Сибирский математический журнал
Март—апрель, 2005. Том 46, № 2

УДК 519.542

О РАСПОЗНАВАНИИ ВСЕХ КОНЕЧНЫХ НЕАБЕЛЕВЫХ ПРОСТЫХ ГРУПП, ПРОСТЫЕ ДЕЛИТЕЛИ ПОРЯДКОВ КОТОРЫХ НЕ ПРЕВОСХОДЯТ 13

А. В. Васильев

Аннотация: Спектром группы называется множество порядков ее элементов. Мы говорим, что для данной конечной группы проблема ее распознаваемости по спектру решена, если мы знаем число попарно неизоморфных конечных групп со спектром, как у данной группы. В статье полностью решена проблема распознаваемости по спектру для конечных неабелевых простых групп, простые делители порядков которых не превосходят 13.

Ключевые слова: распознавание по спектру, конечная простая группа, группа лиева типа.

Введение

Пусть G — конечная группа. Обозначим через $\pi(G)$ множество всех простых делителей порядка группы G. В настоящей работе рассматриваются конечные неабелевы простые группы G со свойством $\pi(G) \subseteq \{2, 3, 5, 7, 11, 13\}$. Мы обозначим множество всех таких групп через $\mathscr{S}_{13}$. Поскольку существует лишь конечное число конечных неабелевых простых групп G с одним и тем же множеством $\pi(G)$ (см., например, замечание после леммы 2 в [1]), множество $\mathscr{S}_{13}$ содержит конечное число изоморфных типов групп. Используя классификацию конечных простых групп (CFSG), несложно получить полный список всех групп, содержащихся в $\mathscr{S}_{13}$. Всего таких групп 55, и они перечислены в табл. 1 настоящей статьи.

Спектр $\omega(G)$ конечной группы G — это множество всех порядков ее элементов. Другими словами, натуральное число n лежит в $\omega(G)$ тогда и только тогда, когда в G найдется элемент порядка n. Для произвольного подмножества ω множества натуральных чисел обозначим через $h(\omega)$ число попарно неизоморфных конечных групп G таких, что $\omega(G) = \omega$. Мы будем говорить, что для конечной группы G проблема распознаваемости решена, если мы знаем значение $h(\omega(G))$ (для краткости, $h(G)$). Более точно, группа G называется *распознаваемой по спектру* (кратко, *распознаваемой*), если $h(G) = 1$, *почти распознаваемой*, если $1 < h(G) < \infty$, и *нераспознаваемой*, если $h(G) = \infty$.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (коды проектов 02–01–39005 и 05–01–00797), Совета по грантам президента РФ и государственной поддержке ведущих научных школ (код проекта НШ–2069.2003.1), программы Рособразования «Развитие научного потенциала высшей школы» по проекту 8294, а также программы «Университеты России» (код проекта УР.04.01.202).

Поскольку любая конечная простая группа, содержащая нетривиальную нормальную разрешимую подгруппу, нераспознаваема (см. [2, лемма 1]), каждая распознаваемая или почти распознаваемая группа является расширением прямого произведения M неабелевых простых групп с помощью некоторой подгруппы из $\mathrm{Out}(M)$. Поэтому особый интерес представляет вопрос о распознаваемости простых и почти простых групп (напомним, что группа G называется *почти простой*, если $S \leq G \leq \mathrm{Aut}(S)$ для некоторой неабелевой простой группы S). Первые примеры распознаваемых конечных простых групп были указаны Ши в середине 80-х гг. прошлого века (см. [3, 4]). В 1994 г. Ши и Брандл доказали распознаваемость бесконечной серии простых линейных групп $L_2(q)$, $q \neq 9$ (см. [5, 6]). К настоящему времени проблема распознаваемости решена для многих конечных неабелевых простых и почти простых групп. Последний по времени список таких групп можно найти в [7]. Мы обозначим множество групп из этого списка через $\mathscr{R}$. В частности, $\mathscr{R}$ содержит все конечные неабелевы простые группы, простые делители порядков которых не превосходят 11 (см. [2]). Более того, сравнение множеств $\mathscr{R}$ и $\mathscr{S}_{13}$ показывает, что в множестве $\mathscr{S}_{13} \setminus \mathscr{R}$ лежат лишь две группы, а именно группы $L_6(3)$ и $U_4(5)$.

Основная цель настоящей работы — доказать, что группы $L_6(3)$ и $U_4(5)$ почти распознаваемы, и, следовательно, показать, что для всех групп в $\mathscr{S}_{13}$ проблема распознаваемости решена.

Теорема 1. *Пусть G — конечная простая группа $L_6(3)$ и H — конечная группа со свойством $\omega(H) = \omega(G)$. Тогда $H \simeq G$ или $H \simeq G\langle\gamma\rangle$, где γ — графовый автоморфизм группы G порядка 2. В частности, $h(G) = 2$.*

Теорема 2. *Пусть G — конечная простая группа $U_4(5)$ и H — конечная группа со свойством $\omega(H) = \omega(G)$. Тогда $H \simeq G$ или $H \simeq G\langle\gamma\rangle$, где γ — полевой автоморфизм группы G порядка 2. В частности, $h(G) = 2$.*

Следствие. *Для каждой группы G из $\mathscr{S}_{13}$ проблема распознаваемости решена. Значения $h(G)$ перечислены в последнем столбце табл.* 1.

§ 1. Предварительные сведения

Множество $\omega(H)$ конечной группы H замкнуто относительно делимости и однозначно определено множеством $\mu(H)$ тех элементов из $\omega(H)$, которые являются максимальными относительно делимости. Кроме того, множество $\omega(H)$ определяет граф Грюнберга — Кегеля (или граф простых чисел) $GK(H)$, вершинами которого являются все простые делители порядка группы H, и два простых числа p и q смежны, если H содержит элемент порядка $p \cdot q$. Обозначим через $s(H)$ число связных компонент графа $GK(H)$, а через $\pi_i(H)$, $i = 1, \dots, s(H)$, — его i-ю компоненту связности. Если H имеет четный порядок, то положим $2 \in \pi_1(H)$. Обозначим через $\mu_i(H)$ ($\omega_i(H)$) множество чисел $n \in \mu(H)$ ($n \in \omega(H)$) таких, что каждый простой делитель числа n принадлежит $\pi_i(H)$.

Лемма 1.1 (теорема Грюнберга — Кегеля). *Если H — конечная группа с несвязным графом $GK(H)$, то выполняется одно из условий:*

(а) *$s(H) = 2$ и H — группа Фробениуса;*

(б) *$s(H) = 2$ и $H = ABC$, где A, AB — нормальные подгруппы в H; AB, BC — группы Фробениуса с ядрами A, B и дополнениями B, C соответственно;*

Таблица 1. Конечные неабелевы простые группы,
простые делители порядков которых не превосходят 13

G	Порядок G	$\mathrm{Out}(G)$	$s(G)$	$h(G)$
A_5	$2^2 \cdot 3 \cdot 5$	2	3	1
$L_2(7)$	$2^3 \cdot 3 \cdot 7$	2	3	1
A_6	$2^3 \cdot 3^2 \cdot 5$	2^2	3	∞
$L_2(8)$	$2^3 \cdot 3^2 \cdot 7$	3	3	1
$L_2(11)$	$2^2 \cdot 3 \cdot 5 \cdot 11$	2	3	1
$L_2(13)$	$2^2 \cdot 3 \cdot 7 \cdot 13$	2	3	1
A_7	$2^3 \cdot 3^2 \cdot 5 \cdot 7$	2	3	1
$L_3(3)$	$2^4 \cdot 3^3 \cdot 13$	2	2	∞
$U_3(3)$	$2^5 \cdot 3^3 \cdot 7$	2	2	∞
$L_2(25)$	$2^3 \cdot 3 \cdot 5^2 \cdot 13$	2^2	3	1
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	1	3	1
$L_2(27)$	$2^2 \cdot 3^3 \cdot 7 \cdot 13$	6	3	1
A_8	$2^6 \cdot 3^2 \cdot 5 \cdot 7$	2	2	1
$L_3(4)$	$2^6 \cdot 3^2 \cdot 5 \cdot 7$	D_{12}	4	1
$U_4(2)$	$2^6 \cdot 3^4 \cdot 5$	2	2	∞
$\mathrm{Sz}(8)$	$2^6 \cdot 5 \cdot 7 \cdot 13$	3	4	1
$L_2(49)$	$2^4 \cdot 3 \cdot 5^2 \cdot 7^2$	2^2	3	1
$U_3(4)$	$2^6 \cdot 3 \cdot 5^2 \cdot 13$	4	2	1
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	2	2	1
$U_3(5)$	$2^4 \cdot 3^2 \cdot 5^3 \cdot 7$	S_3	2	∞
A_9	$2^6 \cdot 3^4 \cdot 5 \cdot 7$	2	2	1
$L_2(64)$	$2^6 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$	6	3	1
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	2	4	1
J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	2	2	∞
$S_6(2)$	$2^9 \cdot 3^4 \cdot 5 \cdot 7$	1	2	2
A_{10}	$2^7 \cdot 3^4 \cdot 5^2 \cdot 7$	2	1	∞
$U_4(3)$	$2^7 \cdot 3^6 \cdot 5 \cdot 7$	D_8	2	1
$G_2(3)$	$2^6 \cdot 3^6 \cdot 7 \cdot 13$	2	3	1
$S_4(5)$	$2^6 \cdot 3^2 \cdot 5^4 \cdot 13$	2	2	∞
$L_4(3)$	$2^7 \cdot 3^6 \cdot 5 \cdot 13$	2^2	2	1
$U_5(2)$	$2^{10} \cdot 3^5 \cdot 5 \cdot 11$	2	2	∞
${}^2F_4(2)'$	$2^{11} \cdot 3^3 \cdot 5^2 \cdot 13$	2	2	1
A_{11}	$2^7 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11$	2	2	1
$L_3(9)$	$2^7 \cdot 3^6 \cdot 5 \cdot 7 \cdot 13$	2^2	2	2
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	2	3	1
$S_4(7)$	$2^8 \cdot 3^2 \cdot 5^2 \cdot 7^4$	2	2	∞
$O_8^+(2)$	$2^{12} \cdot 3^5 \cdot 5^2 \cdot 7$	S_3	2	2
${}^3D_4(2)$	$2^{12} \cdot 3^4 \cdot 7^2 \cdot 13$	3	2	1

Продолжение таблицы 1

G	Порядок G	$\mathrm{Out}(G)$	$s(G)$	$h(G)$
A_{12}	$2^9 \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11$	2	2	1
$G_2(4)$	$2^{12} \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 13$	2	2	1
M^cL	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	2	2	1
$S_4(8)$	$2^{12} \cdot 3^4 \cdot 5 \cdot 7^2 \cdot 13$	6	2	∞
A_{13}	$2^9 \cdot 3^5 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	2	3	1
$S_6(3)$	$2^9 \cdot 3^9 \cdot 5 \cdot 7 \cdot 13$	2	2	2
$O_7(3)$	$2^9 \cdot 3^9 \cdot 5 \cdot 7 \cdot 13$	2	2	2
$U_6(2)$	$2^{15} \cdot 3^6 \cdot 5 \cdot 7 \cdot 11$	S_3	3	1
$U_4(5)$	$2^7 \cdot 3^4 \cdot 5^6 \cdot 7 \cdot 13$	2^2	1	2
A_{14}	$2^{10} \cdot 3^5 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13$	2	2	1
$L_5(3)$	$2^9 \cdot 3^{10} \cdot 5 \cdot 11^2 \cdot 13$	2	2	1
Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	2	3	1
A_{15}	$2^{10} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$	2	2	1
$O_8^+(3)$	$2^{12} \cdot 3^{12} \cdot 5^2 \cdot 7 \cdot 13$	S_4	2	2
A_{16}	$2^{14} \cdot 3^6 \cdot 5^3 \cdot 7^2 \cdot 11 \cdot 13$	2	1	1
Fi_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	2	2	1
$L_6(3)$	$2^{11} \cdot 3^{15} \cdot 5 \cdot 7 \cdot 11^2 \cdot 13^2$	2^2	2	2

(в) *существует такая неабелева простая группа S, что $S \leq \overline{H} = H/K \leq \mathrm{Aut}(S)$ для некоторой нильпотентной нормальной $\pi_1(H)$-подгруппы K из H и группа $\overline{H}/S$ является $\pi_1(H)$-подгруппой; более того, граф $GK(S)$ несвязен, $s(S) \geq s(H)$ и для любого числа i, $2 \leq i \leq s(H)$, существует j, $2 \leq j \leq s(S)$, такое, что $\omega_i(H) = \omega_j(S)$.*

Доказательство см. в [8].

Лемма 1.2. *Пусть S — конечная простая группа с несвязным графом $GK(S)$. Тогда $|\mu_i(S)| = 1$ для $2 \leq i \leq s(S)$. Обозначим через $n_i = n_i(S)$ единственный элемент в $\mu_i(S)$, $i \geq 2$. Тогда S, $\pi_1(S)$ и $n_i(S)$, $2 \leq i \leq s(S)$, будут такими, как в табл.* 2a–2c *из* [7].

Доказательство см. в [8–10].

Замечание. Теорема Грюнберга — Кегеля (лемма 1.1) и классификация всех конечных неабелевых простых групп с несвязным графом простых чисел (лемма 1.2) используются в большинстве работ, посвященных проблеме распознавания. На самом деле в списке $\mathscr{R}$ содержатся лишь две группы со связным графом простых чисел. А именно, знакопеременные группы A_{10} с $h(A_{10}) = \infty$ и A_{16} с $h(A_{16}) = 1$. Отметим, что группа $U_4(5)$, рассматриваемая в настоящей работе, также имеет связный граф простых чисел. Поскольку оказывается, что $h(U_4(5)) = 2$, эта группа является первым примером почти распознаваемой простой группы со связным графом простых чисел.

Лемма 1.3. *Пусть G — группа Фробениуса с ядром F и дополнением C. Тогда*

(а) *F нильпотентна. Если U — подгруппа порядка pq в C, где p и q — (необязательно различные) простые числа, то U циклическая. В частности,* *для каждого нечетного простого числа p силовская p-подгруппа группы C циклическая.*

(б) *Пусть H — конечная группа, $K \lhd H$ и $H/K = G$. Если C — циклическая, $(|F|, |K|) = 1$ и F не лежит в $KC_H(K)/K$, то $p|C| \in \omega(H)$ для некоторого простого делителя p порядка группы K.*

Доказательство см. в [1, лемма 1] и [11, лемма 1].

Следуя [12], обозначим через $A \cdot B$ $(A : B)$ расширение (расщепляемое расширение) группы A с помощью группы B, а через A^m — прямое произведение m изоморфных копий группы A. Кроме того, мы будем обозначать циклическую подгруппу порядка n просто через n, исключая случаи, когда это может привести к недоразумениям. Например, запись $2^2 : 3$ означает расщепляемое расширение элементарной абелевой 2-группы порядка 4 с помощью циклической группы порядка 3.

§ 2. Доказательство теоремы 1

Пусть G — конечная простая группа $L_6(3)$ и H — конечная группа со свойством $\omega(H) = \omega(G)$. Имеем $\mu(G) = \mu(H) = \{182, 121, 120, 104, 80, 78, 36\}$. Таким образом, $s(G) = 2$, и мы можем применить лемму 1.1. Результат, полученный в [13], позволяет нам исключить случаи (a) и (b) леммы. Поэтому мы приходим к следующей ситуации. Существует такая неабелева простая группа S, что $S \le \overline{H} = H/K \le \mathrm{Aut}(S)$ для некоторой нильпотентной нормальной $\pi_1(H)$-подгруппы K из H и группа $\overline{H}/S$ является $\pi_1(H)$-подгруппой. Более того, граф $GK(S)$ несвязен, $s(S) \ge s(H)$, и существует j, $2 \le j \le s(S)$, такое, что $\omega_2(H) = \omega_j(S)$. Очевидно, $\pi(S) \subseteq \pi(H) = \pi(G)$. Поэтому $S \subseteq \mathscr{S}_{13}$. С другой стороны, $n_2(H) = n_2(G) = 121$. Следовательно, одна из связных компонент графа $GK(S)$ должна быть равна $\{121\}$. В $\mathscr{S}_{13}$ только две группы удовлетворяют этому условию: $L_5(3)$ и сама G. Пусть $S \simeq L_5(3)$. Поскольку 7 не делит порядок группы $\mathrm{Aut}(S)$, силовская 7-подгруппа P группы H лежит в K. Так как группа K нильпотентна, подгруппа P нормальна в H. Поскольку $21 = 7 \cdot 3 \notin \omega(H)$, группа $P : R$, где R — силовская 3-подгруппа в H/K, является группой Фробениуса с ядром P и дополнением R. По лемме 1.3 R должна быть циклической. Но силовская 3-подгруппа группы $S \le H/K$, очевидно, циклической не является; противоречие.

Таким образом, $S \simeq G$, и мы будем писать G вместо S. Пусть $K \ne 1$. Поскольку K нильпотентна, используя индукцию по порядку группы H, мы можем полагать, что K — p-группа для некоторого простого числа p. Если мы возьмем фактор-группу $H/\Phi(K)$ вместо H, где $\Phi(K)$ — подгруппа Фраттини группы K, аналогичное индукционное рассуждение позволит нам рассматривать K как элементарную абелеву p-группу. Предположим, что $p \ne 3$. Группа G содержит подгруппу Фробениуса с ядром F порядка $3^5 = 243$ и циклическим дополнением C порядка $(3^5 - 1)/2 = 121$ (см. доказательство леммы 3 в [14]). Поскольку $p \ne 3$ и группа G проста, выполняются условия $(|F|, |K|) = 1$ и $C_H(K) = K$. По лемме 1.3 H содержит элемент порядка $121 \cdot p$; противоречие.

Таким образом, мы можем полагать, что K является 3-группой. Группа H/K содержит подгруппу L, изоморфную простой группе $S_6(3)$, которая действует на K сопряжениями. Изучение таблицы брауэровских 3-характеров для группы L из [15] показывает, что элемент $x \in L$ порядка 7 имеет неподвижную точку в любом абсолютно неприводимом модуле над полем характеристики 3. Таким образом, x централизует некоторый нетривиальный элемент в K, откуда

$21 \in \omega(H)$; противоречие.

Имеем $G \leq H \leq \mathrm{Aut}(G)$. Группа $\mathrm{Out}(G)$ — элементарная абелева группа порядка 4. Пусть δ — диагональный автоморфизм и γ — графовый автоморфизм группы G. Тогда $\mathrm{Aut}(G) = G\langle\delta,\gamma\rangle$. Действие δ и γ на G можно представить следующим образом. Пусть g обозначает образ в G матрицы A из $SL_6(3)$. Тогда g^δ — образ матрицы A^D, где $D = \mathrm{diag}\{1,1,1,1,1,-1\}$, и g^γ — образ матрицы A^{-T}, т. е. матрицы, обратной к транспонированной матрице A. Таким образом, $|\delta| = |\gamma| = 2$. Кроме того, так как $D^{-T} = D$, то δ и γ перестановочны и автоморфизм $\tau = \gamma\delta$ также имеет порядок 2.

Предположим, что $H \not\leq G\langle\gamma\rangle$. Поскольку D централизует в $SL_6(3)$ подгруппу, изоморфную $SL_5(3)$, δ централизует образ этой подгруппы в G. Значит, если $\delta \in H$, то в H найдется элемент порядка $121 \cdot 2$, что невозможно. Рассмотрим теперь в $SL_6(3)$ матрицу

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

Непосредственное вычисление показывает, что матрица $B = A \cdot (A^{-T})^D$ имеет порядок 24 и циклическая группа, порожденная B, тривиально пересекается с центром группы $SL_6(3)$. Если g — образ A в G, то $(g\tau)^2 = gg^{\gamma\delta}$ — образ B в G порядка 24. Следовательно, $g\tau$ имеет порядок 48. Поскольку $48 \notin \omega(H)$, имеем $\tau \notin H$.

Таким образом, $H \leq G\langle\gamma\rangle$. Используя GAP (см. [16]), мы получаем матричные представители A всех классов сопряженных элементов в $SL_6(3)$. Вычисление проективных порядков матриц вида AA^{-T} позволяет найти спектр группы $G\langle\gamma\rangle$. Оказывается, что $\omega(G) = \omega(G\langle\gamma\rangle)$. Значит, $H = G$ или $H = G\langle\gamma\rangle$, и $h(G) = 2$. Теорема доказана.

§ 3. Доказательство теоремы 2

Пусть G — конечная простая группа $U_4(5)$ и H — конечная группа со свойством $\omega(H) = \omega(G)$. Имеем $\mu(G) = \mu(H) = \{63, 60, 52, 24\}$. Граф простых чисел $GK(G) = GK(H)$ имеет следующий вид:

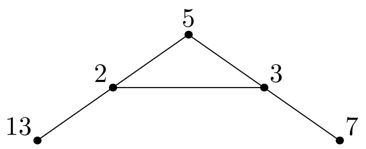

Рис. 1.

Поскольку граф связен, мы не можем применить лемму 1.1 напрямую. Поэтому доказательство будет более сложным и мы разделим его на несколько естественных шагов.

Лемма 3.1. *Пусть K — максимальная нормальная разрешимая подгруппа в H. Тогда только одно из трех простых чисел* 5, 7, 13 *может делить порядок K. В частности, H неразрешима.*

Доказательство. Сначала предположим, что все три простых числа 5, 7, 13 делят порядок K. Поскольку K разрешима, она содержит разрешимую холлову $\{5,7,13\}$-подгруппу R. Так как любые два простых числа из $\{5,7,13\}$ несмежны в $GK(H)$, то же верно и для $GK(R)$. Тогда $s(R)=3$ и R неразрешима по лемме 1.1; противоречие. Следовательно, $K\neq H$, и H неразрешима.

Пусть p,q,r — различные простые числа из $\{5,7,13\}$, взятые в произвольном порядке. Предположим, что два из них, для определенности p и q, делят $|K|$, а r не делит. Рассмотрим холлову $\{p,q\}$-подгруппу T в K. В силу аргумента Фраттини $H=KN_H(T)$. Следовательно, нормализатор $N=N_H(T)$ содержит элемент порядка r, который действует на T без неподвижных точек. Из леммы 1.3 следует, что T нильпотентна. Отсюда $p\cdot q\in\omega(T)\subseteq\omega(H)$; противоречие.

Лемма 3.2. *Существует конечная простая группа $S\in\mathscr{S}_{13}$ такая, что $S\leq\overline{H}=H/K\leq\mathrm{Aut}(S)$.*

Доказательство. Если мы обозначим через $L=S_1\times\cdots\times S_m$ цоколь группы $\overline{H}$, где S_i — неабелевы простые группы, то $\overline{H}\leq\mathrm{Aut}(L)$. Очевидно, что любая группа S_i лежит в $\mathscr{S}_{13}$. Поэтому нам надо лишь доказать, что $m=1$.

Предположим, что $m\geq 2$. По лемме 3.1 существует простое число $p\in\{7,13\}$, которое делит порядок $\overline{H}$. Предположим, что p делит $|L|$. Если $p=7$, то в L найдется элемент порядка $7\cdot 2$, что невозможно, так как $14\notin\omega(H)$. Если $p=13$, то либо $13\cdot 3\in\omega(H)$, либо каждая группа S_i является группой Сузуки $Sz(8)$ и, следовательно, $13\cdot 5\in\omega(H)$. В обоих случаях получается противоречие.

Таким образом, мы можем полагать, что p делит только порядок группы $\mathrm{Out}(L)$. Пусть $\varphi\in\overline{H}$ — автоморфизм группы L порядка p и $P=S_1^{\varphi}$. Поскольку P проста, любая ее естественная проекция P_i на S_i, $i=1,\ldots,m$, либо тривиальна, либо изоморфна S_1. С другой стороны, так как P нормальна в L, то нормальна и каждая подгруппа P_i, $i=1,\ldots,m$. Значит, $P_i=1$ или $P_i=S_i$. Следовательно, существует единственное число $j\in\{1,\ldots,m\}$ такое, что $S_1^{\varphi}=S_j$. Если $j\neq 1$, то возникает φ-орбита Δ длины p, состоящая из подгрупп, изоморфных S_1. Без потери общности мы можем полагать, что $\Delta=\{S_1,S_2,\ldots,S_p\}$. Пусть a_1 — элемент порядка t в S_1 и $a_i=a_1^{\varphi^i}$. Пусть g — элемент из L, проекции которого g_i на S_i определяются следующим образом: $g_i=a_i$ при $i=1,\ldots,p$ и $g_i=1$ в остальных случаях. Тогда g имеет порядок t, а элемент $g\varphi\in\overline{H}$ — порядок $t\cdot p$. Если $p=7$, возьмем элемент a_1 порядка $t=2$. Но $7\cdot 2\notin\omega(H)$; противоречие. Если $p=13$, то либо возьмем a_1 порядка 3, либо $S_1\simeq Sz(8)$ и мы возьмем a_1 порядка 5. В обоих случаях получим противоречие. Итак, $S_1^{\varphi}=S_1$, и то же самое верно для каждой S_i, $i=1,\ldots,m$. Поскольку $\varphi\neq 1$, φ действует нетривиально на некоторой S_k. Тогда φ индуцирует внешний автоморфизм группы S_k порядка p. Так как $S_k\in\mathscr{S}_{13}$, это невозможно (см. третий столбец табл. 1). Таким образом, $m=1$. Лемма доказана.

Лемма 3.3. $S\simeq G$.

Доказательство. Рассмотрим последовательно все возможности для группы S.

A. $S\simeq A_5,A_6,L_2(7),L_2(9),L_2(8),U_3(3),U_4(2),U_5(2),L_3(3)$. Поскольку $\mathrm{Out}(S)$ не делится на $5,7,13$ и только одно из этих чисел делит порядок S, получаем противоречие, используя лемму 3.1.

B. $S\simeq L_2(11),M_{11},M_{12},M_{22},HS,M^cL,U_6(2),L_5(3),Suz,Fi_{22},L_6(3)$ и A_n, где $n=11,\ldots,16$. Поскольку $11\in\omega(S)\setminus\omega(G)$, получается противоречие.

C.1. $S\simeq L_2(49)$. В этом случае $25\in\omega(S)\setminus\omega(G)$; противоречие.

C.2. $S \simeq L_2(64), S_4(8)$. Имеем $65 \in \omega(S) \setminus \omega(G)$, что невозможно.

C.3. $S \simeq {}^2F_4(2)', L_3(9)$. В этом случае $16 \in \omega(S) \setminus \omega(G)$; противоречие.

C.4. $S \simeq {}^3D_4(2), S_6(3), O_7(3), S_4(7), L_2(27)$. Поскольку $14 \in \omega(S) \setminus \omega(G)$, получаем противоречие.

D. $S \simeq L_3(4), U_3(5), J_2, S_6(2), U_4(3), O_8^+(2)$ и A_n, где $n = 7, \dots, 10$. Поскольку 13 не делит $|\operatorname{Aut}(S)|$, имеем $13 \in \omega(K)$. С другой стороны, все перечисленные группы содержат подгруппу, изоморфную $L_2(7)$ и, следовательно, содержат группу Фробениуса $F \simeq 7:3$. Рассмотрим фактор-группу $\widetilde{H} = H/O_{13'}(K)$. Имеем $P = O_{13}(\widetilde{H}) \neq 1$. Поэтому F действует на P точно и ее ядро порядка 7 действует на P без неподвижных точек. По лемме 1.3 в H существует элемент порядка $13 \cdot 3$; противоречие.

E. $S \simeq L_2(25), U_3(4), S_4(5), L_3(3)$. Поскольку $7 \in \omega(K)$ и S содержит подгруппу Фробениуса $5:2$, получаем $7 \cdot 2 \in \omega(H)$; противоречие.

F. $S \simeq L_2(13), G_2(3)$. Поскольку число 5 не делит $|\operatorname{Aut}(S)|$, оно делит порядок группы K. Так как $3 \cdot 7 \notin \omega(\operatorname{Aut}(S))$, то $\omega(K)$ содержит 7 или 9. Тогда из леммы 3.1 следует, что $9 \in \omega(K)$. Пусть T — холлова $\{3,5\}$-подгруппа в K. Поскольку 13 не делит порядок $|K|$, в $N_H(T)$ найдется элемент порядка 13, который действует на T без неподвижных точек. Значит, T нильпотентна. Поэтому $9 \cdot 5$ лежит $\omega(H)$; противоречие.

G. $S \simeq G_2(4)$. В силу того, что в $\operatorname{Aut}(S)$ нет элементов порядка 9, $|K|$ делится на 3. С другой стороны, S содержит подгруппу Фробениуса с ядром порядка 13 и циклическим дополнением порядка 6. Следовательно, $3 \cdot 6$ лежит в $\omega(H)$; противоречие.

H. $S \simeq Sz(8) \simeq {}^2B_2(8)$. Используя [12], получаем, что $\mu(S) = \{4, 5, 7, 13\}$, $|\operatorname{Out}(S)| = 3$ и $\mu(\operatorname{Aut}(S)) = \{7, 12, 13, 15\}$. Поскольку S содержит подгруппы Фробениуса $2^6 : 7$ и $13 : 4$, в K нет элементов порядка $5, 7, 13$. Кроме того, $4 \cdot 5, 9 \cdot 7 \in \omega(H)$, откуда $4, 9 \in \omega(K)$. Если $\overline{H} \simeq \operatorname{Aut}(S)$, то $\overline{H}$ содержит группу Фробениуса $13 : 12$ и, следовательно, в H существует элемент порядка 36; противоречие. Таким образом, $\overline{H} = S$ и K является $\{2,3\}$-группой.

Рассмотрим фактор-группу $\widetilde{H} = H/O_2(K)$ и ее подгруппу $\widetilde{K} = K/O_2(K)$. Предположим, что $O_{3,2}(\widetilde{K}) \neq O_3(\widetilde{K})$. Прежде всего отметим, что нетривиальная абелева группа $P = Z(O_2(\widetilde{K}/O_3(\widetilde{K})))$ действует на $O_3(\widetilde{K})$ точно. Кроме того, если $C = C_{\widetilde{H}/O_3(\widetilde{K})}(P)$ содержит элемент порядка 13, то $C = H/O_3(\widetilde{K})$. Отсюда $7 \cdot 2 \in \omega(H)$; противоречие. Пусть X — подгруппа порядка 13 из $\widetilde{H}/O_3(\widetilde{K})$. Подгруппа $F = [P, X] : X$ является группой Фробениуса с ядром $[P, X]$ и дополнением X. Группа F действует на $O_3(\widetilde{K})$ точно. Поэтому в H существует элемент порядка $3 \cdot 13$; противоречие. Таким образом, $O_{3,2}(\widetilde{K}) = O_3(\widetilde{K})$, и $O_2(K)$ является силовской 2-подгруппой в K.

Теперь обозначим через $\widetilde{H}$ и через $\widetilde{K}$ фактор-группы $H/O_3(K)$ и $K/O_3(K)$ соответственно. Предположим, что $O_{2,3}(\widetilde{K}) \neq O_2(\widetilde{K})$. Используя рассуждения, аналогичные рассуждениям в предыдущем абзаце, и элемент порядка 7 вместо элемента порядка 13, получим противоречие. Следовательно, $O_3(K)$ — силовская 3-подгруппа в K.

Итак, K является прямым произведением силовской 2-подгруппы и силовской 3-подгруппы. Значит, K содержит элемент порядка 36, что невозможно. Лемма доказана.

Таким образом, $S \simeq G$, и мы будем писать G вместо S.

Лемма 3.4. $G \leq H \leq \mathrm{Aut}(G)$.

Доказательство. Пусть $K \neq 1$. Существует такое простое число p, что $O^p(K) \neq K$. Обозначим через $\widetilde{H}$ фактор-группу $H/O^p(K)$. Нормальная подгруппа $\widetilde{K} = K/O^p(K)$ является нетривиальной p-группой. Обозначим через $\widehat{H}$ фактор-группу $\widetilde{H}/\Phi(\widetilde{K})$ и через $\widehat{K}$ фактор-группу $\widetilde{K}/\Phi(\widetilde{K})$, где $\Phi(\widetilde{K})$ — подгруппа Фраттини группы $\widetilde{K}$. Поскольку $H/K \simeq \widetilde{H}/\Phi(\widetilde{K})$, достаточно показать, что $\omega(\widehat{H}) \not\subseteq \omega(H)$. Поэтому мы предположим, что $H = \widehat{H}$ и K — нетривиальная элементарная абелева p-группа для некоторого простого числа p.

Предположим, что $C = C_H(K) \not\subseteq K$. Поскольку подгруппа CK нормальна в H, группа CK/K содержит G. Тогда H содержит элемент порядка $13 \cdot p$. Отсюда $p = 2$ и $2 \cdot 7 \in \omega(H)$; противоречие. Таким образом, мы можем предполагать, что $C \leq K$ и G действует на K точно.

Группа G содержит подгруппу $L_2(25)$, которая содержит подгруппу Фробениуса с ядром, изоморфным 5^2, и циклическим дополнением порядка 12. Если $p = 3, 7, 13$, имеем $p \cdot 12 \in \omega(H)$, что невозможно.

Пусть $p = 2$ или 5. Группа G содержит подгруппу L, изоморфную $U_3(5)$, которая действует на K сопряжениями. Изучение таблиц брауэровских p-характеров для группы L в [15] показывает, что элемент $x \in L$ порядка 7 имеет неподвижную точку в каждом абсолютно неприводимом модуле над полем характеристики p (т. е. 2 или 5). Таким образом, x централизует некоторый нетривиальный элемент в K и, значит, $p \cdot 7 \in \omega(H)$; противоречие. Лемма доказана.

Замечание. Случай $p = 5$ может быть исключен и другим способом, так как в $S_4(5) \leq G$ существует подгруппа Фробениуса $2^4 : 5$.

Лемма 3.5. *$H = G$ или $H = G\langle\gamma\rangle$, где γ — полевой автоморфизм группы G порядка 2.*

Доказательство. Имеем $G \leq H \leq \mathrm{Aut}(G)$. Прежде всего заметим, что G является централизатором в $L_4(25)$ автоморфизма $\sigma = \theta\gamma$, где θ — графовый автоморфизм и γ — полевой автоморфизм группы $L_4(25)$. Отсюда следует, что действие θ и действие γ на G совпадают. Мы зафиксируем обозначение γ для автоморфизма группы G, индуцированного этим действием.

Группа $\mathrm{Out}(G)$ элементарная абелева порядка 4. Пусть δ — диагональный автоморфизм и γ — полевой автоморфизм группы G. Тогда $\mathrm{Aut}(G) = G\langle\delta, \gamma\rangle$. Действие δ и γ на G можно представить следующим образом. Пусть g обозначает образ в G матрицы A из $SU_4(5)$. Тогда g^δ — образ матрицы A^D, где $D = \mathrm{diag}\{1, 1, 1, -1\}$, и g^γ — образ матрицы A^{-T}, т. е. матрицы, обратной к транспонированной матрице A (см. замечание в предыдущем абзаце). Таким образом, $|\delta| = |\gamma| = 2$. Кроме того, так как $D^{-T} = D$, то δ и γ перестановочны, и автоморфизм $\tau = \gamma\delta$ также имеет порядок 2.

Предположим, что $H \not\leq G\langle\gamma\rangle$. Поскольку D централизует в $SU_4(5)$ подгруппу, изоморфную $SU_3(5)$, δ централизует образ этой подгруппы в G. Значит, если $\delta \in H$, то в H найдется элемент порядка $7 \cdot 2$, что невозможно. Рассмотрим теперь в $SU_4(5)$ матрицу

$$A = \begin{pmatrix} \lambda & \lambda^2 & 0 & 0 \\ \lambda^{10} & \lambda^{17} & 0 & 0 \\ 0 & 0 & \lambda & \lambda^2 \\ 0 & 0 & \lambda^{10} & \lambda^{17} \end{pmatrix},$$

где λ порождает мультипликативную группу поля $\mathbf{F}_{5^2}$. Непосредственное вычисление показывает, что матрица $B = A \cdot (A^{-T})^D$ имеет порядок 20 и циклическая группа, порожденная B, тривиально пересекается с центром группы $SU_4(5)$. Если g — образ A в G, то $(g\tau)^2 = gg^{\gamma\delta}$ — образ B в G порядка 20. Следовательно, $g\tau$ имеет порядок 40. Поскольку $40 \notin \omega(H)$, имеем $\tau \notin H$.

Таким образом, $H \le G\langle\gamma\rangle$. Используя GAP (см. [16]), получаем матричные представители A всех классов сопряженных элементов в $SU_4(5)$. Вычисление проективных порядков матриц вида AA^{-T} позволяет найти спектр группы $G\langle\gamma\rangle$. Оказывается, что $\omega(G) = \omega(G\langle\gamma\rangle)$. Значит, $H = G$ или $H = G\langle\gamma\rangle$, и $h(G) = 2$. Теорема доказана.

Автор благодарен В. Д. Мазурову, М. А. Гречкосеевой, а также рецензенту данной статьи за полезные замечания по содержанию и оформлению работы.

ЛИТЕРАТУРА

1. *Мазуров В. Д.* О множестве порядков элементов конечной группы // Алгебра и логика. 1994. Т. 33, № 1. С. 81–89.
2. *Мазуров В. Д.* Распознавание конечных простых групп по множеству порядков их элементов // Алгебра и логика. 1998. Т. 37, № 6. С. 651–666.
3. *Shi W.* A characteristic property of $PSL_2(7)$ // J. Austral. Math. Soc. Ser. A. 1984. V. 36, N 3. P. 354–356.
4. *Shi W.* A characteristic property of A_5 // J. Southwest-China Teach. Univ. 1986. V. 3. P. 11–14.
5. *Shi W.* A characteristic property of J_1 and $PSL_2(2^n)$ // Adv. Math. 1987. V. 16. P. 397–401.
6. *Brandl R., Shi W.* The characterization of $PSL(2,q)$ by its element orders // J. Algebra. 1994. V. 163, N 1. P. 109–114.
7. *Mazurov V. D.* Characterizations of groups by arithmetic properties // Algebra Colloq. 2004. V. 11, N 1. P. 129–140.
8. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.
9. *Кондратьев А. С.* О компонентах графа простых чисел конечных простых групп // Мат. сб. 1989. Т. 180, № 6. С. 787–797.
10. *Кондратьев А. , Мазуров В. Д.* Распознавание знакопеременных групп простой степени по порядкам их элементов // Сиб. мат. журн. 2000. Т. 41, № 2. С. 359–371.
11. *Мазуров В. Д.* Характеризация конечных групп множествами порядков их элементов // Алгебра и логика. 1997. Т. 36, № 1. С. 37–53.
12. *Conway J. H., Curtis R. T., Norton S. P., Parker R. A., Wilson R. A.* Atlas of finite groups. Oxford: Clarendon Press, 1985.
13. *Алеева М. Р.* О конечных простых группах с множеством порядков элементов как у группы Фробениуса или двойной группы Фробениуса // Мат. заметки. 2003. Т. 73, № 3. С. 323–339.
14. *Заварницин А. В.* Порядки элементов в накрытиях групп $L_n(q)$ и распознаваемость знакопеременной группы A_{16}. Новосибирск, 2000. (Препринт/НИИДМИ; № 48).
15. *Jansen C., Lux K., Parker R. A., Wilson R. A.* An atlas of Brauer characters. Oxford: Clarendon Press, 1995.
16. *The GAP Group*, GAP — Groups, algorithms, and programming. Version 4.4. 2004 (http://www.gap-system.org).

Статья поступила 14 октября 2004 г.

Васильев Андрей Викторович
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
vdr@gorodok.net