] = 1 \rangle.$$

Либо  $G = S \rtimes \langle b \rangle_9 \rtimes \langle \tau \rangle_2$ , где  $[b^3, S] = 1$ ,  $\tau^{-1}b\tau = b^{-1}$ . И в этом случае группа  $G$  задается следующим образом:

$$G_{[72,15]} = \langle a, b \mid a^9 = b^4 = (ab)^2 = (ab^{-1}a)^2 = 1 \rangle.$$

Теперь, с помощью команды `Display(CharacterTable(G));`, которая выводит таблицу характеров групп  $G$ , можно получить, что в обоих указанных выше случаях  $cd(G) = \{1, 1, 2, 2, 2, 2, 3, 3, 6\}$ , где  $cd(G)$  — множество степеней неприводимых характеров группы  $G$ . Отсюда ясно, что тензорный квадрат неприводимого характера степени 6 не может иметь в разложении на неприводимые характеры коэффициенты 0 или 1, а значит, обе группы не являются  $SR$ -группами.

Остается случай, когда  $O(G) = O_3(G)$  — элементарная абелева нециклическая группа. Имеем  $G = O_3(G) \rtimes K$ , где  $K \cong S_4$ , и  $O_3(G)$  — минимальная нормальная подгруппа. Отсюда  $C_G(K) = 1$  (иначе  $G/G'$  не элементарная абелева 2-группа). Таким образом,  $K$  действует неприводимо на  $V = O_3(G)$  как на векторном пространстве над  $GF(3)$ . Известно (см. [3], с. 604-605), что существуют ровно 2 неприводимых точных  $K$ -модуля, оба размерности 3. Несложный поиск в системе GAP приводит нас к следующим группам:

$$G_{[648,703]} = \langle a, b \mid a^3 = b^4 = (ab^2ab)^2 = (aba^{-1}ba^{-1}b^{-1})^2 = 1 \rangle,$$

$$G_{[648,704]} = \langle a, b \mid a^3 = b^4 = (ab)^4 = (ab^2)^3 = (ab^{-1})^6 = 1 \rangle.$$

С помощью GAP находим степени неприводимых характеров этих групп:  $cd(G_{[648,703]}) = \{1, 1, 2, 3, 3, 6, 6, 6, 6, 8, 8, 8, 12, 12\}$  и  $cd(G_{[648,704]}) = \{1, 1, 2, 3, 3, 4, 4, 4, 4, 6, 6, 6, 6, 8, 8, 12, 12\}$ . Отсюда, также рассмотрев тензорный квадрат любого неприводимого характера степени 12 этих групп, легко убедиться, что его разложение на неприводимые содержит коэффициенты, отличные от 0 и 1. То есть  $G_{[648,703]}$  и  $G_{[648,704]}$  не являются  $SR$ -группами. Лемма доказана.  $\square$

Введем обозначения: если  $G$  — группа и  $g \in G$ , то  $\sqrt{g}(M) = \{x \in M \subseteq G \mid x^2 = g\}$  (если  $M = G$ , то положим  $\sqrt{g} = \sqrt{g}(G)$ );  $|M|$  — число элементов множества  $M$ . Для доказательства остальных теорем нам потребуется следующее утверждение.

**Предложение 2.** *Конечная группа  $G$  является  $SR$ -группой тогда и только тогда, когда она обращает в равенство неравенство Вигнера:*

$$\sum_{g \in G} |\sqrt{g}|^3 \leq \sum_{g \in G} |C_G(g)|^2. \tag{1}$$

*Доказательство.* См. [4], §5.8.  $\square$

**Лемма 3.** Пусть  $G \cong E_{p^m} \rtimes D_{2^n}$  — атомарная группа. Группа  $G$  является несверхразрешимой SR-группой тогда и только тогда, когда  $m = 2$  и  $n = q + 1$ , где  $p = 2^q - 1$  — простое число Мерсенна.

*Доказательство.* Сначала покажем, что  $n \geq 3$ . Предположим, что  $G = V \rtimes D_4$ , где  $D_4 = C_2 \times C_2$  по определению. Тогда  $S = \langle \tau \rangle \times \langle \nu \rangle$  — 2-силовская подгруппа. Получаем, что  $\tau$  — оператор с минимальным многочленом  $x^2 - 1$ , корни которого  $+1$  и  $-1$  есть в любом поле. Тогда  $V = V_1 \times V_{-1}$ , где  $V_1 = \{v \mid v^\tau = v\}$  и  $V_{-1} = \{v \mid v^\tau = v^{-1}\}$ . Если  $v \in V_1$ , то  $v^{\nu\tau} = v^{\nu} = v^\nu$ . Отсюда  $V_1^\nu = V_1$ , т.е.  $V_1$  инвариантно относительно  $\nu$ . Аналогично получаем  $V_{-1}^\nu = V_{-1}$ . Это означает, что оба подпространства  $V_1, V_{-1}$  инвариантны. Если теперь  $S$  неприводима на  $V$ , то либо  $V = V_1$ , либо  $V = V_{-1}$ . Если  $V = V_1$ , то  $\tau$  централизует  $G = V \rtimes S$ , что не так, поскольку  $Z(G) = 1$  (иначе  $G$  сверхразрешима). Если  $V = V_{-1}$ , то аналогично для каждого  $w \in V$ ,  $w^\nu = -w$ , но тогда  $w^{\tau\nu} = w$ . Получаем, что  $\tau\nu = \mu \in Z(G)$ . Итак, в обоих случаях получаем, что группа  $G$  сверхразрешима, что противоречит условию теоремы. Значит,  $n \geq 3$ .

Пусть  $G = V \rtimes S$ , где  $G$  несверхразрешима и  $S = D_{2^n}$  действует неприводимо и точно на  $V$ ,  $n \geq 3$ , а  $S = \langle t \rangle_{2^{n-1}} \rtimes \langle \tau \rangle_2$ , где  $t^\tau = t^{-1}$ . При этом группа  $C_V(t)$  допустима относительно  $\tau$ , откуда  $C_V(t) = 1$ . Здесь возможны два случая. В первом, который мы будем называть неприводимым случаем,  $\langle t \rangle$  действует неприводимо на  $V$ . Во втором случае, который мы будем называть приводимым,  $V = V_0 \times V_0^\tau$ , где  $\langle t \rangle$  неприводима на  $V_0$ .

Докажем, что  $m$  четно. В неприводимом случае получаем, что  $\langle t \rangle \leq GL_m(p)$  и действует неприводимо на  $V$ . Получаем, что  $p^m - 1 \equiv 0 \pmod{2^{n-1}}$ , и в этом случае  $V \rtimes \langle t \rangle$  — группа Фробениуса. Так как  $t \in GL_m(p)$ , то линейная оболочка  $\langle t, t^2, \dots, t^{2^{n-1}} \rangle$  — конечное поле  $GF(p^m)$ , причем  $GF(p^m)^* = \langle x \rangle$ ,  $|x| = p^m - 1$ . В частности,  $2^{n-1} \mid p^m - 1$ . При этом неприводимость влечет утверждение  $2^{n-1} \mid p^m - 1$  и  $2^{n-1}$  не делит  $p^j - 1$  при  $1 \leq j < m$ . По теореме II.7.3 из [5]  $N_G(\langle t \rangle) = N_G(\langle x \rangle)$  и поэтому  $|N_G(\langle t \rangle)/C_G(\langle t \rangle)|$  делит  $m$ . Так как  $N_G(\langle t \rangle) = S$  и  $|S/\langle t \rangle| = 2$ , то  $2 \mid m$ . В частности,  $2^{n-1} \mid p^{2k} - 1 = (p^k - 1)(p^k + 1)$ . При этом  $2^{n-1}$  не делит  $p^k - 1$ . Так как  $(p^k - 1, p^k + 1) = 2$ , то отсюда следует, что  $2^{n-2} \mid p^k + 1$ . В приводимом случае,  $\langle t \rangle$  приводима на  $V$ . Тогда  $V = V_0 \times V_0^\tau$ , где  $V_0$  — неприводимый  $\langle t \rangle$ -модуль. Отсюда  $2^{n-1} \mid p^k - 1$  и  $m = 2k$ . В обоих случаях получаем, что  $m = 2k$ .

Покажем, что  $V \rtimes \langle t \rangle$  — группа Фробениуса. В неприводимом случае это очевидно. Пусть  $V_0$  — неприводимый подмодуль и  $V = V_0 \times V_0^\tau$ . Положим  $\nu = t^{2^{n-1}}$ . В этом случае,  $V_0 \rtimes \langle t \rangle$  и  $V_0^\tau \rtimes \langle t \rangle$  — группы Фробениуса. Если предположить, что  $C_{V_0}(\nu) \neq 1$  для некоторого  $v \in V$ , то и  $C_{V_0^\tau}(\nu) = C_{V_0}(\nu)^\tau \neq 1$ . Тогда  $Z(V \rtimes S) \neq 1$  — противоречие. Поэтому и в приводимом случае  $V \rtimes \langle t \rangle$  — группа Фробениуса.

Вычислим порядки централизаторов элементов группы  $G$ .

Порядок централизатора единичного элемента равен  $|C_G(1)| = |G| = 2^n p^{2k}$ . Причем, поскольку  $Z(G) = 1$ , то это единственный элемент с таким свойством.

Найдем число инволюций в  $G$  и порядки их централизаторов. Поскольку  $V \rtimes \langle t \rangle$  — группа Фробениуса, то все инволюции из  $V \rtimes \langle t \rangle$  сопряжены с инволюцией  $\nu$ , а их число равно  $p^m$ . Рассмотрим группу  $S = \langle t \rangle_{2^{n-1}} \rtimes \langle \tau \rangle_2$ . Если  $g \in S \setminus \langle t \rangle$ , то  $g = t^i \tau$ , для некоторого  $i$ . Имеем  $g^2 = (t^i \tau)^2 = 1$ ,  $|C_S(g)| = 4$ , число сопряженных с  $g$  равно  $2^n/4 = 2^{n-2}$ . Число элементов в  $S \setminus \langle t \rangle$  равно  $2^{n-1}$ . Число сопряженных инволюций в  $S$  с нецентральной инволюцией равно  $2^{n-2}$ . Отсюда есть два класса сопряженных инволюций в  $S \setminus \langle t \rangle$ . Значит, в группе  $G$  имеется три класса сопряженных инволюций:  $(\nu)^G, (\tau)^G, (t\tau)^G$ . Инволюции, сопряженные с  $\nu$ , мы будем называть центральными, а остальные — нецентральными. Найдем порядки централизаторов нецентральных инволюций. В самом деле, если  $w = v_1 v_2^\tau$  для  $v_1, v_2 \in V_0$ , то  $(v_1 v_2^\tau)^{t\tau} = v_1^{t\tau} v_2^{t\tau\tau} = v_1 v_2^\tau$ . Откуда из  $v_1^{t\tau} \in V_0^\tau$  и  $v_2^{t\tau\tau} \in V_0$  получаем  $v_1 = v_2^{t-1}$  и  $v_1^{t\tau} = v_2^\tau$ , т.е.  $v_2 = v_1^{t-1}$ . Поэтому  $C_V(t\tau) = \{v_1 v_1^{t-1\tau} \mid v_1 \in V_0\}$ . То есть  $|C_V(t\tau)| = p^k = |C_V(\tau)|$ . Итак,  $|C_G(\tau)| = |C_G(t\tau)| = 2^2 p^k$ , и  $|(t\tau)^G| = |(t\tau)^G| = 2^{n-2} p^k$ .

Найдем теперь порядки централизаторов элементов  $w \in V$ . Поскольку  $V \rtimes \langle t \rangle$  — группа Фробениуса, то для любого  $w \in V$ ,  $w^\nu = w^{-1}$ . Отсюда следует, что  $w^{t^i} \neq w$ , для любого  $i \neq 2^{n-2}$ ,  $1 \leq i < 2^{n-1}$ . Так как расширенный централизатор  $C_G^*(w)$  содержит  $\langle \tau_w \rangle$  в качестве 2-силовской подгруппы, то для элемента из  $w \in V^\sharp$  возможны два случая: 1) либо существует (с точностью до сопряженности в  $C_G^*(w)$ ) единственная инволюция  $\tau_w$ , которая его централизует, 2) либо  $w^\tau \neq w$  для любой нецентральной инволюции. Случай, когда элемент  $w \in V$  централизуется двумя и более не сопряженными нецентральными инволюциями, например  $\tau_1, \tau_2$ , невозможен, так как  $C_G(w) = V \rtimes \langle \tau_1, \tau_2 \rangle$ , откуда  $\nu \in C_G(w)$ . Противоречие. Поскольку  $C_V(w) = V$ , то для случая 1) получаем, что  $|C_G(w)| = 2p^{2k}$ , а для случая 2), что  $|C_G(w)| = p^{2k}$ . Как было сказано,  $|C_G(\tau)| = 2^2 p^k$ , что означает существование множества  $\{w \in V \mid w^\tau = w\} = p^k$ . Для этих элементов  $w$  выполняется  $|C_G(w)| = 2p^{2k}$ , поскольку их централизует любой элемент из  $V$ , а также инволюция  $\tau$ . Найдем теперь число элементов, соответствующих случаям 1) и 2). Для любого смежного класса с инволюцией  $\tau$  в качестве представителя, где  $\tau$  — нецентральная инволюция,  $V\tau = T_0 \cup T_1$ , где  $T_0$  — элементы порядка  $2p$ , а  $T_1$  — инволюции. Подсчитаем число инволюций в  $V\tau$ . Их ровно  $p^k$ , ибо  $|V\langle \tau \rangle : C_{V\langle \tau \rangle}(\tau)| = |V : V_1| = p^k$ . Поэтому остальные элементы имеют четный порядок, но не инволюции,

следовательно, их  $p^{2k} - p^k$ . Так как всего инволютивных представителей нецентральных  $2^{n-1}$ , то  $2^{n-1}(p^{2k} - p^k)$  — количество элементов порядка  $2p$ . Все эти элементы разбиваются на классы  $x \approx y$ , если  $x^2 = y^2$ , т.е. если они корни из одного и того же элемента порядка  $p$ . Число таких корней равно  $p^k$  для фиксированного элемента (как сказано выше). Пусть  $x$  — число классов  $p$ -элементов, отличных от единичного, из которых извлекается корень квадратный в  $G \setminus V$ . Тогда  $x2^{n-1}p^k$  — число элементов порядка  $2p$ . Отсюда  $x2^{n-1}p^k = 2^{n-1}(p^{2k} - p^k) = 2^{n-1}p^k(p^k - 1)$ . Поэтому  $x = p^k - 1$ .

Найдем централизаторы элементов  $g \in (V \rtimes \langle t \rangle) \setminus V$ . Положим  $M = V \rtimes \langle t \rangle$ . Если  $g = \nu\nu$ , то  $g$  — центральная инволюция, поэтому  $C_V(\nu) = 1$  и  $C_S(\nu) = 2^n$ . Значит,  $|C_G(\nu)| = 2^n$  и  $|(\nu)^G| = |G|/|C_G(\nu)| = p^{2k}$ . Пусть  $g = \nu t^i$ , где  $t^i \neq \nu$ . Поскольку  $C_V(t) = 1$ , то  $C_V(g) = 1$ . Далее,  $C_S(t) = \langle t \rangle$ . Поэтому  $|C_G(g)| = 2^{n-1}$ , а их число равно  $|M| - |(\nu)^G| - |V| = 2^{n-1}p^{2k} - p^{2k} - p^{2k}$ .

Найдем централизаторы элементов  $g = w\tau$ , где  $g$  не является инволюцией. Имеем  $C_V(w\tau) = C_V(w) \cap C_V(\tau) = C_V(\tau)$ . Как было показано выше,  $|C_V(\tau)| = p^k$ . С другой стороны,  $C_S(w\tau) = \langle \tau \rangle$ . Поэтому для таких элементов  $|C_G(g)| = 2p^k$ . Общее их число равно  $|G| - |M| - |(\tau)^G| - |(t\tau)^G| = 2^{n-1}p^{2k} - 2^{n-1}p^k - 2^{n-1}p^k$ .

Для удобства оформим полученные значения порядков централизаторов в виде таблицы.

Таблица 1.

Порядки централизаторов элементов $G = E_{p^m} \rtimes D_{2^n}$		
расположение $g \in G$	число таких $g$	$ C_G(g) $
1	1	$2^n p^{2k}$
$\{w_1 \in V^\# \mid C_G(w) \not\subseteq V\}$	$2^{n-1}(p^k - 1)$	$2p^{2k}$
$\{w_2 \in V^\# \mid C_G(w) \subseteq V\}$	$p^{2k} - 1 - 2^{n-1}(p^k - 1)$	$p^{2k}$
$\tau^G$	$2^{n-2}p^k$	$2^2 p^k$
$(t\tau)^G$	$2^{n-2}p^k$	$2^2 p^k$
$w\tau \notin \{(\tau)^G \cup (t\tau)^G\}, w \in V$	$2^{n-1}p^{2k} - 2^{n-1}p^k - 2^{n-1}p^k$	$2p^k$
$(\nu)^G$	$p^{2k}$	$2^n$
$g \in M \setminus \{(\nu)^G \cup V\}$	$2^{n-1}p^{2k} - p^{2k} - p^{2k}$	$2^{n-1}$

Из таблицы 1 получаем следующее выражение для правой части тождества Вигнера:

$$\sum_{g \in G} |C_G(g)|^2 = 1 \cdot (2^n p^{2k})^2 + 2^{n-1}(p^k - 1) \cdot (2p^{2k})^2 + (p^{2k} - 1 - 2^{n-1}(p^k - 1)) \cdot (p^{2k})^2 + 2^{n-1}p^k \cdot (2^2 p^k)^2 + 2^{n-1}(p^{2k} - p^k) \cdot (2p^k)^2 + p^{2k} \cdot (2^n)^2 + (2^{n-1}p^{2k} - p^{2k} - p^{2k}) \cdot (2^{n-1})^2. \quad (1)$$

Вычислим теперь количества квадратных корней из элементов группы  $G$ .

Корнями из единицы являются все инволюции группы  $G$  и сама единица. Имеем:  $|(\nu)^G| = |V| = p^{2k}$ ,  $|(\tau)^G| = |(t\tau)^G| = 2^{n-2}p^k$ . Таким образом,  $|\sqrt{1}| = 1 \cdot (2^{n-1}p^k + p^{2k} + 1)^3$ .

Найдем корни из элементов  $w \in V$ . В неприводимом случае, поскольку  $V$  — неприводимый  $\langle t \rangle$ -модуль, то мы можем выбрать в качестве  $\tau$  автоморфизм порядка 2 поля  $GF(p^{2k})$  (так как  $(\alpha^{p^k})^{p^k} = \alpha^{p^k p^k} = \alpha^{p^{2k}} = \alpha \alpha^{p^{2k-1}} = \alpha$ ) и тогда  $|C_V(\tau)|$  — число элементов  $w \in V = GF(p^{2k})$ , удовлетворяющих соотношению  $\alpha^{p^k} = \alpha$ . Таким образом, из элемента  $w \in V$ , такого, что  $w^\tau = w$ , извлекается  $p^k$  корней вида  $w_1\tau$ , где  $w_1 \in V$ . Кроме того, из элемента  $w$  в подгруппе  $V$  извлекается ровно 1 корень, как из элемента нечетного порядка. Значит,  $|\sqrt{w}| = p^k + 1$ . Покажем, что в приводимом случае выполняется то же самое. Пусть  $w \in V^\#$  такой, что  $C_G(w) \neq V$ . Тогда  $C_G(w) = V \rtimes \langle \tau \rangle = V_1 \times (V_2 \langle \tau \rangle)$ , где  $(w\tau)^2 = 1$ , для любого  $w \in V_2$  и  $V_1 = C_V(\tau)$ , где  $V = C_V(\tau)$ . Для любого  $g \in Vt'$ , где  $t'$  — элемент из  $\langle t \rangle$ ,  $g$  сопряжен с  $t'$ . Поэтому число сопряженных с  $t'$  в  $G$  равно  $2p^k$  при условии, что  $t' \in \langle \nu \rangle$ . Если же  $t' = \nu$ , то  $|t^G| = p^{2k}$ . Пусть  $w^2 \in V_1^\#$  — любой элемент, централизующий  $\tau$ . Тогда  $ww_1\tau = \sqrt{w^2}$  для любого  $w_1 \in V_2$ . В самом деле,  $(ww_1\tau)^2 = w^2 w_1 \tau w_1 \tau = w^2 w_1 w_1^{-1} = w^2$ . Значит, число корней из  $w^2$  в  $V\tau$  равно  $p^k$ . Кроме того,  $w$  — корень из  $w^2$  в  $V$ . Отсюда в  $V \rtimes \langle \tau \rangle$  число корней из  $w$  равно  $p^k + 1$ . Число элементов  $w \in V$ , для которых  $|\sqrt{w}| = p^k + 1$ , в обоих случаях совпадает с числом тех элементов  $w$ , у которых  $C_G(w) \not\subseteq V$ . Таким образом, их число равно  $2^{n-1}(p^k - 1)$ .

Для тех элементов  $w \in V$ , для которых  $w^\tau \neq w$ , для любой нецентральной инволюции  $\tau$ , выполнено  $|\sqrt{w}| = 1$  (как для любого элемента нечетного порядка). Их число равно  $(p^{2k} - 1 - 2^{n-1}(p^k - 1))$ .

Корни из элементов множества  $M = G' \setminus V$ . Покажем, что из каждого такого элемента извлекаются ровно два корня. Любой элемент  $g \in G' \setminus V$  имеет вид  $g = wt^i$ , для некоторого четного  $i$ . Поэтому  $(wt^i)^2 = wt^i wt^i = wt^i wt^{-i} t^{2i} = (ww^{t^{-i}}) t^{2i} = w' t^{2i}$ , где  $w' \in V$ . Отсюда следует, что  $o(wt^i) = o(t^i) = 2^{i'}$  для некоторого  $i'$ . Следовательно, элемент  $wt^i$  сопряжен с элементом вида  $t^{i'1} \in S$ , того же порядка, откуда

$|\sqrt{wt^i}| = |\sqrt{t^{i_1}}|$ . Но из любого элемента  $t^i \in S' \setminus 1$  извлекаются ровно 2 корня:  $t^{i/2}$  и  $t^{i/2+2^{n-2}}$ . Поэтому  $|\sqrt{g}| = 2$ , для любого  $g \in G' \setminus V$ , причем  $|G' \setminus V| = 2^{n-2} p^{2k} - p^{2k}$ .

Корни из элементов  $g \in G \setminus G'$  не извлекаются. Действительно, по предложению 1 получаем, что  $G/G'$  – элементарная абелева 2-группа. Поэтому квадрат любого элемента лежит в  $G'$ . Значит, для элементов  $g \in G \setminus G'$  выполняется  $|\sqrt{g}| = 0$  и вклад их в левую часть неравенства Вигнера нулевой.

Для удобства оформим полученные значения порядков квадратных корней элементов в виде таблицы.

Таблица 2.

Порядки корней группы $G = E_{p^m} \rtimes D_{2^n}$		
расположение $g \in G$	число таких $g$	$ \sqrt{g} $
1	1	$2^{n-1} p^k + p^{2k} + 1$
$\{w_1 \in V^\sharp \mid C_G(w) \not\subseteq V\}$	$2^{n-1}(p^k - 1)$	$p^k + 1$
$\{w_2 \in V^\sharp \mid C_G(w) \subseteq V\}$	$p^{2k} - 1 - 2^{n-1}(p^k - 1)$	1
$G' \setminus V$	$2^{n-2} p^{2k} - p^{2k}$	2
$G \setminus G'$	$2^n p^{2k} - 2^{n-2} p^{2k}$	0

Из таблицы 2 получаем следующее выражение для левой части тождества Вигнера:

$$\sum_{g \in G} |\sqrt{g}|^3 = 1 \cdot (2^{n-1} p^k + p^{2k} + 1)^3 + 2^{n-1} (p^k - 1) \cdot (p^k + 1)^3 + (2^{n-2} p^{2k} - p^{2k}) \cdot (2)^3 + (p^{2k} - 1 - 2^{n-1} (p^k - 1)) \cdot (1)^3. \quad (2)$$

Приравняем выражения (1) и (2), а после перенесем все в правую часть. После упрощений получим квадратный многочлен относительно  $p^k$ :

$$(2^{2n-2} - 4) \cdot p^{2k} + (2^{n+1} - 2^{3n-3}) \cdot p^k + (2^{3n-3} - 2^{2n-2} - 2^{n+1} + 4) = 0.$$

Раскладывая этот многочлен, получим:

$$(2^{2n-2} - 4)(p^k - 1)(p^k + 1 - 2^{n-1}) = 0.$$

Учитывая то, что  $n \geq 3$ ,  $p > 2$ ,  $k \geq 1$ , получим равенство:  $p^k = 2^{n-1} - 1$ . Согласно лемме IX.2.7 в [6], такое равенство возможно, только когда  $k = 1$  и  $p = 2^{n-1} - 1$  – простое число Мерсенна, причем с необходимостью  $(n - 1) = q$  – также некоторое простое число. Теорема доказана.  $\square$

**Лемма 4.** Пусть  $G \cong (E_1 \times E_2) \rtimes D_{2^{q+1}}$ , где  $E_1 \rtimes D_{2^{q+1}} \cong E_2 \rtimes D_{2^{q+1}} \cong E_{p^2} \rtimes D_{2^{q+1}}$  изоморфны атомарной группе SR-группе,  $p = 2^q - 1$ . Тогда  $G$  не является SR-группой.

*Доказательство.* Доказательство этой леммы во многом повторяет доказательство леммы 3 и использует те же методы. Поэтому мы приведем только соответствующие таблицы порядков централизаторов и корней. Положим  $D_{2^{q+1}} = \langle t \rangle_{2^q} \rtimes \langle \tau \rangle_2 \in Syl_2(G)$ ,  $\nu = t^{2^{q-1}}$ ,  $V = E_1 \times E_2$ ,  $M = V \rtimes \langle t \rangle_{2^q}$ .

Таблица порядков централизаторов для элементов группы  $G$ :

Таблица 3.

Порядки централизаторов элементов $G = (E_1 \times E_2) \rtimes D_{2^{q+1}}$		
расположение $g \in G$	число таких $g$	$ C_G(g) $
1	1	$2^{q+1} p^4$
$\{w_1 \in V^\sharp \mid C_G(w) \not\subseteq V\}$	$2^q(p^2 - 1)$	$2p^4$
$\{w_2 \in V^\sharp \mid C_G(w) \subseteq V\}$	$p^4 - 2^q(p^2 - 1) - 1$	$p^4$
$g \in (\tau)^G$	$2^{q-1} p^2$	$2^2 p^2$
$g \in (t\tau)^G$	$2^{q-1} p^2$	$2^2 p^2$
$g \in G \setminus \{M \cup (\tau)^G \cup (t\tau)^G\}$	$2^q p^4 - 2 \cdot 2^{q-1} p^2$	$2p^2$
$g \in (\nu)^G$	$p^4$	$2^{q+1}$
$g \in M \setminus \{V \cup (\nu)^G\}$	$2^q p^4 - 2 \cdot p^4$	$2^q$

Из таблицы 3 получаем выражение для правой части неравенства Вигнера группы  $G$ :

$$\sum_{g \in G} |C_G(g)|^2 = 1 \cdot (2^{q+1} p^4)^2 + 2^q (p^2 - 1) \cdot (2p^4)^2 + (p^4 - 2^q (p^2 - 1) - 1) \cdot (p^4)^2 + 2 \cdot 2^{q-1} p^2 \cdot (2^2 p^2)^2 + (2^q p^4 - 2 \cdot 2^{q-1} p^2) \cdot (2p^2)^2 + p^4 \cdot (2^{q+1})^2 + (2^q p^4 - 2 \cdot p^4) \cdot (2^q)^2. \quad (3)$$

Таблица количеств корней из элементов группы  $G$ :

Таблица 4.

Количества корней элементов группы $G = (E_1 \times E_2) \rtimes D_{2^{q+1}}$		
расположение $g \in G$	число таких $g$	$ \sqrt{g} $
1	1	$p^4 + 2^q p^2 + 1$
$\{v \in V^\# \mid C_G(v) \not\subseteq V\}$	$2^q(p^2 - 1)$	$p^2 + 1$
$\{v \in V^\# \mid C_G(v) \subseteq V\}$	$p^4 - 2^q(p^2 - 1) - 1$	1
$g \in G' \setminus V$	$2^{q-1}p^4 - p^4$	2
$g \in G \setminus G'$	$2^{q+1}p^4 - 2^{q-1}p^4$	0

Из таблицы 4 получаем выражение для левой части неравенства Вигнера группы  $G$ :

$$\sum_{g \in G} |\sqrt{g}|^3 = 1 \cdot (p^4 + 2^q p^2 + 1)^3 + 2^q(p^2 - 1) \cdot (p^2 + 1)^3 + (p^4 - 2^q(p^2 - 1) - 1) \cdot (1)^3 + (2^{q-1}p^4 - p^4) \cdot (2)^3. \quad (4)$$

Приравняем теперь выражения (3) и (4) и сделаем замену  $2^q = p + 1$ . После упрощений получим:

$$p^5(p + 3)(p + 1)(p - 1)^3 = 0.$$

Поскольку  $p > 2$ , последнее равенство не может иметь места. Итак,  $G$  не является  $SR$ -группой. □

*Доказательство теоремы 1.* Пусть  $G$  — несверхразрешимая  $SR$ -группа. Положим  $S \in Syl_2(G)$ . Если  $O(G) = 1$ , то, согласно [7], группа  $G$  является 2-скованной, поэтому  $C_G(O_2(G)) \leq O_2(G)$ . Откуда  $O_2(G) \triangleleft S$ . Но  $O_2(G)$  может быть либо четверной группой  $T \cong C_2 \times C_2$  (при  $|S| \leq 8$ ), либо диэдральной меньшего порядка, либо циклической группой. Рассмотрим эти случаи отдельно. Если  $O_2(G) \cong T$ , тогда  $G/T \leq Aut(T) \cong S_3$ . Откуда либо  $G \cong A_4$ , либо  $G \cong S_4$ . Так как  $A_4$  не является  $SR$ -группой, то получаем, что  $G \cong S_4$ . Пусть теперь  $O_2(G)$  циклическая или диэдральная, где  $|O_2(G)| > 4$ . Тогда  $Aut(O_2(G))$  является 2-группой и потому  $G$  не имеет нетривиальных элементов нечетного порядка, т.е.  $G$  является 2-группой. Итак, из  $G/O(G) \neq S_4$  и  $O(G) \neq 1$  следует, что  $G$  имеет нормальное 2-дополнение. Случай, когда  $O_p(G) = O(G) \neq 1$ , невозможен, согласно лемме 4. Таким образом, если  $G$  не 2-нильпотентна, то  $G/O(G) \cong S_4$ .

Пусть группа  $G$  2-нильпотентна. Это значит, что  $G = P \rtimes S$ , где  $P \in Syl_p(G)$ ,  $S \in Syl_2(G)$ . Обозначим  $P = Syl_p(G)$ . Имеем  $G = P \rtimes S$ . По условию  $\Phi(G) = 1$ , отсюда  $\Phi(P) \leq \Phi(G) = 1$ ,  $\Phi(P) = 1$ . Значит,  $P = E_{p^m}$  — элементарная абелева группа. Имеем  $G = E_{p^m} \rtimes D_{2^n}$ .

Группа  $P$  раскладывается в произведение  $T = E_1 \times \dots \times E_k$  нормальных подгрупп группы  $G$ , где  $E_i$  — минимальная нормальная подгруппа в  $G$ . Положим  $\hat{E}_i = E_1 \times \dots \times E_{i-1} \times E_{i+1} \times \dots \times E_k$ , тогда  $G/\hat{E}_i \cong E_i \rtimes D_{2^n}$  — атомарная группа.

В лемме 3 было доказано, что атомарная группа является несверхразрешимой  $SR$ -группой тогда и только тогда, когда  $p$  — простое число Мерсенна. Значит, без ограничения общности можно считать, что минимальным контрпримером является группа  $G \cong (E_1 \times E_2) \rtimes D_{2^n}$ , где  $E_1 \rtimes D_{2^n}$ , и  $E_2 \rtimes D_{2^n}$  — атомарные группы. В лемме 4 мы показали, что такая группа не является  $SR$ -группой, что завершает доказательство теоремы 1. □

Автор выражает глубокую благодарность своему научному руководителю Л.С. Казарину за полезные советы и обсуждения, способствовавшие улучшению этой работы.

### Список литературы

1. Струнков, С.П. О расположении характеров просто приводимых групп / С.П. Струнков // Математические заметки. — 1982. — Т. 31, № 3 — С. 357 — 362.
2. The GAP Group. GAP — Groups, Algorithms and Programming, Version 4.4.9, Aachen, St.Andrews, 2006. [Электронный ресурс]. Режим доступа: <http://www.gap-system.org>
3. Кертис, Ч. Теория представлений групп и ассоциативных алгебр / Ч. Кертис, И. Райнер. — М.: Наука, 1969.
4. Хамермеш, М. Теория групп и ее применение к физическим проблемам / М. Хамермеш. М.: Мир, 1966.

5. *Huppert, B.* Endliche Gruppen I. / *B. Huppert.* — Berlin; Heidelberg; New York: Springer, 1967.
6. *Huppert, B.* Finite Groups II / *B. Huppert, N. Blackburn.* — Berlin e.a.: Springer, 1982.
7. *Gorenstein D.* Finite groups / *D. Gorenstein* — N.Y.: Harper and Row, 1968.

### **SR-groups of Order $2^n p^m$ with Dihedral Sylow 2-subgroup**

Yanishevskiy V.V.

The structure of *SR*-groups with dihedral Sylow 2-subgroup modulo Frattini subgroup is described. It is proved that if a group  $G$  is a non-supersolvable *SR*-group of order  $2^n p^m$  with dihedral Sylow 2-subgroup,  $p$  is Mersenne prime.