Сибирский математический журнал
Сентябрь—октябрь, 2001. Том 42, № 5

УДК 519.44

О ЧИСЛЕ ПАР ПОРОЖДАЮЩИХ ГРУПП $L_2(2^m)$ И $Sz(2^{2k+1})$

Н. М. Сучков, Д. М. Приходько

Аннотация: Для простой группы G, где $G = L_2(2^m)$ либо $G = Sz(2^{2k+1})$, найдено такое максимальное число $n = n(G)$, что прямое произведение n экземпляров группы G порождается двумя элементами. Библиогр. 5.

Введение

Пусть G — группа, G^n — прямое произведение n экземпляров группы G. В Коуровской тетради [1] С. А. Сыскиным поставлена следующая задача 12.86: для каждой известной простой конечной группы G найти такое максимальное число $n = n(G)$, что G^n порождается двумя элементами.

Еще в 1936 г. Ф. Холл [2] доказал, что

$$n(G) = \frac{N(G)}{|\operatorname{Aut} G|},$$

где G — любая конечная простая неабелева группа, $N(G)$ — число всех упорядоченных пар порождающих группы G. В этой же работе установлено, что $n(A_5) = 19$.

В настоящей статье задача 12.86 решается для всех простых групп $L_2(2^m)$ и $Sz(2^{2k+1})$. Сформулируем полученные результаты.

Теорема 1. *Пусть*

$$\varphi(m) = \frac{1}{m}(2^m - 2)(4^m + 2^m - 1)$$

для каждого натурального m. Если m — простое число, то $n(L_2(2^m)) = \varphi(m)$. При составном m имеет место рекуррентная формула

$$n(L_2(2^m)) = \varphi(m) - \frac{1}{m}\sum_{\substack{1<t<m\\ t\backslash m}} tn(L_2(2^t)).$$

Теорема 2. *Для натурального m полагаем*

$$\psi(m) = \frac{1}{m}(2^m - 2)(16^m + 8^m + 2\cdot 4^m + 4\cdot 2^m - 1).$$

Если m — простое нечетное число, то $n\big(Sz(2^m)\big) = \psi(m)$. При нечетном составном m справедлива рекуррентная формула

$$n(Sz(2^m)) = \psi(m) - \frac{1}{m}\sum_{\substack{1<t<m\\ t\backslash m}} tn(Sz(2^t)).$$

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований и Красноярского краевого фонда науки.

§ 1. Доказательство теоремы 1

Пусть $G = L_2(q)$, $q = 2^m$, $m > 1$. Напомним известные факты, которые можно найти в [3, 4]. Порядок группы G равен $q(q^2-1)$. Максимальная разрешимая подгруппа из G сопряжена к одной из следующих подгрупп:

1) $B = S \leftthreetimes H = N_G(S)$ — группа Фробениуса с ядром S и дополнительным множителем H, где S — элементарная абелева подгруппа порядка q, H — циклическая подгруппа порядка $q-1$;

2) $D = H \leftthreetimes \langle t\rangle = N_G(H)$ — группа диэдра порядка $2(q-1)$;

3) $A = T \leftthreetimes \langle t\rangle = N_G(T)$ — группа диэдра порядка $2(q+1)$.

Всякий элемент группы G сопряжен некоторому элементу одной из подгрупп S, H, T, которые являются сильно изолированными в G, т. е. содержат централизатор каждого своего неединичного элемента. Неразрешимая подгруппа группы G сопряжена к одной из подгрупп $G_k \simeq L_2(2^k)$, где $k \neq 1$ и $k \backslash m$. Наконец, $|\operatorname{Aut} G| = m|G|$.

Лемма 1.1. *Если $M_1 = \{(x,y) \mid |x| = 2,\ \langle x,y\rangle$ — неразрешимая подгруппа$\}$, то $|M_1| = |G|(q-1)(q-2)$.*

Доказательство. Фиксируем инволюцию $z \in B$. Группа G содержит $(|S|-1)|G:B| = (q^2-1)$ инволюций, и все они сопряжены в G. Так как $|D^G| = |G:D| = \frac{q}{2}(q+1)$ и D содержит $q-1$ инволюций, то z лежит в $r = \frac{q}{2}$ сопряженных с D подгруппах $D_1,\dots,D_r$. Аналогично выводим, что z содержится точно в r сопряженных с A подгруппах $A_1,\dots,A_r$. Итак, $\Delta_1 = \{B, D_1,\dots,D_r, A_1,\dots,A_r\}$ — множество всех максимальных разрешимых подгрупп, которые содержат инволюцию z.

Заметим, что пересечение двух различных подгрупп из Δ_1 совпадает с $\langle z\rangle$. Действительно, так как числа $q-1$ и $q+1$ взаимно просты, то $|B \cap A_j| = |D_i \cap A_j| = 2$ $(i,j = 1,\dots,r)$. Если $|D_i \cap D_j| > 2$ для $1 \le i < j \le r$, то пересечение $D_i \cap D_j$ содержит неединичный элемент нечетного порядка из подгруппы, сопряженной к H. Но ввиду сильной изолированности в G подгруппы H отсюда легко выводим, что $D_i = D_j$. Противоречие. Аналогично $A_i \cap A_j = \langle z\rangle$ при $1 \le i < j \le r$. Предположим, наконец, что $B \cap D_i$ содержит более двух элементов. Тогда снова это пересечение содержит неединичный элемент нечетного порядка и на основании сильной изолированности в G подгруппы B заключаем, что $D_i < B$. Это противоречит строению подгруппы B.

Таким образом, если Ω_1 — объединение всех подгрупп множества Δ_1, то

$$\begin{aligned}|\Omega_1| &= |B| + r(|D|-2) + r(|A|-2)\\ &= q(q-1) + \frac{q}{2}(2(q-1)-2) + \frac{q}{2}(2(q+1)-2) = 3q(q-1).\end{aligned}$$

Далее, очевидно, подгруппа $\langle z,y\rangle$ тогда и только тогда неразрешима, когда $y \in G\backslash\Omega_1$. Поэтому

$$\begin{aligned}|M_1| &= |G\backslash\Omega_1|\cdot(q^2-1) = (q(q^2-1) - 3q(q-1))(q^2-1)\\ &= q(q-1)(q-2)(q^2-1) = |G|(q-1)(q-2).\end{aligned}$$

Лемма доказана.

Лемма 1.2. *Пусть $M_2 = \{(x,y) \mid |x|\backslash(q-1),\ \langle x,y\rangle$ неразрешимая подгруппа$\}$. Тогда $|M_2| = |G|\frac{q}{2}(q-1)(q-2)$.*

Доказательство. Пусть h — любой неединичный элемент подгруппы H. Так как $(|H|,|T|) = 1$, то $h \notin A^g$ при всех $g \in G$. В силу равенства $C_G(h) = H$

(сильная изолированность H в G) включение $h \in H^g$ $(g \in G)$ справедливо только при $g \in N_G(H) = D$. Поскольку $|H^G| = |G : D| = \frac{q}{2}(q+1)$, $|B^G| = |G : B| = q+1$, $|H^B| = q$, то h содержится точно в двух подгруппах B и B_1 из класса B^G. Следовательно, D, B, B_1 — все максимальные разрешимые подгруппы, содержащие элемент h. Так как эти подгруппы попарно пересекаются по H, то, обозначая $\Omega_2 = D \cup B \cup B_1$, получим

$$|\Omega_2| = |D| + 2(|B| - |H|) = 2(q-1) + 2(q(q-1) - (q-1)) = 2(q-1)q.$$

Ясно, что подгруппа $\langle h, y\rangle$ тогда и только тогда неразрешима, когда $y \in G \backslash \Omega_2$.

Наконец, заметим, что число неединичных элементов, порядки которых делят $q-1$, равно $l = (|H|-1)|H^G| = (q-2)\frac{q}{2}(q+1)$. Значит,

$$|M_2| = |G\backslash\Omega_2|l = (q(q^2-1) - 2(q-1)q)(q-2)\frac{q}{2}(q+1) = |G|\frac{q}{2}(q-1)(q-2).$$

Лемма доказана.

Лемма 1.3. *Порядок множества* $M_3 = \{(x,y) \mid |x|\backslash(q+1),\ \langle x,y\rangle$ *— неразрешимая подгруппа*$\}$ *равен* $|G|\frac{q}{2}(q+1)(q-2)$.

Доказательство. Так как A является единственной максимальной разрешимой подгруппой, содержащей произвольный неединичный элемент из T, то

$$|M_3| = (|G|-|A|)(|T|-1)|T^G| = (q(q^2-1)-2(q+1))q\frac{q}{2}(q-1) = |G|\frac{q}{2}(q+1)(q-2).$$

Лемма доказана.

Лемма 1.4. *Если* $M = \{(x,y) \mid \langle x,y\rangle$ *— неразрешимая подгруппа*$\}$, *то* $|M| = |G|(q-2)(q^2+q-1)$.

Доказательство. Поскольку M является объединением попарно не пересекающихся множеств M_1, M_2, M_3, то $|M| = |M_1| + |M_2| + |M_3|$. Теперь ввиду трех предыдущих лемм простым арифметическим подсчетом убеждаемся, что лемма верна.

Завершим доказательство теоремы 1. Если m — простое число, то все собственные подгруппы группы $G_m = L_2(2^m)$ разрешимы, а потому $N(G_m) = |M|$. Так как $|\operatorname{Aut}(G_m)| = m|G_m|$, в силу леммы 1.4 по формуле Ф. Холла получаем $n(G_m) = \varphi(m)$.

Пусть теперь m — составное число. Ввиду вышеизложенного описания неразрешимых подгрупп группы G_m и простоты всех подгрупп G_k $(k>1,\ k\backslash m)$ заключаем, что эти подгруппы совпадают со своими нормализаторами, а значит, число подгрупп, сопряженных с подгруппой G_k, равно $|G_m : G_k|$. В силу определения множества M имеем

$$N(G_m) = |M| - \sum_{\substack{1<k<m\\ k\backslash m}} N(G_k)|G_m : G_k| = |M| - |G_m| \sum_{\substack{1<k<m\\ k\backslash m}} \frac{N(G_k)}{|G_k|}.$$

Применяя формулу Ф. Холла, отсюда выводим

$$n(G_m) = \frac{|M|}{|\operatorname{Aut} G_m|} - \frac{|G_m|}{|\operatorname{Aut} G_m|} \sum_{\substack{1<k<m\\ k\backslash m}} \frac{n(G_k)|\operatorname{Aut} G_k|}{|G_k|} = \varphi(m) - \frac{1}{m} \sum_{\substack{1<k<m\\ k\backslash m}} kn(G_k).$$

Теорема 1 доказана.

§ 2. Доказательство теоремы 2

Справедливость теоремы 2 установим точно по схеме доказательства теоремы 1. Сформулируем сначала некоторые результаты о подгруппах группы $G = Sz(q)$, $q = 2^m$, m — нечетное целое число, большее 1. Все нижеизложенные факты доказаны в [5].

Порядок группы G равен $q^2(q-1)(q^2+1)$. Максимальная разрешимая подгруппа группы G сопряжена к одной из следующих подгрупп:

1) $B = S \leftthreetimes H = N_G(S)$ — группа Фробениуса с циклическим дополнительным множителем H порядка $q-1$ и ядром S порядка q^2; подгруппа S имеет период 4 и содержит $q-1$ инволюций; если u — фиксированный элемент 4-го порядка из S, то любой элемент 4-го порядка группы G сопряжен к элементу из $\langle u\rangle$;

2) $D = H \leftthreetimes \langle t\rangle = N_G(H)$ — группа диэдра порядка $2(q-1)$;

3) $A = T \leftthreetimes \langle u\rangle = N_G(T)$ — группа Фробениуса с дополнительным множителем $\langle u\rangle$ и циклическим ядром T порядка $q+r+1$, где $r^2 = 2q$;

4) $E = F \leftthreetimes \langle u\rangle = N_G(F)$ — группа Фробениуса с дополнительным множителем $\langle u\rangle$ и циклическим ядром F порядка $q-r+1$.

Подгруппы H, T, F являются холловскими в группе G. Всякий элемент группы G сопряжен некоторому элементу одной из подгрупп S, H, T, F, сильно изолированных в группе G. Неразрешимая подгруппа группы G сопряжена к одной из подгрупп $G_k \simeq Sz(2^k)$, $k \neq 1$, $k\backslash m$. Порядок группы $\operatorname{Aut} G$ равен $m|G|$.

Лемма 2.1. *Если $M_1 = \{(x,y) \mid |x| = 2,\ \langle x,y\rangle$ — неразрешимая подгруппа$\}$, то $|M_1| = |G|(q-2)(q^2+q-1)$.*

Доказательство. Фиксируем инволюцию $z \in B$. Группа G содержит $(q-1)|G:B| = (q-1)(q^2+1)$ инволюций, и все они сопряжены в группе G. Так как $|D^G| = |G:D| = \frac{q^2}{2}(q^2+1)$ и подгруппа D содержит $q-1$ инволюций, то z лежит в $s = \frac{q^2}{2}$ сопряженных с D подгруппах $D_1,\dots,D_s$. Поскольку $|A^G| = |G:A|$ и A содержит $q+r+1$ инволюций, то z принадлежит $l = \frac{q^2}{4}$ сопряженным с A подгруппам $A_1,\dots,A_l$. Аналогично инволюция z входит в l сопряженных с E подгрупп $E_1,\dots,E_l$. Итак, $\Delta_1 = \{B, D_1,\dots,D_s, A_1,\dots,A_l, E_1,\dots,E_l\}$ — множество всех максимальных разрешимых подгрупп группы G, которые содержат инволюцию z.

Обозначим через Ω_1 объединение всех подгрупп из Δ_1. Повторяя рассуждения из доказательства леммы 1.1, убеждаемся, что $D_i \cap D_j = D_i \cap B = \langle z\rangle$ при $i,j = 1,\dots,s$; $i \neq j$. Далее, на основании равенств $\pi(B)\cap\pi(T) = \pi(B)\cap\pi(F) = \varnothing$ и ввиду сильной изолированности в G подгруппы S имеем $|B\cap A_i| = |B \cap E_i| = 4$, $i = 1,\dots,l$. Заметим, наконец, что если R — пересечение двух различных подгрупп из множества Δ_1, то в R нет элементов нечетного порядка ввиду сильной изолированности в G подгрупп H, T, F. Следовательно, либо $R = \langle z\rangle$, либо $R = \langle x\rangle$, где $x^2 = z$. Поскольку $C_G(z) = S \subset B$, то $R \subset B$. Таким образом,

$$\begin{aligned}|\Omega_1| = |B| + \frac{q^2}{2}(|D|-2) + \frac{q^2}{4}(|A|-4) + \frac{q^2}{4}(|E|-4)\\ = q^2[(q-1)+(q-2)+(q+r)+(q-r)] = q^2(4q-3).\end{aligned}$$

Очевидно, подгруппа $\langle z,y\rangle$ тогда и только тогда является неразрешимой, когда

$y \in G \backslash \Omega_1$. Значит,

$$|M_1| = |G\backslash\Omega_1|(q-1)(q^2+1) = (|G| - q^2(4q-3))(q-1)(q^2+1)$$
$$= |G|((q-1)(q^2+1) - (4q-3)) = |G|(q^3 - q^2 - 3q + 2) = |G|(q-2)(q^2+q-1).$$

Лемма доказана.

Лемма 2.2. *Пусть $M_2 = \{(x,y) \mid |x| = 4,\ \langle x,y\rangle$ — неразрешимая подгруппа$\}$. Тогда $|M_2| = |G|q(q-2)(q^2+q+2)$.*

Доказательство. Пусть ω — фиксированный элемент порядка 4 из подгруппы B. Тогда $|M_2| = |M_2'|\lambda$, где $M_2' = \{(\omega,y) \mid \langle\omega,y\rangle$ — неразрешимая подгруппа$\}$, λ — число элементов порядка 4 в группе G. Очевидно, $\lambda = (q^2-q)|G : B| = (q^2-q)(q^2+1)$.

Найдем теперь $|M_2'|$. Ясно, что кроме подгруппы B элемент ω содержится еще в некоторых максимальных разрешимых подгруппах, сопряженных с A и E. Так как $|A^G| = |G : A|$ и A содержит $2(q+r+1)$ элементов порядка 4, то ω принадлежит $\frac{1}{\lambda}|G : A|2(q+r+1) = \frac{q}{2} = d$ сопряженным с A подгруппам $A_{i_1},\dots,A_{i_d}$. Подобными рассуждениями устанавливаем, что ω принадлежит d сопряженным с E подгруппам $E_{j_1},\dots,E_{j_d}$. Таким образом, максимальные разрешимые подгруппы, содержащие элемент ω, составляют множество $\Delta_2 = \{B, A_{i_1},\dots,A_{i_d}, E_{j_1},\dots,E_{j_d}\}$.

Пусть Ω_2 — объединение подгрупп из множества Δ_2. Поскольку, как установлено при доказательстве предыдущей леммы, пересечение двух различных подгрупп множества Δ_2 не содержит элементов нечетного порядка, то это пересечение совпадает с $\langle\omega\rangle$. Отсюда выводим, что

$$|\Omega_2| = |B| + d(|A|-4) + d(|E|-4)$$
$$= q^2(q-1) + \frac{q}{2}\bigl(4(q+r+1) - 4 + 4(q-r+1) - 4\bigr) = q^2(q-1) + \frac{q}{2}8q = q^2(q+3),$$
$$|M_2'| = |G\backslash\Omega_2| = q^2((q-1)(q^2+1) - (q+3)) = q^2(q-2)(q^2+q+2),$$
$$|M_2| = |M_2'|\lambda = |G|q(q-2)(q^2+q+2).$$

Лемма доказана.

Лемма 2.3. *Пусть $M_3 = \{(x,y) \mid |x|\backslash(q-1),\ \langle x,y\rangle$ — неразрешимая подгруппа$\}$. Тогда $|M_3| = |G|(q^2-1)(q-2)\frac{q^2}{2}$.*

Доказательство. Фиксируем любой неединичный элемент $h \in H$, и пусть $M_3' = \{(h,y) \mid \langle h,y\rangle$ — неразрешимая подгруппа$\}$. Тогда

$$|M_3| = |M_3'|(|H|-1)|H^G| = |M_3'|(q-2)|G : D| = |M_3'|(q-2)\frac{q^2}{2}(q^2+1).$$

Остается вычислить $|M_3'|$. Так как подгруппа H сильно изолирована в группе G, то $h \in H^G$ тогда и только тогда, когда $g \in N_G(H) = D$. Далее, из равенств $|B^G| = |G : B| = q^2+1$, $|H^B| = q^2$, $|H^G| = |G : D| = \frac{q^2}{2}(q^2+1)$ вытекает, что подгруппа H (элемент h) содержится точно в двух подгруппах B и B_0 из класса B^G. Итак, D, B, B_0 — все максимальные разрешимые подгруппы группы G, содержащие элемент h. Поскольку все эти подгруппы попарно пересекаются по H, то, обозначая $\Omega_3 = D \cup B \cup B_0$, получим

$$|\Omega_3| = |D| + 2(|B| - |H|) = 2(q-1) + 2(q^2(q-1) - (q-1)) = 2(q-1)q^2.$$

Очевидно, подгруппа $\langle h,y\rangle$ неразрешима тогда и только тогда, когда $y \in G\backslash\Omega_3$. Поэтому $|M_3'| = |G| - 2(q-1)q^2 = q^2(q-1)(q^2-1)$. Отсюда и из вышеизложенного непосредственно убеждаемся, что лемма верна.

Лемма 2.4. *Порядок множества* $M_4 = \{(x,y) \mid |x| \backslash (q+r+1),\ \langle x,y\rangle$ — *неразрешимая подгруппа*$\}$ *равен* $|G|\bigl(\frac{q^2}{4}(q-1)(q^2-q+r)-q-r\bigr)$.

Доказательство. Так как A является единственной максимальной разрешимой подгруппой группы G, содержащей произвольный неединичный элемент подгруппы T, то

$$|M_4| = (|G|-|A|)(|T|-1)|T^G|$$
$$= (q^2(q-1)(q^2+1)-4(q+r+1))(q+r+1-1)\frac{|G|}{4(q+r+1)}$$
$$= |G|\left(\frac{q^2}{4}(q-1)(q-r+1)-1\right)(q+r) = |G|\left(\frac{q^2}{4}(q-1)(q^2-q+r)-q-r\right).$$

Лемма 2.5. *Порядок множества* $M_5 = \{(x,y) \mid |x| \backslash (q-r+1),\ \langle x,y\rangle$ — *неразрешимая подгруппа*$\}$ *равен* $|G|\bigl(\frac{q^2}{4}(q-1)(q^2-q-r)-q+r\bigr)$.

Доказательство. Достаточно повторить вычисления при доказательстве предыдущей леммы, заменяя A и T на E и F, соответственно. Лемма доказана.

Лемма 2.6. *Если* $M = \{(x,y) \mid \langle x,y\rangle$ — *неразрешимая подгруппа*$\}$, *то* $|M| = |G|(q-2)(q^4+q^3+2q^2+4q-1)$.

Доказательство. Поскольку M является объединением попарно не пересекающихся множеств $M_1,\dots,M_5$, то $|M| = |M_1|+\dots+|M_5|$. На основании предыдущих лемм простым арифметическим подсчетом убеждаемся, что лемма верна.

Завершим доказательство теоремы 2. Если m — простое нечетное число, то все собственные подгруппы группы $G_m = Sz(2^m)$ разрешимы. Следовательно, $N(G_m) = |M|$, и ввиду леммы 2.6 по формуле Ф. Холла получаем $n(G_m) = \psi(m)$.

Пусть теперь m — составное нечетное число. Вывод рекуррентной формулы теоремы 2 проводится дословным повторением (при замене лишь $\varphi(m)$ на $\psi(m)$) доказательства в конце § 1 истинности рекуррентной формулы теоремы 1. Теорема 2 доказана.

ЛИТЕРАТУРА

1. *Коуровская* тетрадь. Новосибирск: Ин-т математики СО РАН, 1999.
2. *Hall P.* The Eulerian functions of a group // Quart. J. Math. 1936. V. 7. P. 134–151.
3. *Бусаркин В. М. Горчаков Ю. М.* Конечные расщепляемые группы. М.: Наука, 1968.
4. *Горенстейн Д.* Конечные простые группы. М.: Мир, 1985.
5. *Suzuki M.* On a class of doubly transitive groups // Ann. Math. 1962. V. 75, N 1. P. 105–145.

Статья поступила 20 декабря 2000 г.

Сучков Николай Михайлович
Красноярский гос. университет, кафедра алгебры и математической логики, просп. Свободный, 79, Красноярск 660041

Приходько Денис Михайлович
Красноярский гос. университет, кафедра алгебры и математической логики, просп. Свободный, 79, Красноярск 660041
DPrihodko@beep.ru