В. Д. Мазуров, Распознавание конечных простых групп $S_4(q)$ по порядкам их элементов, *Алгебра и логика*, 2002, том 41, номер 2, 166–198

Алгебра и логика, 41, N 2 (2002), 166—198

УДК 512.542

РАСПОЗНАВАНИЕ КОНЕЧНЫХ ПРОСТЫХ ГРУПП $S_4(q)$ ПО ПОРЯДКАМ ИХ ЭЛЕМЕНТОВ*)

В. Д. МАЗУРОВ

Для конечной группы G обозначим через $\omega(G)$ множество порядков элементов группы G. Оно замкнуто относительно делимости и поэтому однозначно определено множеством $\mu(G)$ тех элементов из $\omega(G)$, которые являются максимальными по отношении делимости.

Группа G называется *распознаваемой по* $\omega(G)$ (короче, *распознаваемой*), если каждая конечная группа H, для которой $\omega(H) = \omega(G)$, изоморфна G. Иными словами, G распознаваема, если $h(G) = 1$, где $h(G)$ — число попарно неизоморфных групп H, для которых $\omega(H) = \omega(G)$. Список конечных простых групп, для которых в настоящее время известно, распознаваемы они или нет, приведен в § 7. В частности, в [1] было доказано, что для каждой простой симплектической группы $S = S_4(2^m)$ размерности 4 над полем порядка 2^n число $h(S)$ бесконечно.

Цель настоящей работы — доказать, что среди групп $S_4(q)$, где q нечетно, распознаваемы только группы $S_4(3^n)$, где число $n > 1$ и нечетно. Мы показываем также, что простые группы $U_3(9)$, ${}^3D_4(2)$, $G_2(4)$, $S_6(3)$, $F_4(2)$, ${}^2E_6(2)$ распознаваемы, а $L_3(3)$ нераспознаваема.

ОСНОВНАЯ ТЕОРЕМА. *Пусть $S = S_4(q)$ — конечная простая симплектическая группа размерности* 4 *над полем порядка q. Если $q =$*

*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект N 99-01-0550, Минобразования России в области фундаментального естествознания, грант Е00-1.0-77, и программы "Университеты России", грант УР.04.01.031.

$= 3^{2n+1} > 3$, *то* S *распознаваема. Во всех остальных случаях* $h(S) = \infty$.

Множество $\omega(H)$ конечной группы H определяет *граф Грюнберга—Кегеля* $GK(H)$: его вершинами служат все простые делители порядка H, а два простых числа p, q смежны, если H содержит элемент порядка pq. Обозначим через $s = s(H)$ число компонент связности графа $GK(H)$, а через $\pi_i = \pi_i(H)$ — i-тую компоненту связности, $i = 1, ..., s$. Если порядок группы H четен, положим $2 \in \pi_1$. Обозначим через $\mu_i = \mu_i(H)$ (соответственно, через $\omega_i = \omega_i(H)$) множество, состоящее из $n \in \mu(H)$ ($n \in \omega(H)$) таких, что каждый простой делитель числа n принадлежит π_i.

§ 1. Предварительные результаты

ЛЕММА 1 [2]. *Если* G — *конечная группа с несвязным графом* $GK(G)$, *то выполняется одно из следующих условий*:

1) $s(G) = 2$, G — *группа Фробениуса*;

2) $s(G) = 2$, $G = ABC$, *где* A, AB — *нормальные подгруппы в* G, B — *нормальная подгруппа в* BC *и* AB, BC — *группы Фробениуса*;

3) *Существует такая неабелева простая группа* P, *что* $P \leq \leq \overline{G} = G/K \leq \mathrm{Aut}(P)$ *для некоторой нильпотентной нормальной* $\pi_1(G)$*-подгруппы* K *из* G *и* $\overline{G}/P$ *является* $\pi_1(G)$*-группой. Более того, граф* $GK(P)$ *несвязен,* $s(P) \geqslant s(G)$ *и для любого числа* i, $2 \leqslant i \leqslant s(G)$, *существует* j, $2 \leqslant j \leqslant s(P)$, *такое, что* $\omega_i(G) = \omega_j(P)$.

ЛЕММА 2 [3]. *Пусть* P — *конечная простая группа с несвязным графом* $GK(P)$. *Тогда* $|\mu_i(P)| = 1$ *для* $2 \leqslant i \leqslant s(P)$. *Обозначим через* n_i *единственный элемент в* $\mu_i(P)$, $i \geqslant 2$. *Тогда* P, $\pi_1(P)$ *и* n_i, $2 \leqslant i \leqslant s(P)$, *будут такие, как в табл.* 1*a*—1*c*.

В табл. 1*a*—1*c* символом p обозначается нечетное простое число. Отметим, что в [3, табл. 1b, строки ${}^2G_2(q)$, $F_4(q)$, и табл. 1c, строка Fi'_{24}] имеются опечатки.

ЛЕММА 3. *Пусть* p — *простое число,* s — *натуральное число,* $s \geqslant 2$. *Тогда верно одно из следующих утверждений*:

Таблица 1а

Конечные простые группы P с $s(P) = 2$

P	Ограничения на P	$\pi_1(P)$	n_2
A_n	$6 < n = p, p+1, p+2$;	$\pi((n-3)!)$	p
	одно из чисел $n, n-2$ не просто		
$A_{p-1}(q)$	$(p,q) \neq (3,2), (3,4)$	$\pi(q\prod_{i=1}^{p-1}(q^i-1))$	$(q^p-1)/(q-1)(p,q-1)$
$A_p(q)$	$(q-1)\|(p+1)$	$\pi(q(q^{p+1}-1)\prod_{i=1}^{p-1}(q^i-1))$	$(q^p-1)/(q-1)$
${}^2A_{p-1}(q)$		$\pi(q\prod_{i=1}^{p-1}(q^i-(-1)^i))$	$(q^p+1)/(q+1)(p,q+1)$
${}^2A_p(q)$	$(q+1)\|(p+1)$,	$\pi(q(q^{p+1}-1)\prod_{i=1}^{p-1}(q^i-(-1)^i))$	$(q^p+1)/(q+1)$
	$(p,q) \neq (3,3), (5,2)$		
${}^2A_3(2)$		$\{2,3\}$	5
$B_n(q)$	$n = 2^m \geqslant 4$, q нечетно	$\pi(q\prod_{i=1}^{n-1}(q^{2i}-1))$	$(q^n+1)/2$
$B_p(3)$		$\pi(3(3^p+1)\prod_{i=1}^{p-1}(3^{2i}-1))$	$(3^p-1)/2$
$C_n(q)$	$n = 2^m \geqslant 2$	$\pi(q\prod_{i=1}^{n-1}(q^{2i}-1))$	$(q^n+1)/(2,q-1)$
$C_p(q)$	$q = 2, 3$	$\pi(q(q^p+1)\prod_{i=1}^{p-1}(q^{2i}-1))$	$(q^p-1)/(2,q-1)$
$D_p(q)$	$p \geqslant 5$, $q = 2, 3, 5$	$\pi(q\prod_{i=1}^{p-1}(q^{2i}-1))$	$(q^p-1)/(q-1)$
$D_{p+1}(q)$	$q = 2, 3$	$\pi(q(q^p+1)\prod_{i=1}^{p-1}(q^{2i}-1))$	$(q^p-1)/(2,q-1)$
${}^2D_n(q)$	$n = 2^m \geqslant 4$	$\pi(q\prod_{i=1}^{n-1}(q^{2i}-1))$	$(q^n+1)/(2,q+1)$
${}^2D_n(2)$	$n = 2^m+1 \geqslant 5$	$\pi(2(2^n+1)\prod_{i=1}^{n-2}(2^{2i}-1))$	$2^{n-1}+1$

$^2D_p(3)$	$5 \leqslant p \neq 2^m+1$	$\pi(3\prod_{i=1}^{p-1}(3^{2i}-1))$	$(3^p+1)/4$
$^2D_n(3)$	$9 \leqslant n = 2^m+1 \neq p$	$\pi(3(3^n+1)\prod_{i=1}^{n-2}(3^{2i}-1))$	$(3^{n-1}+1)/2$
$G_2(q)$	$2 < q \equiv \varepsilon \pmod 3$, $\varepsilon = \pm 1$	$\pi(q(q^2-1)(q^3-\varepsilon))$	$q^2-\varepsilon q+1$
$^3D_4(q)$		$\pi(q(q^6-1))$	q^4-q^2+1
$F_4(q)$	q нечетно	$\pi(q(q^6-1)(q^8-1))$	q^4-q^2+1
$^2F_4(2)'$		$\{2,3,5\}$	13
$E_6(q)$		$\pi(q(q^5-1)(q^8-1)(q^{12}-1))$	$(q^6+q^3+1)/(3,q-1)$
$^2E_6(q)$	$q>2$	$\pi(q(q^5+1)(q^8-1)(q^{12}-1))$	$(q^6-q^3+1)/(3,q+1)$
M_{12}		$\{2,3,5\}$	11
J_2		$\{2,3,5\}$	7
Ru		$\{2,3,5,7,13\}$	29
He		$\{2,3,5,7\}$	17
McL		$\{2,3,5,7\}$	11
Co_1		$\{2,3,5,7,11,13\}$	23
Co_3		$\{2,3,5,7,11\}$	23
Fi_{22}		$\{2,3,5,7,11\}$	13
HN		$\{2,3,5,7,11\}$	19

Таблица 1b

Конечные простые группы P с $s(P) = 3$

P	Ограничения на P	$\pi_1(P)$	n_2	n_3
A_n	$n > 6$, $n = p, p-2$ — простые числа	$\pi((n-3)!)$	p	$p-2$
$A_1(q)$	$3 < q \equiv \varepsilon \pmod 4$, $\varepsilon = \pm 1$	$\pi(q-\varepsilon)$	$\pi(q)$	$(q+\epsilon)/2$
$A_1(q)$	$q > 2$, q четно	$\{2\}$	$q-1$	$q+1$
$^2A_5(2)$		$\{2,3,5\}$	7	11
$^2D_p(3)$	$p = 2^m+1$	$\pi(3(3^{p-1}-1)\prod_{i=1}^{p-2}(3^{2i}-1))$	$(3^{p-1}+1)/2$	$(3^p+1)/4$
$G_2(q)$	$q \equiv 0 \pmod 3$	$\pi(q(q^2-1))$	q^2-q+1	q^2+q+1
$^2G_2(q)$	$q = 3^{2m+1} > 3$	$\pi(q(q^2-1))$	$q-\sqrt{3q}+1$	$q+\sqrt{3q}+1$
$F_4(q)$	q четно	$\pi(q(q^4-1)(q^6-1))$	q^4+1	q^4-q^2+1
$^2F_4(q)$	$q = 2^{2m+1} > 2$	$\pi(q(q^3+1)(q^4-1))$	$q^2-\sqrt{2q^3}+q-\sqrt{2q}+1$	$q^2+\sqrt{2q^3}+q+\sqrt{2q}+1$
$E_7(2)$		$\{2,3,5,7,11,13,17,19,31,43\}$	73	127
$E_7(3)$		$\{2,3,5,7,11,13,19,37,41,61,73,547\}$	757	1093
M_{11}		$\{2,3\}$	5	11
M_{23}		$\{2,3,5,7\}$	11	23
M_{24}		$\{2,3,5,7\}$	11	23
J_3		$\{2,3,5\}$	17	19
HiS		$\{2,3,5\}$	7	11
Suz		$\{2,3,5,7\}$	11	13
Co_2		$\{2,3,5,7\}$	11	23

Fi_{23}		$\{2,3,5,7,11,13\}$	17	23
F_3		$\{2,3,5,7,13\}$	19	31
F_2		$\{2,3,5,7,11,13,17,19,23\}$	31	47

Таблица 1с

Конечные простые группы P с $s(P) > 3$

$s(P)$	P	Ограничения на P	$\pi_1(P)$	n_2	n_3	n_4	n_5	n_6
4	$A_2(4)$		$\{2\}$	3	5	7		
	${}^2B_2(q)$	$q = 2^{2m+1} > 2$	$\{2\}$	$q-1$	$q-\sqrt{2q}+1$	$q+\sqrt{2q}+1$		
	${}^2E_6(2)$		$\{2,3,5,7,11\}$	13	17	19		
	$E_8(q)$	$q \equiv 2,3 \pmod 5$	$\pi(q(q^8-1)(q^{14}-1)(q^{12}-1)(q^{18}-1)$ $(q^{20}-1))$	$\frac{q^{10}-q^5+1}{q^2-q+1}$	$\frac{q^{10}+q^5+1}{q^2+q+1}$	q^8-q^4+1		
	M_{22}		$\{2,3\}$	5	7	11		
	J_1		$\{2,3,5\}$	7	11	19		
	$O'N$		$\{2,3,5,7\}$	11	19	31		
	LyS		$\{2,3,5,7,11\}$	31	37	67		
	Fi'_{24}		$\{2,3,5,7,11,13\}$	17	23	29		
	F_1		$\{2,3,5,7,11,13,17,19,23,29,31,47\}$	41	59	71		
5	$E_8(q)$	$q \equiv 0,1,4 \pmod 5$	$\pi(q(q^8-1)(q^{10}-1)(q^{12}-1)(q^{14}-1)$ $(q^{18}-1))$	$\frac{q^{10}-q^5+1}{q^2-q+1}$	$\frac{q^{10}+q^5+1}{q^2+q+1}$	q^8-q^4+1	$\frac{q^{10}+1}{q^2+1}$	
6	J_4		$\{2,3,5,7,11\}$	23	29	31	37	43

а) *существует простое число* q, *что* q *делит* $p^s - 1$ *и* q *не делит* $p^t - 1$ *при любом натуральном* $t < s$;

б) $s = 6$ *и* $p = 2$;

в) $s = 2$ *и* $p = 2^t - 1$ *для некоторого натурального числа* t.

ДОКАЗАТЕЛЬСТВО см. в [8].

Простое число q, удовлетворяющее п. "а", называется *примитивным* простым делителем числа $p^s - 1$.

ЛЕММА 4. а) *Пусть* $x = 3^a < 3^b = y < 3^{2s}$, *где* a, b, s — *неотрицательные целые числа. Если одно из чисел* $x \pm y$ *делится на* $3^s + 1$, *то* $b = a + s$.

б) *Если* $s \in \mathbb{N}$ *и* $a, b, c < 2s$ — *попарно различные неотрицательные целые числа, то либо одно из чисел вида* $2 \cdot 3^a \pm 3^b \pm 3^c$ *делится на* 5, *либо ни одно из этих чисел не делится на* $2(1 + 3^s)$.

в) *Если* $a_1, a_2, ..., a_t$ — *целые числа, не делящиеся на* 5 *и* $t \geqslant 4$, *то найдутся такие числа* $\varepsilon_i = \pm 1, i = 1, 2, ..., t$, *что* $\sum\limits_{i=1}^{t} \varepsilon_i a_i$ *делится на* 5.

ДОКАЗАТЕЛЬСТВО. а) Очевидно.

б) Можно считать, что $a = 0$ или $c = 0$. При этом только числа $2 + 3^{s+1} - 3^s$ и $2 \cdot 3^{s-1} - 3^{2s-1} + 1$ требуемого вида делятся на $2(1 + 3^s)$. Поскольку $3^{2s-1} \equiv \pm 3 \pmod 5$ и числа вида $\pm 3 \pm 1$ (соответственно, вида $\pm 3^{s+1} \pm 3^s$) составляют полную систему ненулевых вычетов по модулю 5, одно из чисел $2 \cdot 3^{s-1} \pm 3^{2s-1} \pm 1$ (соответственно, одно из чисел $2 \pm 3^{s+1} \pm 3^s$) делится на 5.

в) Заметим, что верно более общее утверждение, а именно, множество $\left\{ \sum\limits_{i=1}^{t} \varepsilon_i a_i + 5\mathbb{Z} \;\middle|\; \varepsilon_i = \pm 1,\ i = 1, 2, ..., t \right\}$ совпадает с $\mathbb{Z}/5\mathbb{Z}$. Его легко доказать для $t = 4$ (достаточно рассмотреть только четверки (a_1, a_2, a_3, a_4) из множества $\{(1, 1, 1, 1), (1, 1, 1, 2), (1, 1, 2, 2)\}$). Для $t > 4$ достаточно рассмотреть смежные классы вида $\sum\limits_{i=1}^{4} \varepsilon_i a_i + a_5 + \ldots + a_t + 5\mathbb{Z}$.

§ 2. Порядки элементов в накрытиях групп Фробениуса

ЛЕММА 5. *Пусть* G — *группа Фробениуса с ядром* H *и дополнением* C. *Тогда* $GK(H)$, $GK(C)$ — *компоненты связности графа* $GK(G)$ *и* *имеют место следующие утверждения:*

а) *Подгруппа H нильпотентна. В частности, $|\mu(H)| = 1$ и граф $GK(H)$ полный, т. е. любые две вершины в $GK(H)$ смежны.*

б) *Любая подгруппа из C порядка pq, где p и q — (не обязательно различные) простые числа, является циклической. В частности, любая силовская подгруппа нечетного порядка из C является циклической, а силовская 2-подгруппа из C — либо циклической, либо (обобщенной) кватернионной группой. Если $|C|$ — четное число, то порядок центра группы C четен. Если C содержит элемент порядка 16, то C обладает нормальным 2-дополнением. Подгруппа C_0, порожденная всеми элементами простого порядка из C, изоморфна $Z \times C_1$, где Z — циклическая группа, а подгруппа C_1 либо тривиальна, либо изоморфна одной из групп $SL_2(3), SL_2(5)$. Кроме того, либо C разрешима и граф $GK(C)$ полный, либо C содержит нормальную подгруппу $L \simeq SL_2(5)$ такую, что $(|L|, |C : L|) \leqslant 2$, и граф $GK(C)$ получается из полного графа на $\pi(C)$ удалением ребра $(3, 5)$.*

ДОКАЗАТЕЛЬСТВО. Лемма вытекает из таких результатов: п. "а" — это теорема Томпсона [4], п. "б" — из классификации дополнений Фробениуса (см. [5, 6]).

ЛЕММА 6. *Пусть G — конечная группа, $N \lhd G$, G/N — группа Фробениуса с ядром F и циклическим дополнением C. Если $(|F|, |N|) = 1$ и F не содержится в $NC_G(N)/N$, то $p|C| \in \omega(G)$ для некоторого простого делителя p числа $|N|$.*

ДОКАЗАТЕЛЬСТВО. Эта лемма — часть леммы 1 из [7].

ЛЕММА 7. *Пусть выполняются условия случая 2 леммы 1. Тогда для $t = |C|$ справедливо следующее:*

1) *Подгруппа A нильпотентна, B — циклическая группа нечетного порядка, C — циклическая группа, и G содержит элемент порядка $t \prod_{p\in\pi(A)} p$. В частности, $GK(B), GK(AC)$ — связные компоненты графа $GK(G)$ и являются полными графами.*

2) *Если подгруппа A абелева и m — наибольший общий делитель*

порядков элементов из A, то для порождающего элемента c группы C существует элемент $a \in A$ такой, что $(ac^{-1})^t$ — элемент порядка m в $C_A(C)$. В частности, порядок элемента ac^{-1} равен mt.

3) *Если $t = 3$, $|A|$ не делится на 3 и подгруппа $C_A(C)$ элементарная абелева, то факторы нижнего центрального ряда группы A элементарные абелевы и ступень нильпотентности группы A не выше двух.*

ДОКАЗАТЕЛЬСТВО. 1) Содержится в [1].

2) Достаточно рассмотреть случай $m = p^n$, где p — простое число. Пусть $A_1 = \{a^{p^{n-1}} \mid a \in A\}$. Известно (см., напр., [7, док-во леммы 1]), что группа A_1, рассматриваемая как C-модудь над полем F_p порядка p, содержит регулярный C-подмодуль, иными словами существует $x \in A_1$ такой, что элементы x^{c^i}, $i = 0, 1, ..., t$, линейно независимы. Пусть $x = a^{p^{n-1}}$, $a \in A$. Тогда

$$\langle a^{c^i} \mid i = 0, 1, ..., t-1\rangle = \langle a\rangle \times \langle a^c\rangle \times \ldots \times \langle a^{c^{t-1}}\rangle. \qquad (1)$$

В самом деле, предположим, что $a^{m_0}a^{cm_1}\cdots a^{c^{t-1}m_{t-1}} = 1$, где m_i — целое число, $i = 0, 1, ..., t-1$. Тогда

$$x^{m_0}x^{cm_1}\cdots x^{c^{t-1}m_{t-1}} = (a^{m_0}a^{cm_1}\cdots a^{c^{t-1}m_{t-1}})^{p^{n-1}} = 1$$

и поэтому $m_i = pl_i$, где l_i — целое число, $i = 0, 1, ..., t-1$. По той же причине, $x^{l_0}x^{cl_1}\cdots x^{c^{t-1}l_{t-1}} = 1$, и следовательно, $l_i = pk_i$, где k_i целое, $i = 0, 1, ..., t-1$. Повторив $n-1$ раз, получим, что m_i, $i = 0, 1, ..., t-1$, делятся на p^n, т. е. $a^{m_0} = a^{cm_1} = \ldots = a^{c^{t-1}m_{t-1}} = 1$, и (1) доказано. Теперь из (1) следует, что порядок элемента $y = aa^c\cdots a^{c^{t-1}} = (ac^{-1})^t$ равен p^n и $y \in C_A(C)$.

3) Можно считать, что $q = |B|$ — простое число. Положим $B = \langle b\rangle$, $C = \langle c\rangle$ и $b^c = b^r$ для некоторого целого числа r. Отметим, что $r^2 + r + 1$ делится на q.

По п. 2 подгруппа A является p-группой для некоторого простого числа p, и все факторы ее нижнего центрального ряда элементарные абелевы. Таким образом, ассоциированное кольцо Ли L группы A (см. в [13] определение и соответствующие факты) является алгеброй над полем F_p

порядка p, BC действует на L, и $C_L(C)$ — абелева подалгебра. Кроме того, B действует на L регулярно. То же самое остается справедливым после замены L на $\widehat{L} = L\bigotimes_{F_p} F$, где F — расширение поля F_p, содержащее нетривиальный корень степени q из единицы. Для доказательства нам потребуется следующее утверждение:

(7.1) *Пусть $x, y \in \widehat{L}$ такие, что $xb = \alpha x, yb = \beta y$, где $\alpha, \beta \in F$ и $[x,y] \neq 0$. Тогда $\beta = \alpha^r$ или $\beta = \alpha^{r^2}$, а $[x,y]b = \alpha^{-r^2}[x,y]$ или $[x,y]b = = \alpha^{-r}[x,y]$ соответственно.*

Чтобы доказать (7.1), заметим, что $\alpha \neq 1 \neq \beta$, $\alpha^q = \beta^q = 1$, и поэтому $\alpha^{r^2+r+1} = \beta^{r^2+r+1} = 1$. Кроме того,

$$\begin{gathered}(xc)b = xb^{r^2}c = \alpha^{r^2}(xc),\ (xc^2)b = \alpha^r(xc^2),\\ (yc)b = \beta^{r^2}(xc),\ (yc^2)b = \beta^r(xc^2).\end{gathered} \tag{2}$$

Тогда векторы x, xc, xc^2 линейно независимы, и то же самое верно для y, yc, yc^2. Векторы $x + xc + xc^2$, $y + yc + yc^2$ содержатся в $C_{\widehat{L}}(C)$, и поэтому

$$[x + xc + xc^2, y + yc + yc^2] = \sum_{i,j=0}^{2} [xc^i, yc^j] = 0. \tag{3}$$

По (2), $[xc^i, yc^j]$, $i,j = 0,1,2$, является собственным вектором для b с собственным значением $\alpha^{r^{2i}}\beta^{r^{2j}}$, поэтому $\alpha^{r^{2i}}\beta^{r^{2j}} \neq 1$, и по (3) существует пара $(i,j) \neq (0,0)$ такая, что $\alpha\beta = \alpha^{r^{2i}}\beta^{r^{2j}}$. Очевидно, что если $i = 0$, то $j = 0$ и наоборот. Тогда $1 \neq \alpha^{1-r^{2i}} = \beta^{r^{2j}-1}$ и, поскольку $\alpha\beta \neq 1$, либо $i = 1$, $j = 2$ и $\beta = \alpha^{-1-r} = \alpha^{r^2}$, либо $i = 2$, $j = 1$ и $\beta = \alpha^{-1-r^2} = \alpha^r$. Следовательно, $[x,y]b = \alpha\beta[x,y] = \alpha^{1+r^2}[x,y] = \alpha^{-r}[x,y]$ или $[x,y]b = = \alpha^{1+r}[x,y] = \alpha^{-r^2}[x,y]$, и (7.1) доказано.

Как векторное пространство над полем F, алгебра $\widehat{L}$ обладает базой, состоящей из собственных векторов элемента b, поэтому, если ступень нильпотентности $\widehat{L}$ больше двух, существуют такие собственные векторы u, v, w для b, что $[u,v,w] \neq 0$. Пусть $ub = \alpha u$. Поскольку $[u,v] \neq 0$ и по (7.1), или $vb = \alpha^r v$ и $[u,v]b = \alpha^{-r^2}[u,v]$, или $vb = \alpha^{r^2}v$ и $[u,v]b = \alpha^{-r}[u,v]$. Полагая $x = [u,v], y = w$ в (7.1), получим

$$wb = \alpha^s w,\ \text{где } s = -1, -r \text{ или } -r^2. \tag{4}$$

С другой стороны, $[u,v,w] = -[v,w,u]-[w,u,v]$, поэтому или $[v,w] \neq \neq 0$, или $[w,u] \neq 0$. Снова по (7.1), $wb = \alpha^s w$, где s равно 1, r или r^2, что противоречит (4). Следовательно, ступень нильпотентности алгебры $\widehat{L}$, а значит, и группы A, не превосходит двух. Лемма доказана.

ЛЕММА 8. *Пусть C — нетривиальная конечная группа, в которой подгруппа C_0, порожденная всеми элементами простых порядков, изоморфна $Z \times C_1$, где $(|Z|,|C_1|) = 1$, Z — циклическая группа, а C_1 либо тривиальна, либо изоморфна одной из групп $SL_2(3), SL_2(5)$. Если $m > 1$ — натуральное число, взаимно простое с $|C|$, то существует конечная группа Фробениуса с абелевым ядром, содержащим элемент порядка m, и дополнением, изоморфным C.*

ДОКАЗАТЕЛЬСТВО. Достаточно рассмотреть случай, когда $m = = p^n$, где p — простое число. Существует натуральное число s, для которого $p^s - 1$ делится на $|C_0|$. Группа $SL_2(p^s)$ содержит подгруппу A, изоморфную C_1, а центр группы $GL_2(p^s)$ — подгруппу B, изоморфную Z, при этом любой нетривиальный элемент из $\langle A, B\rangle = A \times B$ не имеет нетривиальных неподвижных точек при действии на естественном $GL_2(p^s)$-модуле V над полем порядка p^s. Иными словами, V является C_0-модулем, и естественное полупрямое произведение VC_0 будет группой Фробениуса с ядром V и дополнением C_0. Пусть W — это C-модуль, индуцированный C_0-модулем V. Тогда W — прямая сумма C_0-подмодулей, сопряженных с V, и поэтому WC_0 также является группой Фробениуса. Поскольку C_0 содержит все элементы простого порядка из C, группой Фробениуса является и WC. Пусть $|W| = p^r$ и U — прямое произведение r циклических подгрупп порядка m. Тогда $U/U^p \simeq W$ и $\mathrm{Aut}(U)/I \simeq \mathrm{Aut}(W)$, где I состоит из автоморфизмов группы U, действующих тривиально на U/U^p. Поскольку I является p-группой и p не делит $|C|$, $\mathrm{Aut}(U)$ содержит подгруппу H, изоморфную C, которая действует на U/U^p подобно тому, как C действует на W. Следовательно, полупрямое произведение UH является искомой группой Фробениуса.

§ 3. Представления некоторых групп

ЛЕММА 9. *Пусть H — расширение нетривиальной конечной 3-группы V посредством симметрической группы S_6 степени 6. Тогда H содержит элемент порядка* 15 *или* 18.

ДОКАЗАТЕЛЬСТВО. Достаточно рассмотреть случай, когда V — абсолютно неприводимый S_6-модуль. Если χ — соответствующий характер Брауэра, то, в силу [9], χ совпадает с одним из характеров X_i, приведенных в следующей таблице:

Характеры Брауэра группы $S_6 \pmod 3$

	1A	2A	4A	5A	2B	2C	4B
X_1	1	1	1	1	1	1	1
X_2	1	1	1	1	−1	−1	−1
X_3	6	−2	2	1	.	.	.
X_4	4	.	−2	−1	2	−2	.
X_5	4	.	−2	−1	−2	2	.
X_6	9	1	1	−1	3	3	−1
X_7	9	1	1	−1	−3	−3	1

Предположим, что заключение леммы не верно. Тогда, очевидно, $\dim(C_V(x)) = 0$ для любого элемента порядка 5 из S_6. Легко вычислить, что $\dim(C_V(x)) = (\chi(1A)+4\chi(5A))/5 = 0$ для $x \in 5A$ только в том случае, если $\chi(1A) = 4$. В этом случае для некоторой инволюции $i \in S_6 \setminus A_6$ и любой элементарной абелевой подгруппы U порядка 4 из $C_{A_6}(i)$ справедливо $1 = \dim(C_V(U)) < \dim(C_V(i))$, и поэтому подгруппа из $C_{A_6}(i)$, изоморфная A_4, действует на $C_V(i)$ точно. По лемме 6, $C_H(i)$ содержит элемент порядка 9, и поэтому H содержит элемент порядка 18.

ЛЕММА 10. *Пусть F — конечное поле порядка $q = p^n > 3$, где p — простое число, и $W_i = W_i(q)$, $i = 0, 1, ..., p-1$, — пространство однородных полиномов степени i от переменных x_1, x_2 над F. Пусть α —*

автоморфизм F, отображающий каждый элемент из F в его p-тую степень. Для $j = 0, ..., n-1$ превратим W_i в $SL_2(q)$-модуль $W_i^j = W_i^j(q)$, положив $f(x_1, x_2)a = f(a_{11}^{\alpha^j}x_1 + a_{12}^{\alpha^j}x_2, a_{21}^{\alpha^j}x_1 + a_{22}^{\alpha^j}x_2)$ для $f(x_1, x_2) \in W_i$ и $a = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in SL_2(q)$. В частности, W_0^j будет тривиальным одномерным $SL_2(q)$-модулем.

1) *Модули $W(i_0, ..., i_{n-1}) = \bigotimes_{j=0}^{n-1} W_{i_j}^j$ составляют полное множество попарно неэквивалентных абсолютно неприводимых $SL_2(q)$-модулей над полем характеристики p. Если q нечетно, то центр группы $SL_2(q)$ действует тривиально на $W(i_0, ..., i_{n-1})$ (и поэтому $W(i_0, ..., i_{n-1})$ является $L_2(q)$-модулем) в точности тогда, когда $i_0 + \ldots + i_{n-1}$ — четное число.*

2) *Если λ, λ^{-1} — характеристические числа элемента $a \in SL_2(q)$, то характеристическими корнями a в W_1^j будут $\lambda^{p^j}, \lambda^{-p^j}$, в W_2^j — $1, \lambda^{2p^j}, \lambda^{-2p^j}$ и в $W(i_0, ..., i_{n-1})$ — $\lambda_{i_0} \cdots \lambda_{i_{n-1}}$ (где λ_{i_j} — характеристические корни a в W_i^j).*

ДОКАЗАТЕЛЬСТВО. 1) Это хорошо известный результат Брауэра и Несбит [10]. В качестве базы векторного пространства W_i можно взять $x_1^i, x_1^{i-1}x_2, ..., x_2^i$ и эта база не зависит от q. Поэтому $W_i^j(q)$ можно расширить до $W_i^j(q^s)$ для любого s, и для того, чтобы доказать п. 2, можно считать, что a треугольна.

2) Для треугольных a это очевидно.

§ 4. Группы $S_4(q)$, $q \neq 3^n$

Пусть $S = S_4(q)$, $q \neq 3^n$. В этом параграфе докажем, что $h(S) = \infty$. Случай четного q рассмотрен в [1], поэтому при доказательстве основной теоремы будем предполагать, что $q = p^n$, p — нечетное простое число. На протяжении этого параграфа считаем, что $p \neq 3$.

ЛЕММА 11. *Множество $\omega(S)$ состоит из всех делителей чисел $(q^2+1)/2$, $(q^2-1)/2$, $p(q+1)$, $p(q-1)$.*

ДОКАЗАТЕЛЬСТВО см. в [11].

ПРЕДЛОЖЕНИЕ 1. *Пусть $L = L_2(q^2)$, где $q = p^n$, $p > 3$ — простое число. Пусть $V = W_1^0 \otimes W_1^n$ — L-модуль, где модуль W_i^j определен в лемме 10. Тогда V можно рассматривать как $\underline{L}$-модуль, где $\underline{L} = L\langle\sigma\rangle$ и σ — полевой автоморфизм порядка 2 группы L, и для естественного полупрямого произведения $E = V\underline{L}$ имеет место равенство $\omega(L) = \omega(S_4(q))$. В частности, $h(S_4(q)) = \infty$.*

ДОКАЗАТЕЛЬСТВО. Используем обозначения леммы [10]. Определим действие автоморфизма σ на $W_1^0 \otimes W_1^n$ по правилу $\left(\sum\limits_{i,j=1}^{2} a_{ij}(x_i \otimes x_j)\right)\sigma = \sum\limits_{i,j=1}^{2} a_{ij}(x_j \otimes x_i)$. Легко проверить, что тем самым V превращается в $\underline{L}$-модуль.

Для $x \in SL_2(q^2)$ обозначим через $\overline{x}$ образ x в L. Пусть $L \ni a = \overline{\begin{pmatrix} 0 & \lambda \\ -1/\lambda & 0 \end{pmatrix}}\sigma$, где λ — примитивный корень (q^2-1)-й степени из единицы. Тогда порядок a четен,

$$a^2 = \overline{\begin{pmatrix} 0 & \lambda \\ -1/\lambda & 0 \end{pmatrix}\begin{pmatrix} 0 & \lambda \\ -1/\lambda & 0 \end{pmatrix}^{\sigma}} = \overline{\begin{pmatrix} -\lambda^{1-q} & 0 \\ 0 & -\lambda^{q-1} \end{pmatrix}}$$

и порядок a равен $q+1$.

Векторы $v_1 = x_1 \otimes x_1, v_2 = x_1 \otimes x_2, v_3 = x_2 \otimes x_1, v_4 = x_2 \otimes x_2$ составляют базу пространства V. Так как $v_1 a = \lambda^{1+q} v_4, v_4 a = \lambda^{-1-q} v_1$, то a оставляет неподвижным нетривиальный вектор в подпространстве, натянутом на v_1, v_4, поэтому E содержит элемент порядка $p(q+1)$.

Пусть $b = \overline{\begin{pmatrix} \lambda & 0 \\ 0 & -1/\lambda \end{pmatrix}}\sigma$. Тогда порядок b четен, $b^2 = \overline{\begin{pmatrix} \lambda^{1+q} & 0 \\ 0 & \lambda^{-q-1} \end{pmatrix}}$ и порядок элемента b равен $q-1$. Так как $v_2 b = \lambda^{1-q} v_3, v_3 b = \lambda^{q-1} v_2$, то E содержит элемент порядка $p(q-1)$. Поскольку $\omega(L)$ содержит числа $(q^2+1)/2$, $(q^2-1)/2$ и в силу леммы 11, имеем $\omega(S_4(q)) \subseteq \omega(E)$.

Пусть a — элемент из E. Предположим вначале, что подгруппа $\langle a\rangle \cap V$ нетривиальна. Тогда порядок a делится на p. Так как $\dim(V) = 4$ и $p \geqslant 5$, то E не содержит элемент порядка p^2, и поэтому порядок a равен ps, где s взаимно просто с p. Поэтому существует элемент $b \in \underline{L}$ порядка s, который централизует нетривиальный элемент в V. Пусть $c = b^2$. Тогда $c \in L$.

Положим $c = \bar{d}$ для $d \in SL_2(q^2)$. Пусть $\alpha, 1/\alpha$ — характеристические корни d. По лемме 10 характеристические корни c в V равны $\alpha^{\pm 1 \pm q}$. Поскольку один из этих корней равен единице, порядок d делит $q+1$ или $q-1$, и поэтому порядок a делит $p(q+1)$ или $p(q-1)$.

Пусть пересечение $\langle a \rangle \cap V$ тривиально. Тогда порядок a равен порядку некоторого элемента в $\underline{L}$, и можно считать, что $a \in \underline{L}$. Если $a \in L$, то порядок a делит $p, (q^2-1)/2$ или $(q^2+1)/2$, и поэтому он содержится в $\omega(S_4(q))$. Пусть $a \in \underline{L} \setminus L$. Тогда порядок a равен $2s$, где s — порядок элемента $a^2 \in L$. Если s делится на p, то $s = p$ и $2s \in \omega(S_4(q))$. Значит, можно считать, что s взаимно просто с p. Пусть $a = \bar{c}$, где $c \in SL_2(q)\sigma$. Положим $c = d\sigma$, где $d \in SL_2(q^2)$. Тогда $(c^2)^d = (c^2)^\sigma$, и поэтому характеристические корни c^2 $(\in SL_2(q^2))$ и $(c^2)^\sigma$ совпадают. Пусть $\alpha, 1/\alpha$ — характеристические корни $d = c^2$. Тогда характеристические корни d^σ равны $\alpha^q, 1/\alpha^q$, следовательно, $\alpha^{q-1} = 1$ или $\alpha^{q+1} = 1$. Значит, порядок a делит $(q^2-1)/2 \in \omega(S_4(q))$.

ЗАМЕЧАНИЕ. Этот результат, в частности, исправляет ошибку в [7], где в предложении 7 неверно утверждается, что группа $S_4(7)$ распознаваема. Автор благодарен А. В. Заварницину, указавшему на неполноту доказательства предложения 7 в [7].

§ 5. Группы $S_4(3^n)$

В этом параграфе докажем основную теорему для $S_4(3^n)$. Пусть $q = 3^n$ и $S = S_4(q)$. Поскольку уже известно [7], что $h(S) = \infty$ при $n = 1$, далее считаем, что $n > 1$.

ЛЕММА 12. *Справедливо равенство* $\mu(S) = \{n_2\ (= (q^2+1)/2), (q^2-1)/2, 3(q+1), 3(q-1), 9\}$. *В частности,* $s(S) = 2$.

ДОКАЗАТЕЛЬСТВО см. в [11].

Пусть G — конечная группа с $\omega(G) = \omega(S)$.

ЛЕММА 13. *Имеет место случай* 3 *леммы* 1.

ДОКАЗАТЕЛЬСТВО. По лемме 12, G удовлетворяет условиям леммы 1. Предположим вначале, что имеет место случай леммы 1, т. е.

$G = HC$ — группа Фробениуса с ядром H и дополнением C. По леммам 5 и 12, $\mu(H) = \{n_2\ (= (q^2+1)/2)\}$, $\mu(C) = \{(q^2-1)/2, 3(q+1), 3(q-1), 9\}$, и центр группы C содержит элемент порядка 2. Тогда C содержит элемент порядка 18, что неверно.

Предположим, имеет место случай 2 леммы 1. По леммам 7 и 12 B — циклическая группа порядка $(q^2+1)/2$, тогда $|C|$ делит $|B|-1 = (q^2-1)/2$. Таким образом, A содержит силовскую 3-подгруппу группы G. Поскольку $9 \in \mu(G)$, A будет силовской 3-подгруппой из G, и поэтому C — циклическая группа порядка $(q^2-1)/2$. По лемме 7, G содержит элемент порядка $3(q^2-1)/2$, что противоречит лемме 12. Лемма доказана.

Леммы 13, 2 и 12 показывают, что в табл. 1a—1c существует такая неабелева простая группа P, что $P \le \overline{G} = G/K \le \mathrm{Aut}(P)$ для некоторой нильпотентной нормальной $\pi_1(S)$-подгруппы K из G и $\overline{G}/P$ является $\pi_1(S)$-группой. Кроме того, существует j, $2 \leqslant j \leqslant s(P)$, что $n_j(P) = (q^2+1)/2$ и $\omega(P) \subseteq \omega(S)$.

ЛЕММА 14. *Группа P изоморфна S или $L_2(q^2)$.*

ДОКАЗАТЕЛЬСТВО. По лемме 12, имеет место утверждение

(14.1) *Число $m = (q^2+1)/2 = n_j(P)$ — наибольший порядок элементов в P. Если t — наименьшее общее кратное порядков элементов в P, не делящих m, то $t = 9(m-1)$, в частности, $t/m < 9$. Если $q \geqslant 27$ и u — порядок элемента из P, не делящий m, то либо $u = m-1, (m-1)/2$, либо $m/u > 4$.*

Рассмотрим по-отдельности каждую группу из табл. 1a—1c.

Предположим, $P = A_r$, r равно p, $p+1$ или $p+2$. Тогда $m = p$ или $m = p+2$, и поскольку $q \geqslant 9$, то $p \geqslant 39$. Следовательно, $3(p-3)/2 > m$. С другой стороны, A_r содержит элемент порядка $3(p-3)/2$, который является произведением независимых циклов длин 3, $(p-3)/2$, $(p-3)/2$. Это противоречит утверждению (14.1).

Предположим, $P = A_{p-1}(r)$, где пара (p,r) отлична от $(3,2)$ и $(3,4)$. Тогда $m = (r^p-1)/(r-1)(p,r-1)$. Это равенство невозможно для $q = 9$, поэтому $q > 9$. Поскольку группа $A_{p-1}(r)$ изоморфна фактор-группе по центру группы $SL_p(r)$ и $SL_p(r)$ содержит циклическую группу порядка

$r^{p-1}-1, A_{p-1}(r)$ содержит элемент порядка $u=(r^{p-1}-1)/(p, r-1)$, не делящего m. Поскольку $m-u \neq 1$ и в силу (14.1), имеем $m/u>2$. Это неравенство верно только при $r=2$, тогда равенство $(q^2+1)/2=2^p-1$ невозможно. Итак, этот случай невозможен. Аналогично отвергается случай: $P={}^2A_p(r)$, $r+1$ делит $p+1$.

Предположим, $P=A_p(r)$, $r-1$ делит $p+1$. В этом случае $m= =(r^p-1)/(r-1)$, но $A_p(r)$ содержит элемент порядка $(r^{p+1}-1)/(r-1)^2>m$, что противоречит (14.1). Случай $P={}^2A_{p-1}(r)$ аналогичен.

Понятно, что случай $P={}^2A_3(2)$ невозможен.

Если $P=B_p(3)$, то $(q^2+1)/2=(3^p-1)/2$, что невозможно.

Предположим, $P=C_d(r)$, $d=2^s\geqslant 2$. Тогда $\pi_1(P)= =\pi\left(r\prod\limits_{i=1}^{d-1}(r^{2i}-1)\right)$, $m=(r^d+1)/(2, r-1)$. Пусть вначале r нечетно. Тогда $r^{2^s}=q^2$, в частности, r — степень числа 3. Значит, порядок любого элемента из P, если он взаимно прост с rm, должен делить $m-1=(r^d-1)/2$. Если $d=2$, то $P\simeq S$. Пусть $d\geqslant 4$, h — примитивный простой делитель числа $r^{d-1}-1$, существующий по лемме 3. Поскольку $(r^{d-1}-1, r^d-1)=(r-1)$ и $(r^{d-1}-1, r^d+1)=2$, h не делит $9m(m-1)=tm$. Так как h — порядок некоторого элемента из P, этот случай невозможен. Пусть теперь r четно. Тогда $m=r^d+1, 3^{2n}-1=2r^d$, поэтому $n=1$, $q=3$. Этот случай был заранее исключен. Аналогично рассматривается случай $P=B_d(r)$, $d=2^m\geqslant 4$, r нечетно.

Если $P=C_p(2)$, то $(q^2+1)/2=2^p-1$, значит, $q^2+3=2^{p+1}$, что невозможно. Случаи $P=D_p(2)$ и $P=D_{p+1}(2)$ рассматриваются аналогично.

Если $P=C_p(3)$, то $(q^2+1)/2=(3^p-1)/2$, что снова невозможно. Случаи $P=D_p(3)$ и $P=D_{p+1}(3)$ рассматриваются аналогично.

Если $P=D_p(5)$, то $(q^2+1)/2=(5^p-1)/4$, то $2q^2+3=5^p$, что, очевидно, невозможно.

Предположим, $P={}^2D_d(r)$, $d=2^s\geqslant 4$. Если r нечетно, то $m= =(q^2+1)/2=(r^d+1)/2$ и $q^{m/2}\geqslant q^2$, поэтому из леммы 3 вытекает, что r^6-1 делится на простое число $h\in\omega(P)$, которое не делит $q(q^4-1)(q^2-1)$ и поэтому не делит порядок S. Если r четно, то $(q^2+1)/2=r^d+1$, $q^2-1=2r^d$, что невозможно. Случай $P = {}^2D_d(2)$, $d = 2^s + 1 \geqslant 5$ рассматривается аналогично, а случай $P = {}^2D_p(3)$, $5 \leqslant p \neq 2^s + 1$, очевидно, невозможен.

Предположим, $P = {}^2D_d(3)$, $d = 2^s + 1 \neq p$, $s \geqslant 2$. Тогда $q = 3^{(d-1)/2}$, $(3^d + 1, q^2 + 1) = 2$, $(3^d + 1, q^2 - 1) = 4$. По лемме 3, $3^d + 1$ делится на нечетное простое число, которое, очевидно, делит $|P|$, но не $|S|$.

Пусть $P = G_2(r)$, $2 < r \equiv \varepsilon \pmod 3$, $\varepsilon = \pm 1$. Тогда $m = r^2 - \varepsilon r + 1$, поэтому $q^2 = 2r^2 - 2\varepsilon r + 1 \equiv 1 \pmod 3$, что невозможно.

Если $P = {}^3D_4(r)$ или $F_4(r)$, r нечетно, то $(q^2 + 1)/2 = r^4 - r^2 + 1 \equiv \equiv 1 \pmod 3$, что неверно. Случай $P = {}^2F_4(2)'$ очевидным образом невозможен.

Пусть $P = E_6(r)$. Тогда $(q^2 + 1)/2 = (r^6 + r^3 + 1)/(3, r - 1)$. Если $(3, r - 1) = 3$, то $q^2 - 1 = 2(r^6 + r^3 - 2)/3$ и $(r^3 + 1, q^2 - 1)$ делит 4. Поскольку $r^3 + 1$ делит $|P|$, по лемме 3 существует простое число, делящее $|P|$, но не $|S|$. Следовательно, $(3, r - 1) = 1$ и $q^2 - 1 = 2(r^6 + r^3)$, поэтому $(r^3 - 1, q^2 - 1)$ делит 4, и мы приходим к прежнему заключению. Случай $P = {}^2E_6(r)$ аналогичен. Поскольку $m = (q^2 + 1)/2 \geqslant 41$, все остальные случаи в табл. 1a невозможны.

Пусть $P = A_1(r)$, r нечетно. Если r — простое число, то $(q^2+1)/2 = r$ и $(q^2 - 1)/2 = r - 1$, поэтому $(r + 1)/2 \in \omega(P)$ — нечетное число, взаимно простое с $(q^2 - 1)$. Таким образом, $(r + 1)/2 = 3$ или $(r + 1)/2 = 9$, что легко приводит к противоречию. Поэтому r не является простым числом и, следовательно, $(q^2 + 1)/2 = (r + 1)/2$. В этом случае $P = L_2(q^2)$, как и утверждалось.

Предположим, $P = A_1(2^s)$. Тогда $(q^2 + 1)/2 = 2^s + 1$, что приводит к исключенному случаю $q = 3$.

Случай $P = {}^2A_5(2)$ очевидным образом невозможен, в случаях $P = = {}^2D_p(3), p = 2^s + 1 \geqslant 5$, $P = G_2(r)$, $r = 3^m$ и $P = {}^2G_(r)$, $r = 3^{2s+1}$ мы получаем равенства $q^2 + 1 = (3^p + 1)/2$, $(q^2 + 1)/2 = r^2 + r + 1$ и $(q^2 + 1)/2 = r + \sqrt{3r} + 1$ соответственно, которые невозможны. Пусть $P = = F_4(r)$, $r = 2^s > 2$. Тогда $(q^2 + 1)/2 = r^4 - r^2 + 1$ и $q^2 - 1 = 2(r^4 - r^2)$. Поскольку $(r^4+1, q^2-1) = 1$ и r^4+1 делит $|P|$, по лемме 3 существует простое число, которое делит $|P|$, но не делит $|S|$, а этот случай невозможен.

Предположим, $P = {}^2F_4(r)$, $r = 2^{2s+1} > 2$. Тогда $(q^2+1)/2 = r^2 + \sqrt{2r^3} + r + \sqrt{2r} + 1$, и следовательно, $r \neq 8$, $r \geqslant 32$. Для такого r имеем

$$(r^2 + \sqrt{2r^3} + r + \sqrt{2r} + 1)/(r^2 - \sqrt{2r^3} + r - \sqrt{2r} + 1) < 2,$$

поэтому и по (14.1), выполняется $2(\sqrt{2r^3} + \sqrt{2r}) = 1$, что невозможно.

Все остальные случаи в табл. 1b очевидны.

Пусть P — группа из табл. 1c. Случай $P = {}^2B_2(r)$, $r = 2^{2s+1} > 2$ аналогичен случаю $P = {}^2F_4(r)$, а случай $P = {}^2E_6(2)$ понятным образом невозможен, поэтому пусть $P = E_8(r)$. Поскольку $n_i/n_j < 2$ и $n_i - n_j \neq 1$ для всех $2 \leqslant i, j \leqslant s(P)$, этот случай невозможен по (14.1). Все остальные случаи в табл. 1c легко отвергаются. Лемма доказана.

ПРЕДЛОЖЕНИЕ 2. *Если $q = 3^{2s}$, то существует расширение E 3-группы V посредством $L = L_2(q^2)$, для которого $\omega(E) = \omega(S_4(q))$. В частности, $h(S_4(q)) = \infty$.*

ДОКАЗАТЕЛЬСТВО. Пусть $\widehat{L} = SL_2(q^2)$ и $V = W_1^{2s} \otimes W_1^{2s+1} \otimes W_2^0$ — $\widehat{L}$-модуль, определенный в лемме 10. В силу этой леммы V является L-модулем. Пусть $E = VL$ — естественное полупрямое произведение V на L.

Во-первых, прямыми вычислениями можно проверить, что жорданова форма элемента $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \widehat{L}$ на V содержит клетку размерности 3 и, следовательно, E содержит элемент порядка 9. Поскольку L не содержит элементов порядка $3r$ для $r > 1$, E не может содержать элементов порядка $9r$ при $r > 1$.

Пусть $a \in L$ — элемент порядка m, не делящегося на 3. Можно выбрать прообраз $\widehat{a} \in \widehat{L}$ элемента a так, чтобы порядок $\widehat{a}$ был равен $2m$. Пусть $\alpha, 1/\alpha$ — характеристические корни $\widehat{a}$ в $\widehat{L}$. Тогда мультипликативный порядок α равен $2m$, и $2m$ делит q^2+1 или q^2-1. По лемме 10 характеристические корни a в V имеют вид α^t, где $t = \pm 3^{2s} \pm 3^{2s+1}$ или $t = \pm 2 \pm 3^{2s} \pm 3^{2s+1}$. Следовательно, E содержит элемент порядка $3m$, где m взаимно просто с 3, тогда и только тогда, когда m делит $q+1$ или $q-1$.

Если порядок m элемента E не делится на 3, то m — порядок элемента из L, поэтому m делит $(q^2 \pm 1)/2$. Следовательно, $\mu(E) = \mu(S_4(q))$, и предложение вытекает из [7, лемма 1].

ЛЕММА 15. *Пусть* $L = L_2(3^{4s+2}) \leq H \leq \mathrm{Aut}(L)$ *и* $\omega(H) \subseteq \omega(S_4(3^{2s+1}))$. *Тогда* $H = L$ *или* $H = L\langle\sigma\rangle$, *где* σ — *полевой автоморфизм порядка* 2 *группы* L.

ДОКАЗАТЕЛЬСТВО. Пусть $q = 3^{2s+1}$. Хорошо известно (см., напр., [12]), что $A = \mathrm{Aut}(L) = PGL_2(q^2)\langle\phi\rangle$, где ϕ — полевой автоморфизм порядка $4s+2$. Очевидно, что H/L является $\pi_1(S_4(q))$-группой, и поэтому ни один элемент из $H \setminus L$ не может централизовать нетривиальный элемент из L порядка, делящего $3^{4s+2}+1$. Поскольку ϕ^2 централизует элемент порядка 5 и 5 делит $3^{4s+2}+1$, выполняется $H \leq PGL_2(q^2)\langle\sigma\rangle$. Если $L \neq H \neq L\langle\sigma\rangle$, то силовская 2-подгруппа в H является диэдральной или полудиэдральной группой порядка 2^{t+1}, где 2^t — наибольшая степень числа 2, делящая q^2-1, и поэтому содержит элемент порядка $2^t \notin \omega(S_4(q))$.

Далее будем предполагать, что $q = 3^{2s+1} > 3$.

ЛЕММА 16. *Если* $P = S$, *то* $P \simeq G$.

ДОКАЗАТЕЛЬСТВО. Предположим вначале, что $K \neq 1$. Без потери общности можно считать, что K — элементарная абелева p-группа. Пусть H — полный прообраз P в G. Очевидно, $KC_H(K) = K$, поэтому P действует на K точно. Предположим, что $p \neq 3$. Поскольку P содержит подгруппу L, изоморфную $L_2(q^2)$, которая, в свою очередь, содержит группу Фробениуса F порядка $q^2(q^2-1)/2$, и в силу леммы 6, полный прообраз F в G содержит элемент порядка $p(q^2-1)/2 \notin \omega(S)$. Следовательно, $p = 3$. Поскольку P содержит группу $S_4(3)$, которая содержит S_6 и по лемме 9, имеем $K = 1$.

Итак, P — нормальная подгруппа группы G. По предложению 4.3.10 из [12] P содержит подгруппу $L \simeq L_2(q^2).2$ и $G = PN_G(L)$. Учитывая, что L содержит элемент порядка $(q^2+1)/2$, имеем $C_G(L) = 1$. По лемме 15, $N_G(L) = L$ и $G = P$.

ЛЕММА 17. *Если* $P = L_2(q^2)$, *то* $G/K \simeq P$ *и* K — *нетривиальная* 3-*группа.*

ДОКАЗАТЕЛЬСТВО. По лемме 15, G/K не содержит элементов порядка 9, поэтому 3 делит порядок группы K. По лемме 1, K является $\pi_1(G)$-группой и поэтому циклическая подгруппа из P порядка $(q^2+1)/2$ действует на K регулярно. По лемме 5, K нильпотентна.

Предположим, что существует простое число $r \neq 3$, делящее $|K|$. Пусть K_0 — нормальная подгруппа группы G такая, что $K_0 \leq K$ и $V = K/K_0$ — нетривиальная элементарная абелева r-подгруппа. Тогда P действует на V, и это действие точно. Поскольку P содержит группу Фробениуса порядка $q^2(q^2-1)/2$ с циклическим дополнением порядка $(q^2-1)/2$ и в силу леммы 6, G содержит элемент порядка $r(q^2-1)/2 \neq \omega(S)$. Поэтому K — нетривиальная 3-группа.

Если $G/K \neq P$, то, по лемме 15, $G/K \simeq L\langle\sigma\rangle$, где σ — автоморфизм соответствующего поля F порядка $q^2 = 3^{4s+2}$, отображающий каждый элемент f в f^q. Если F_0 — подполе порядка 9 поля F, то для $f \in F_0$ имеет место равенство $f^q = f^{3^{2s+1}} = f^3$, поэтому σ действует на F_0 нетривиально, и значит, G/K содержит подгруппу $S_6 \simeq L_2(9)\langle\delta\rangle$, где δ — нетривиальный полевой автоморфизм группы $L_2(9)$. По лемме 9, $\omega(G) \neq \omega(S)$. Полученное противоречие доказывает лемму.

ЛЕММА 18. *Группы P и $L_2(q^2)$ не изоморфны.*

ДОКАЗАТЕЛЬСТВО. Предположим противное. По лемме 17, $G/K = P$ и K — нетривиальная 3-группа. Поскольку G, в отличие от P, содержит элемент порядка $3(q+1)$, существует элемент порядка $q+1$ в G, который централизует элемент $k \in K$ порядка 3. Пусть $1 = K_0 < K_1 < \ldots < K_t = K$ — верхний центральный ряд группы K и $k \in K_i \setminus K_{i-1}$. Тогда $V = K_i/K_{i-1}$ является P-модулем, и существует элемент порядка $q+1$ в P, для которого 1 является характеристическим корнем в V. С другой стороны, любая подгруппа порядка $(q^2+1)/2$ из G действует на K регулярно, и, поскольку 5 делит q^2+1, элемент порядка 5 из P не может иметь 1 своим характеристическим корнем в V. Очевидно, некоторая абсолютно неприводимая компонента W модуля V также обладает этими свойствами. Поэтому

(18.1) *W — абсолютно неприводимый P-модуль над полем характеристики 3 такой, что 1 является характеристическим корнем в W для* *некоторого элемента $x \in P$ порядка $q+1$ и не содержится во множестве характеристических корней в W для некоторого элемента $y \in P$ порядка* 5.

По лемме 10, $W = W_{i_1}^{t_1} \otimes \ldots \otimes W_{i_r}^{t_r}$, где $t_1, ..., t_r$ — попарно различные числа, $0 \leqslant t_1, ..., t_r < 4s+2$ и $i_1, ..., i_r \in \{1,2\}$. Для $a \in P = L_2(q^2)$ пусть $\underline{a}$ — прообраз a в $\underline{L} = SL_2(q^2)$ и $\alpha, 1/\alpha$ — характеристические корни $\underline{a}$ в $\underline{L}$.

Если $r \geqslant 4$, то, по лемме 10, существуют числа $b_1, ..., b_r \in \{0,1\}$ такие, что для $c_j = 2^{b_j} \cdot 3^{t_j}$, $j = 1, ..., r$, множество характеристических корней a в W содержит все степени α^d, где $d \in \left\{ \sum\limits_{j=1}^{r} \varepsilon_j c_j \;\middle|\; \varepsilon_j = \pm 1,\ j = 1, ..., r \right\}$. По п. "в" леммы 4, среди таких d найдутся те, которые делятся на 5. Поэтому, если выбрать в качестве a и $\underline{a}$ элементы порядка 5, то $\alpha^d = 1$, что противоречит (18.1). Поэтому $r < 4$.

По лемме 10 существуют в точности два числа, скажем, 1 и 2, что $i_1 = i_2 = 1$. Если $r = 2$, то характеристические корни a в W равны $\{\alpha^d \mid d = \pm 3^{t_1} \pm 3^{t_2}\}$. По п. "а" леммы 4, d может делиться на $q+1$, лишь только $d = \pm 3^t(q+1)$ для некоторого неотрицательного числа t, и поэтому d не может делиться на $2(q+1)$. С другой стороны, $q+1$ делится на 4, поэтому для элемента a порядка $q+1$ из P порядок любого прообраза $\underline{a}$ элемента a в $\underline{L}$ равен $2(q+1)$, и тогда $\alpha^d \neq 1$ для любого d. Это противоречит (18.1).

Поэтому $r = 3$ и $W = W_1^{t_1} \otimes W_1^{t_2} \otimes W_2^{t_3}$. По лемме 10 множество всех характеристических корней a в W равно $\{\alpha^d | d = \varepsilon_1 3^{t_1} + \varepsilon_2 3^{t_2} + \varepsilon_3 2 \cdot 3^{t_3}$, $\varepsilon_1, \varepsilon_2 = \pm 1$, $\varepsilon_3 = -1, 0$ или $1\}$. Учитывая п. "б" леммы 4, получаем противоречие с (18.1) как в двух предыдущих абзацах. Лемма доказана.

Основная теорема вытекает теперь из предложений 1, 2, лемм 14, 16 и 18.

§ 6. Несколько отдельных простых групп

ПРЕДЛОЖЕНИЕ 3. *Существует расширение E 13-группы V посредством $2.S_4$ такое, что $\omega(E) = \omega(L_3(3))$. В частности, $h(L_3(3)) = \infty$.*

ДОКАЗАТЕЛЬСТВО. Пусть H — такое расширение группы порядка 2 посредством S_4, что силовская 2-подгруппа в H — группа кватернионов.

Тогда $\mu(H) = \{6, 8\}$. По лемме 8 существует расширение E элементарной 13-группы посредством H, которое является группой Фробениуса. Тогда $\mu(E) = \{6, 8, 13\} = \mu(L_3(3))$. Теперь предложение следует из [7, лемма 1].

ПРЕДЛОЖЕНИЕ 4. *Если G — конечная группа и $\omega(G) = \omega(U_3(9))$, то $G \simeq U_3(9)$.*

ДОКАЗАТЕЛЬСТВО. Принимая во внимание [14], имеем $\mu(G) = \{30, 73, 80\}$, поэтому граф $GK(G)$ несвязен. Значит, по лемме 1 имеет место один из следующих случаев.

Случай 1. Пусть $G{=}FH$ — группа Фробениуса с ядром F и дополнением H. Связными компонентами в $GK(G)$ являются $\omega(F)$ и $\omega(H)$.

Случай 2. Пусть $G = ABC$, где A, AB — нормальные подгруппы в G, B — нормальная подгруппа в BC, подгруппы B, C циклические и AB, BC — группы Фробениуса. Связными компонентами графа $GK(G)$ являются $\omega(B)$ и $\omega(AC)$.

Случай 3. Существует такая неабелева простая группа P, что $P \leq \overline{G} = G/K \leq \mathrm{Aut}(P)$ для некоторой нильпотентной нормальной $\{2, 3, 5\}$-подгруппы K из G, граф $GK(P)$ несвязен и $\omega_j(P) = \{73\}$ для некоторого j, $2 \leqslant j \leqslant s(P)$.

ЛЕММА 19. *Случай 1 невозможен.*

ДОКАЗАТЕЛЬСТВО. Предположим противное. Поскольку F нильпотентна и является 73-группой, H содержит элемент порядка 16. По п. "б" леммы 5, H содержит нормальное 2-дополнение порядка 15. Тогда H содержит элемент порядка 24, что неверно.

ЛЕММА 20. *Случай 2 невозможен.*

ДОКАЗАТЕЛЬСТВО. Предположим противное. По лемме 6 имеем $|B| = 73$. Поскольку $|C|$ делит $|B| - 1$, первый из них равен 3 или 6. В силу леммы 6, $|C| = 3$, поэтому $A = T \times F$, где F — 5-группа, T — 2-группа периода 16 и $C_T(C)$ — элементарная группа; приходим к противоречию.

Таким образом, имеет место случай 3.

ЛЕММА 21. *Группы G, $U_3(9)$ изоморфны.*

ДОКАЗАТЕЛЬСТВО. По лемме 2, P — одна из групп в табл. 1a—1c. Просмотрев эти таблицы, легко проверить, что $P \simeq U_3(9)$. По [14], $P = G/K$. Можно считать, что K — нетривиальная элементарная абелева p-группа, которую будем рассматривать как P-модуль. В силу [14], P содержит группу Фробениуса порядка $73 \cdot 3$, и применяя лемму 6, имеем $p \neq 3$. Предположим, что $p = 5$. Группа P содержит подгруппу, изоморфную A_6, с циклической силовской 5-подгруппой, и, в силу [15], минимальный полином элемента группы P порядка 5 на K равен $(x-1)^5$. Поэтому G содержит элемент порядка 25, а тогда $p = 2$. По [14] централизатор в P некоторой инволюции $t \in P$ содержит элементарную абелеву подгруппу R порядка 9. Учитывая, что t не централизует K и $K = \langle C_K(r) \mid 1 \neq r \in R\rangle$, t не централизует $C_K(r)$ для некоторого элемента $r \in G$ порядка 3. Отсюда, $C_G(r)$ содержит элемент порядка 4, а G содержит элемент порядка 12, что неверно. Лемма и предложение доказаны.

ПРЕДЛОЖЕНИЕ 5. *Пусть G — конечная группа такая, что $\omega(G) = \omega(^3D_4(2))$. Тогда $G \simeq {}^3D_4(2)$.*

ДОКАЗАТЕЛЬСТВО. Из леммы 2 и [14] вытекает

ЛЕММА 22. *Пусть P — конечная простая группа с несвязным графом Грюнберга—Кегеля $GK(P)$. Если одна из связных компонент графа $GK(P)$ равна $\{13\}$, то P изоморфна одной из групп табл. 2.*

Пусть G — конечная группа, для которой $\omega(G) = \omega(^3D_4(2))$. Тогда

$$\mu(G) = \{13, 7\cdot 3, 7\cdot 4, 9\cdot 2, 3\cdot 4, 8\} \tag{5}$$

и G удовлетворяет условиям 1, 2 или 3 леммы 1. Предположим вначале, что G удовлетворяет условию 1, т.е. $G = FC$ — группа Фробениуса с ядром F и дополнением C. Если F является $\pi_1(G)$-группой, то в силу нильпотентности, она содержит элемент порядка $9\cdot 8$, что неверно, поэтому F — 13-группа. По (5) централизатор в C элемента порядка 7 содержит элемент порядка 6. Следовательно, G содержит элемент порядка $7 \cdot 3 \cdot 2$, что неверно.

Таблица 2

P	$\mu(P)$
A_{13}	$13, 11, 7\cdot5, 7\cdot3, 7\cdot4, 5\cdot3\cdot2, 5\cdot4, 9\cdot2, 3\cdot8$
A_{14}	$13, 11\cdot3, 7\cdot5, 7\cdot3\cdot2, 7\cdot4, 5\cdot9, 5\cdot3\cdot4, 9\cdot2, 3\cdot8$
A_{15}	$13, 11\cdot3, 11\cdot2, 7\cdot5\cdot3, 7\cdot3\cdot2, 7\cdot4, 5\cdot9, 5\cdot3\cdot4, 5\cdot8, 9\cdot4, 3\cdot8$
$L_2(25)$	$13, 5, 3\cdot4$
$L_2(27)$	$13, 7\cdot2, 3$
$L_2(13^n)$	$13, (13^n-1)/2, (13^n+1)/2$
$L_3(3)$	$13, 3\cdot2, 8$
$L_4(3)$	$13, 5\cdot4, 9, 3\cdot4, 8$
$U_3(4)$	$13, 5\cdot3, 5\cdot2, 4$
$S_4(5)$	$13, 5\cdot3\cdot2, 5\cdot4, 3\cdot4$
$S_6(3)$	$13, 7\cdot2, 5\cdot3\cdot2, 5\cdot4, 9\cdot4, 3\cdot8$
$O_7(3)$	$13, 7\cdot2, 5\cdot3, 5\cdot4, 9\cdot2, 3\cdot4, 8$
$O_8^+(3)$	$13, 7\cdot2, 5\cdot3, 5\cdot4, 9\cdot2, 3\cdot4, 8$
$G_2(3)$	$13, 7, 9, 3\cdot4, 8$
$G_2(4)$	$13, 7\cdot3, 5\cdot3, 5\cdot2, 3\cdot4, 8$
$F_4(2)$	$17, 13, 7\cdot3, 7\cdot4, 5\cdot3\cdot2, 5\cdot4, 9\cdot2, 3\cdot8, 16$
$Sz(8)$	$13, 7, 5, 4$
${}^3D_4(2)$	$13, 7\cdot3, 7\cdot4, 9\cdot2, 3\cdot4, 8$
${}^2F_4(2)'$	$13, 5\cdot2, 3\cdot4, 16$
${}^2E_6(2)$	$19, 17, 13, 11\cdot3, 11\cdot2, 7\cdot5, 7\cdot3, 7\cdot4, 5\cdot3\cdot2, 5\cdot4, 9\cdot2, 3\cdot8, 16$
Suz	$13, 11, 7\cdot3, 7\cdot2, 5\cdot3, 5\cdot4, 9\cdot2, 3\cdot8$
Fi_{22}	$13, 11\cdot2, 7\cdot3, 7\cdot2, 5\cdot3\cdot2, 5\cdot4, 9\cdot2, 3\cdot8, 16$

Предположим, G удовлетворяет условию 2. Тогда, по лемме 7, $|B| = 13$ и $|C|$ делит 12. По (5), A содержит элементы порядков 2, 3, 7, и G содержит элемент порядка $7\cdot3\cdot2$, что неверно.

Таким образом, выполняется условие 3, т. е. существует неабелева простая группа P такая, что $P \leq \overline{G} = G/K \leq \mathrm{Aut}(P)$ для некоторой нильпотентной нормальной $\pi_1(G)$-подгруппы K в G и $\overline{G}/P$ является $\pi_1(G)$-группой. По лемме 22, P изоморфна одной из групп $L_2(13)$, $L_2(27)$, $L_3(3)$,

$G_2(3)$, ${}^3D_4(2)$. Рассмотрим каждый случай отдельно.

Пусть $P \simeq L_2(13)$. Поскольку $49 \notin \omega(G)$ и в силу [15], 7 не делит $|K|$. Поэтому K содержит элементы порядков 2 и 3, централизуемые элементом порядка 7 из G. Следовательно, G содержит элемент порядка $7 \cdot 3 \cdot 2$, что противоречит (5).

Предположим, $P \simeq L_2(27)$. Поскольку P содержит группу Фробениуса порядка $27 \cdot 13$, K является 3-группой. Тогда в G не может быть элементов порядка 8, вопреки (5).

Предположим, $P \simeq L_3(3)$. Так как $|\mathrm{Aut}(P)|$ не делится на 7 и P содержит группу Фробениуса порядка $9 \cdot 8$ с циклическим дополнением порядка 8, 7 будет делить $|K|$, а по лемме 6, G содержит элемент порядка $7 \cdot 8$, что неверно.

Пусть $P = G_2(3)$. Так как в G нет элементов порядка 49 и P содержит группу Фробениуса порядка $8 \cdot 7$, то 7 не делит $|K|$, и поэтому K содержит элементы порядков 2 и 3, централизуемые силовской 7-подгруппой из G. Следовательно, G содержит элемент порядка $7 \cdot 3 \cdot 2$, что противоречит (5).

Итак, $P \simeq {}^3D_4(2)$ и $G/K = P$. Предположим, что $K \neq 1$. Можно считать, что K — элементарная абелева p-группа для $p = 2, 3$ или 7. Так как P содержит группу Фробениуса порядка $8 \cdot 7$, то, по лемме 6, $p \neq 7$. Таблицы характеров Брауэра группы P (см. [9]) для $p = 2, 3$ показывают, что в случае, когда элемент порядка 13 из P действует на абсолютно неприводимом модуле V без неподвижных точек, то $p = 2$, $\dim(V) = 8$, и элемент порядка 21 из P обладает в V нетривиальной неподвижной точкой. Значит, G содержит либо элемент порядка $13p$, либо элемент порядка $2 \cdot 21$, что неверно. Следовательно, $K = 1$ и $G = P$. Предложение доказано.

ПРЕДЛОЖЕНИЕ 6. *Если G — конечная группа, для которой $\omega(G) = \omega(G_2(4))$, то $G \simeq G_2(4)$.*

ДОКАЗАТЕЛЬСТВО. По [14] имеем

$$\mu(G) = \{13, 7 \cdot 3, 5 \cdot 3, 5 \cdot 2, 3 \cdot 4, 8\}. \tag{6}$$

Как в доказательстве предложения 5 легко показать, что G удовлетворяет условию 3 леммы 1, т.е. существует неабелева простая группа P такая, что $P \leq \overline{G} = G/K \leq \mathrm{Aut}(P)$ для некоторой нильпотентной нормальной $\pi_1(G)$-подгруппы K в G и $\overline{G}/P$ является $\pi_1(G)$-группой. По лемме 22, P изоморфна одной из групп $L_2(13)$, $L_2(25)$, $L_2(27)$, $L_3(3)$, $Sz(8)$, $U_3(4)$, $G_2(4)$.

Если P изоморфна $L_2(25)$, $L_3(3)$ или $U_3(4)$, то $|G/K|$ не делится на 7, поэтому $|K|$ делится на 7. Поскольку силовская 2-подгруппа группы P содержит абелеву нециклическую подгруппу, G содержит элемент порядка 14, вопреки (6).

Если P изоморфна $L_2(13)$ или $L_2(27)$, то 5 не делит $|\mathrm{Aut}(P)|$, и поэтому 5 делит $|K|$. Поскольку P содержит группу Фробениуса порядка $13 \cdot 6$ или $27 \cdot 13$ и в силу леммы 6, G содержит элемент порядка $5 \cdot 6$ или $5 \cdot 13$, вопреки (6).

Пусть $P \simeq Sz(8)$. Отметим, что $8 \in \mu(G), 8 \notin \omega(\mathrm{Aut}(P))$ и P содержит группу Фробениуса порядка $13 \cdot 4$. Из леммы 6 следует, что K — нетривиальная 2-группа, и поэтому $G/K \simeq Sz(8) : 3$. По [14], G/K содержит группу Фробениуса порядка $13 \cdot 12$, и, по лемме 6, G содержит элемент порядка 24, вопреки (6).

Итак, $P \simeq G_2(4)$. По [14], $G/K = P$. Поскольку P содержит группы Фробениуса порядков $3 \cdot 2$, $4 \cdot 3$, $16 \cdot 5$ и $\omega(G)$ не содержит $7 \cdot 2$, 9, 25, то K является 2-группой.

Покажем, что $K = 1$. Предположим противное. Можно считать, что K — элементарная абелева группа, которая является абсолютно неприводимым P-модулем. По таблице 2-характеров Брауэра группы $G_2(4)$ (см. [9]) и поскольку силовская 7-подгруппа группы P действует на K регулярно, $\dim(K) = 6$, $\dim(C_K(x)) = 2$ и $\dim(C_K(y)) = 0$ для $x \in 5A$, $y \in 5C$. По [14], $C_P(x) = \langle x \rangle \times A$, где $A \simeq A_5$ и силовская 5-подгруппа из A порождена элементом из $5C$. В частности, A действует на $C_K(x)$ точно, а поэтому $C_G(x)$ содержит элемент порядка 4, что противоречит (6). Предложение доказано.

ПРЕДЛОЖЕНИЕ 7. *Если G — конечная группа, для которой $\omega(G) = \omega(S_6(3))$, то $G \simeq S_6(3)$.*

ДОКАЗАТЕЛЬСТВО. По [14],

$$\mu(G) = \{13, 7 \cdot 2, 5 \cdot 3 \cdot 2, 5 \cdot 4, 9 \cdot 4, 3 \cdot 8\}. \tag{7}$$

Как и при доказательстве предложения 5, легко показать, что G удовлетворяет условию 3 леммы 1, т. е. существует неабелева простая группа P такая, что $P \leq \overline{G} = G/K \leq \mathrm{Aut}(P)$ для некоторой нильпотентной нормальной $\pi_1(G)$-подгруппы K в G и $\overline{G}/P$ является $\pi_1(G)$-группой. По лемме 22, P изоморфна одной из групп $L_2(13)$, $L_2(25)$, $L_2(27)$, $U_3(4)$, $S_4(5)$, $O_7(3)$, $O_8^+(3)$, $L_3(3)$, $L_4(3)$, $G_2(3)$, $Sz(8)$, $S_6(3)$.

Если $P \simeq Sz(8)$, то P содержит группу Фробениуса порядка 56, и по лемме 6, K является 2-группой, поэтому G не может содержать элемент порядка 9, вопреки (7).

Предположим, $P \simeq L_3(3)$. Поскольку $L_3(3)$ содержит группу Фробениуса порядка 72 с циклическим дополнением и в силу леммы 6, K является 3-группой, а порядок G не делится на 7, вопреки (7). Такое же рассуждение исключает и случай $P \simeq L_4(3)$.

Предположим, $P \simeq G_2(3)$. Поскольку P содержит подгруппы, изоморфные $L_3(3)$ и $L_2(8)$, получаем, как в предыдущем абзаце, что K — 3-группа, а затем, что G содержит элемент порядка 21. Это невозможно по (7). Поскольку $O_8^+(3) > O_7(3) > G_2(3)$, аналогичные рассуждения показывают, что P не может быть изоморфна $O_7(3)$ или $O_8^+(3)$.

Если P изоморфна $U_3(4)$ или $S_4(5)$, то 7 делит порядок K. Силовская 5- или 3-подгруппа группы P не является циклической, поэтому G содержит элемент порядка 35 или 21, что неверно.

Если $P \simeq L_2(13)$, то $|K|$ делится на 15 и, поскольку P содержит группу Фробениуса порядка $13 \cdot 6$, G содержит элемент порядка $15 \cdot 6$, что неверно.

Если $P \simeq L_2(25)$, то $|K|$ делится на 7 и, поскольку P содержит группу Фробениуса порядка $25 \cdot 12$, G содержит элемент порядка $7 \cdot 12$, что неверно.

Аналогично, если $P \simeq L_2(27)$, то $|K|$ делится на 5 и G содержит элемент порядка $13 \cdot 5$.

Итак, $P \simeq S_6(3)$. По [14], $G/K = P$. Покажем, что $K = 1$. Поскольку P содержит группу Фробениуса порядка $27 \cdot 13$ и в силу леммы 6, K является 3-группой. Предположим, $K \neq 1$. Поскольку P содержит подгруппу, изоморфную $L = L_2(13)$, таблица 3-характеров Брауэра группы L (см. [9]) показывает, что G содержит элемент порядка 21, а это неверно. Предложение доказано.

ПРЕДЛОЖЕНИЕ 8. *Пусть $L = F_4(2)$ или $L = {}^2E_6(2)$. Если G — конечная группа, для которой $\omega(G) = \omega(L)$, то $G \simeq L$.*

ДОКАЗАТЕЛЬСТВО. По [14],

$$\mu(F_4(2)) = \{17, 13, 7\cdot 3, 7\cdot 4, 5\cdot 3\cdot 2, 5\cdot 4, 9\cdot 2, 3\cdot 8, 16\}, \tag{8}$$

$$\begin{aligned}\mu({}^2E_6(2)) \;=\; &\{19, 17, 13, 11\cdot 3, 11\cdot 2, 7\cdot 5, 7\cdot 3,\\ &7\cdot 4, 5\cdot 3\cdot 2, 5\cdot 4, 9\cdot 2, 3\cdot 8, 16\},\end{aligned} \tag{9}$$

поэтому число компонент связности графа $GK(G)$ не меньше трех, а по леммам 1, 22 для некоторой нильпотентной нормальной $\pi_1(G)$-подгруппы K из G справедливо $P \leq \overline{G} = G/K \leq \mathrm{Aut}(P)$, где P изоморфна $F_4(2)$ или ${}^2E_6(2)$. Поскольку ${}^2E_6(2) > F_4(2) > {}^3D_4(2)$, можно показать так же, как в последнем абзаце доказательства предложения 5, что $K = 1$. По [14], $P = G$.

СЛЕДСТВИЕ 1. *Пусть P — конечная простая группа с несвязным графом Грюнберга—Кегеля $GK(P)$. Если одна из компонент связности графа $GK(P)$ равна $\{13\}$, то либо P изоморфна одной из групп $S_4(5), L_3(3)$ и $h(P) = \infty$, либо P изоморфна одной из групп $O_7(3), O_8^+(3)$ и $h(P) = 2$, либо P распознаваема по ее множеству порядков элементов.*

ДОКАЗАТЕЛЬСТВО. По лемме 22, P изоморфна одной из групп A_{13}, A_{14}, A_{15}, $L_2(13^n)$, $L_2(25)$, $L_2(27)$, $L_3(3)$, $L_4(3)$, $U_3(4)$, $S_4(5)$, $S_6(3)$, $O_7(3)$, $O_8^+(3)$, $G_2(3)$, $G_2(4)$, $F_4(2)$, $Sz(8)$, ${}^3D_4(2)$, ${}^2F_4(2)'$, ${}^2E_6(2)$, Suz, Fi_{22}. Для групп $L_3(3), S_4(5), {}^3D_4(2), S_6(3), G_2(4), F_4(2), {}^2E_6(2)$ заключение выполняется по предложениям 1, 3, 5—8. Для остальных групп заключение известно из литературы (см. приложение).

Таблица 3

G	Условия на G	$h(G)$	Ссылки
A_n	$n = 5, 16, p, p+1, p+2$, $p \geqslant 7$ простое	1	[1].21—[1].27, [17]
A_6		∞	[1].23
A_{10}		∞	[7]
$L_2(q)$	$q > 3, q \neq 9$	1	[1].1—[1].5
$L_3(q)$	$q = 7, 2^m$	1	[1], [1].9—[1].11, [1].42
$L_3(3)$		∞	[0]
$L_3(5)$		2	[7].23
$L_3(9)$		2	[7].24
$L_4(3)$		1	[1].11
$L_5(3)$		1	[17]
$U_3(2^m)$	$m \geqslant 2$	1	[1], [1].42
$U_n(q)$	$(n,q) \in \{(3,9),(3,11),(4,3),(6,2)\}$	1	[0], [1].12—[1].14
	$(n,q) \in \{(3,3),(3,5),(3,7),(4,2),(5,2)\}$	∞	[7]
$S_4(q)$	$q = 3^{2m+1} > 3$	1	[0]
	$q = 3, 3^{2m}, p^m, p \neq 3$ простое	∞	[0], [7], [1], [1].42
$S_6(2)$		2	[7].14, [7].22

$S_6(3)$		1	[0]
$O_8^+(2)$		2	[7].14, [7].22
$O_7(3)$		2	[7].14
$O_8^+(3)$		2	[7].14
$Sz(2^{2m+1})$		1	[1].6
$^3D_4(2)$		1	[0]
$G_2(3^m)$		1	[1].11, [16]
$G_2(4)$		1	[0]
$^2G_2(3^{2m+1})$		1	[1].7
$F_4(2)$		1	[0]
$^2F_4(2^{2m+1})$	$m > 1$	1	[1].8
$^2F_4(2)'$		1	[1].11
$^2E_6(2)$		1	[0]
Спорадическая группа	$G \neq J_2$	1	[1].4, [1].14, [1].16—[1].20
J_2		∞	[1].23

§ 7. Приложение

В табл. 3 перечислены конечные простые группы, для которых в настоящее время известно, являются ли они распознаваемыми или нераспознаваемыми по множеству порядков их элементов. В столбце "Ссылки", [i].j означает ссылку [j] в [i]. Ссылка [0] указывает на настоящую работу.

Автор благодарен А. В. Заварницину, прочитавшему рукопись и сделавшему ряд важных замечаний.

ЛИТЕРАТУРА

1. *В. Д. Мазуров, М. Ч. Су, Х. П. Чао*, Распознавание конечных простых групп $L_3(2^m)$ и $U_3(2^m)$ по порядкам их элементов, Алгебра и логика, **39**, N 5 (2000), 567—585.
2. *J. S. Williams*, Prime graph components of finite groups, J. Algebra, **69**, N 2 (1981), 487—513.
3. *А. С. Кондратьев, В. Д. Мазуров*, Распознавание знакопеременных групп простой степени по порядкам их элементов, Сиб. матем. ж., **41**, N 2 (2000), 360—371.
4. *J. G. Thompson*, Normal p-complements for finite groups, Math. Z., **72**, N 2 (1960), 332—354.
5. *H. Zassenhaus*, Kennzeichnung endlicher linearen Gruppen als Permutationsgruppen, Abh. Math. Semin. Univ. Hamb., **11** (1936), 17—40.
6. *H. Zassenhaus*, Über endliche Fastkörper, Abh. Math. Semin. Univ. Hamb., **11** (1936), 187—220.
7. *В. Д. Мазуров*, Характеризации конечных групп множествами порядков их элементов, Алгебра и логика, **36**, N 1 (1997), 37—53.
8. *K. Zsigmondy*, Zur Theorie der Potenzreste, Monatsh. Math. Phys., **3** (1892), 265—284.
9. *C. Jansen, K. Lux, R. Parker, R. Wilson*, An Atlas of Brauer characters, Oxford, Clarendon Press, 1995.
10. *R.Brauer, C. Nesbitt*, On the modular representations of groups of finite order. I (Univ. Toronto Stud., Math. Ser. **4**), Toronto, Univ. Toronto Press, 1937.

11. *B. Srinivasan*, The characters of the finite symplectic group $Sp(4,q)$. Trans. Am. Math. Soc., **131**, N 2 (1968), 488–525.
12. *P. Kleidman, M. Liebeck*, The subgroup structure of the finite classical groups (London Math. Soc. Lect. Note Series, **129**), Cambridge, Cambridge University Press, 1990.
13. *E. I. Khukhro*, Nilpotent groups and their automorphisms (de Gruyter Expo. Math., **8**), Berlin, Walter de Gruyter, 1993.
14. *J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson*, Atlas of finite groups, Oxford, Clarendon Press, 1985.
15. *A. E. Zalesskii*, Minimal polynomials and eigenvalues of p-elements in representations of quasi-simple groups with a cyclic Sylow p-subgroup, J. Lond. Math. Soc., II. Ser., **59**, N 3 (1999), 845–866.
16. *А. В. Васильев*, Распознаваемость групп $G_2(3^n)$ по порядкам их элементов, Алгебра и логика, 42, N 2 (2002), 130–142.
17. *M. R. Darafsheh, A. R. Moghaddamfar*, A characterization of some finite groups by their element orders, Algebra Colloq., **7**, N 4 (2000), 467–476.

Адрес автора:

МАЗУРОВ Виктор Данилович,
РОССИЯ,
630090, г. Новосибирск,
пр. Ак. Коптюга, 4,
Институт математики СО РАН.
e-mail: mazurov@math.nsc.ru

Поступило 29 ноября 2000 г.