В. Д. Мазуров, М. Ч. Су, Ч. П. Чао, Распознавание конечных простых групп $L_3(2^m)$ и $U_3(2^m)$ по порядкам их элементов, *Алгебра и логика*, 2000, том 39, номер 5, 567–585

https://www.mathnet.ru/al292

Алгебра и логика, 39, N 5 (2000), 567–585

УДК 512.542

РАСПОЗНАВАНИЕ КОНЕЧНЫХ ПРОСТЫХ ГРУПП $L_3(2^m)$ И $U_3(2^m)$ ПО ПОРЯДКАМ ИХ ЭЛЕМЕНТОВ*)

В. Д. МАЗУРОВ, М. Ч. СУ, Ч. П. ЧАО

Введение

Для конечной группы G обозначим через $\omega(G)$ множество порядков ее элементов. Это множество замкнуто относительно делимости и поэтому однозначно определяется подмножеством $\mu(G)$, состоящим из максимальных по делимости элементов множества $\omega(G)$.

Будем говорить, что конечная группа G *распознаваема по* $\omega(G)$ (короче, *распознаваема*), если каждая конечная группа H со свойством $\omega(H) = \omega(G)$ изоморфна G.

К настоящему времени доказано, что распознаваемы следующие конечные простые группы: $L_2(q)$, $q > 3$, $q \neq 9$ [1–5], группы Сузуки $Sz(q) = {}^2B_2(q)$ [6], группы Ри $Re(q) = {}^2G_2(q)$ [7] и ${}^2F_4(q)$ [8], $L_3(4)$ [9], $L_3(8)$ [10], $L_3(7), L_4(3), G_2(3)$, ${}^2F_4(2)'$ [11], $U_3(11)$ [12], $U_4(3)$ [13], $U_6(2)$ [14], $O_8^-(2)$, $O_{10}^-(2)$ [15], спорадические группы, отличные от J_2 [4, 14, 16–20], а также знакопеременные группы A_n для $n = 5, 16, p, p+1, p+2$, где $p \geqslant 7$ — простое число, [21–27].

Цель настоящей работы — доказать, что все неабелевы простые группы $L_3(2^m)$ и $U_3(2^m)$ распознаваемы, а любая простая группа $S_4(2^m)$ нерас-

*)Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований, проект N 99-01-00550, Национального фонда естественных наук Китая, грант N 19871066, и Министерства государственного образования Китая, грант N 98083.

познаваема. В качестве следствия получаем список всех распознаваемых конечных простых групп G, для которых $4t \notin \omega(G)$ при $t > 1$.

Множество $\omega(H)$ конечной группы H определяет *граф Грюнберга—Кегеля* $GK(H)$: его вершинами являются простые делители порядка группы H, два простых числа p, q полагаем смежными, если H содержит элемент порядка pq. Число компонент связности графа $GK(H)$ обозначим через $s(H)$, а i-тую компоненту связности — через $\pi_i = \pi_i(H)$, $i = 1, \dots, s(H)$. Для группы H четного порядка пусть $2 \in \pi_1$. Обозначим через $\mu_i = \mu_i(H)$ (соответственно, через $\omega_i = \omega_i(H)$) множество, состоящее из чисел $n \in \mu(H)$ (соответственно, $n \in \omega(H)$) таких, что каждый простой делитель числа n принадлежит π_i.

Предварительные результаты

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

а) *$s(G) = 2$, $G = FC$ — группа Фробениуса с ядром F и дополнением C, и $\pi(F)$, $\pi(C)$ — связные компоненты графа $GK(G)$;*

б) *$s(G) = 2$, $G = ABC$, где A, AB — нормальные подгруппы группы G, B — нормальная подгруппа в группе BC, а AB, BC — группы Фробениуса; более того, $\pi(AC)$, $\pi(B)$ — связные компоненты графа $GK(G)$;*

в) *$G = P$ — неабелева простая группа;*

г) *G — расширение $\pi_1(G)$-группы посредством простой группы P;*

д) *G — расширение группы из п.* в *или п.* г *посредством $\pi_1(G)$-группы.*

В п. г *и п.* д *граф $GK(P)$ несвязен, $s(P) \geqslant s(G)$, и существуют такие $i, j \geqslant 2$, что $\pi_i(G) = \pi_j(P)$.*

ДОКАЗАТЕЛЬСТВО см. в [28].

ЛЕММА 2. 1. *Пусть G — группа Фробениуса с ядром F и дополнением C. Тогда*

а) *подгруппа F нильпотентна;*

б) *любая подгруппа группы C порядка pq, где p и q (не обязательно различные) — простые числа, является циклической. В частности, любая силовская подгруппа нечетного порядка группы C циклична, а силовская 2-подгруппа группы C будет циклической или (обобщенной) группой кватернионов. Если $O(C) = 1$, то либо C является 2-группой, либо C содержит подгруппу индекса $\leqslant 2$, изоморфную $SL_2(3)$ или $SL_2(5)$.*

2. *Пусть G — конечная группа, $N \lhd G$, G/N — группа Фробениуса с ядром Фробениуса 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 порядка N. Если, дополнительно, полный прообраз F в G — группа Фробениуса с ядром N, то*

$$|C| \cdot \prod_{p\in\pi(N)} p \in \omega(G).$$

ДОКАЗАТЕЛЬСТВО. Утверждение п. 1а — это теорема Томпсона [29], доказательство п. 1б см. в [30, 31], п. 2 — это лемма 1 в [24].

ЛЕММА 3. *В п. б леммы 1 подгруппа B является циклической группой нечетного порядка, C — циклической группой, и G содержит элемент порядка $|C| \cdot \prod_{p\in\pi(A)} p$.*

ДОКАЗАТЕЛЬСТВО. По лемме 2 подгруппа B нильпотентна с циклическими или кватернионными силовскими подгруппами. Если $|B|$ — четное число, то BC не может быть группой Фробениуса. Поэтому B — циклическая группа нечетного порядка, и C — абелева группа как группа автоморфизмов циклической группы B. Поскольку C не содержит элементарных абелевых p-подгрупп порядка p^2, группа C является циклической. Последнее утверждение леммы является частным случаем леммы 2.2.

ЛЕММА 4. *Пусть p — простое число, а s — натуральное число, $s \geqslant 2$. Тогда верно одно из следующих утверждений:*

а) *существует простое число q, которое делит $p^s - 1$, но не делит $p^t - 1$ для всех натуральных $t < s$;*

б) $s = 6$ *и* $p = 2$;

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

ДОКАЗАТЕЛЬСТВО см. в [32].

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

ЛЕММА 5. *Пусть* $P = L_3(2^m)$. *Тогда*

а) $\omega(P)$ *состоит из всех делителей чисел* 4, $2(2^m-1)/(3,2^m-1)$, 2^m-1, $(2^{2m}-1)/(3,2^m-1)$, $(2^{2m}+2^m+1)/(3,2^m-1)$;

б) *если* $P \le G \le \mathrm{Aut}(P)$ *и* $\omega(G) = \omega(P)$, *то* $G = P$.

ДОКАЗАТЕЛЬСТВО. Пусть F — поле порядка $q = 2^m$, и α — фиксированный порождающий элемент его мультипликативной группы. Положим $L = SL_3(F)$. Тогда порядок подгруппы

$$Z(L) = \left\{ \begin{bmatrix} \varepsilon & & \\ & \varepsilon & \\ & & \varepsilon \end{bmatrix} \middle| \ \varepsilon \in F, \varepsilon^3 = 1 \right\}$$

равен $(3, q-1)$. Отождествим P с группой $L/Z(L)$ внутренних автоморфизмов группы L. Пусть d — автоморфизм группы L, индуцированный сопряжением матрицей $\begin{bmatrix} 1 & & \\ & \alpha & \\ & & 1 \end{bmatrix}$, пусть f — полевой автоморфизм группы L, переводящий каждую матрицу $a = (a_{ij}) \in L$ в матрицу (a_{ij}^2), и пусть g — графовый автоморфизм, переводящий каждую матрицу a в транспонированную обратную матрицу ${}^t a^{-1}$. Легко вычислить, что

(5.1) *инволюция* $t = \begin{bmatrix} & & 1 \\ & 1 & \\ 1 & & \end{bmatrix}$ *является неподвижной точкой для* $\langle d, f, g \rangle$. *Единственная силовская 2-подгруппа* T *в* $C_L(t)$ *состоит из матриц вида* $(\beta, \gamma, \delta) = \begin{bmatrix} \delta+1 & \beta & \delta \\ \gamma & 1 & \gamma \\ \delta & \beta & \delta+1 \end{bmatrix}$, β, γ, $\delta \in F$, *и является инвариантной относительно* $A = \langle d, f, g \rangle$. *Для всех* β_i, γ_i, δ_i, $i = 1, 2$, *справедливо* $(\beta_1, \gamma_1, \delta_1)(\beta_2, \gamma_2, \delta_2) = (\beta_1+\beta_2, \gamma_1+\gamma_2, \delta_1+\delta_2+\beta_1\gamma_2)$. *Кроме того,* T *— силовская 2-подгруппа в* L, *и все инволюции из* $Z(T)$ *сопряжены в* $N_L(T)$.

Далее, можно проверить прямыми вычислениями, что в обозначениях (5.1) верно следующее:

(5.2) *пусть* $B = \{(\beta, 0, \delta) \mid \beta, \delta \in F\}$, $C = \{(0, \gamma, \delta) \mid \gamma, \delta \in F\}$. *Тогда* B *и* C *— элементарные абелевы группы и* $T = BC$. *Порядок любого элемента из* $T \setminus (B \cup C)$ *равен* 4. *Подгруппы* B *и* C *инвариантны относительно подгруппы* $\langle d, f\rangle$ *и* $B^g = C$.

По [33] можно отождествить $\mathrm{Aut}(L) = PA$, где $A = \langle d, f, g\rangle$ с $\mathrm{Aut}(P)$. Поскольку $T \cap Z(L) = 1$, можно отождествить подгруппу T с ее образом в P. Тогда

(5.3) $C_{\mathrm{Aut}(P)}(t) = TA$ *и* A *действует на* T *точно.*

Очевидно, что

(5.4) *порядок автоморфизма* d *равен* $q-1$, *порядок* f *равен* m, *порядок* g *равен* 2 *и* $d^f = f^{-1}df = d^2$, $d^g = d^{-1}$, $fg = gf$.

Поскольку $d^{(3,q-1)}$ — внутренний автоморфизм группы P, то

(5.5) *любой элемент из* $\mathrm{Aut}(P)$ *единственным образом представим в виде* $pd^xf^yg^z$, *где* $0 \leqslant x \leqslant (3, q-1) - 1$, $0 \leqslant y \leqslant m-1$, $0 \leqslant z \leqslant 1$, $p \in P$.

Любая инволюция из P сопряжена с t, поэтому любой элемент v четного порядка из P сопряжен с элементом из $C_P(t)$. По 5.3, $C_P(t) = P\langle d\rangle$ и порядок элемента v либо равен 4, либо является делителем числа $2(q-1)/(3, q-1)$.

Пусть h — элемент из P нечетного порядка $s \in \mu(P)$, и $\hat{h}$ — его прообраз в L наибольшего порядка. Если $\hat{h}$ неприводим над F, то порядок элемента $\hat{h}$ равен q^2+q+1, а порядок элемента h равен $(q^2+q+1)/(3, q-1)$. Если $\hat{h}$ приводим, то $\hat{h}$ содержится либо в подгруппе группы L, изоморфной $(q-1) \times (q-1)$, либо в циклической подгруппе порядка q^2-1. Следовательно, порядок элемента h равен $q-1$ или $(q^2-1)/(q-1, 3)$. Таким образом, п. а доказан.

Пусть $P < G \leq \mathrm{Aut}(P)$. Поскольку $\mathrm{Aut}(P) = PA$, то $G = P(G \cap A)$. Если $G \cap A$ содержит элемент h простого порядка p, сопряженный с нетривиальным элементом из $\langle f\rangle$, то в случае $p = 2$, h централизует в P нетривиальный элемент порядка $(2^{2m} + 2^m + 1)/(3, 2^m - 1)$, взаимно простого с $2^m - 1$, а в случае $p \neq 2$, h централизует в P элемент порядка 4.

Это противоречит п. а.

Если $G \cap \langle d, f\rangle$ содержит элемент, не принадлежащий P и не сопряженный элементу из $\langle f\rangle$, то по 5.5, $2^m - 1$ делится на 3, и по 5.1 и 5.4, в $T(A \cap G)$ имеется элемент порядка $2(2^m - 1) \notin \omega(G)$.

Теперь, по 5.4, $|G : P| = 2$, и по 5.5, $A \cap G$ содержит 2-элемент $h = pd^x f^y g$. По 5.1 элемент $l = h^2$ содержится в T. Если порядок элемента l равен 4, то порядок элемента h равен 8, что противоречит п. а. По 5.2, $l \in B \cap C = Z(T)$, и для элемента $u = (1,0,0) \in T$ справедливо $(uh)^2 = uu^h l \notin B \cup C$. Снова по 5.2 порядок элемента uh равен $8 \notin \omega(P)$. Лемма доказана.

Аналогичные утверждения верны для унитарных групп.

ЛЕММА 6. *Пусть* $P_0 = U_3(2^s)$, $s > 1$. *Тогда*

а) $\omega(P_0)$ *состоит из всех делителей чисел* 4, $2(2^s+1)/(3, 2^s+1)$, 2^s+1, $(2^{2s}-1)/(3, 2^s+1)$, $(2^{2s}-2^s+1)/(3, 2^s+1)$;

б) *если* $P_0 \leq G_0 \leq \mathrm{Aut}(P_0)$ *и* $\omega(G_0) = \omega(P_0)$, *то* $G_0 = P_0$.

ДОКАЗАТЕЛЬСТВО. Полагаем $m = 2s$, сохраняем обозначения леммы 5 и ее доказательства. Пусть F_0 — подполе порядка 2^s в F. Группа P_0 совпадает с множеством всех неподвижных точек автоморфизма fg в P. Отсюда по 5.1

(6.1) *инволюция* t *центральна в силовской* 2*-подгруппе*

$$T_0 = C_T(fg) = \{(\beta, \beta^{2^s}, \delta) \mid \beta, \delta \in F,\ \beta + \beta^{2^s} = \delta + \delta^{2^s}\}$$

группы P_0, *и* $Z(T_0) = \Phi(T_0) = \{(0,0,\delta) \mid \delta \in F_0\}$. *Порядок любого элемента из* $T_0 \setminus Z(T_0)$ *равен* 4. *Подгруппа* T_0 *инвариантна относительно* $A_0 = \langle f, d^{2^s-1}\rangle$, *и* A_0 *действует на* $T_0/Z(T_0)$ *точно. Все инволюции из* T_0 *сопряжены в* $N_{P_0}(T_0)$.

По [33] имеем

(6.2) $\mathrm{Aut}(P_0) = P_0 A_0$.

Из 5.3 следует, что $C_{\mathrm{Aut}(P_0)}(t) = T_0 A_0$. Теперь элементы множества $\omega(P_0)$ могут быть найдены так же, как в доказательстве леммы.

Докажем п. б. По 6.2, $G_0 = P_0 D$, где $D = G_0 \cap A_0$. Если порядок подгруппы D четен и a — инволюция в D, то по 6.1, $b^a Z(T_0) \neq b^a Z(T_0)$

для некоторого элемента $b \in T_0$ и $(ab)^2 = b^a b \notin Z(T_0)$. Значит, порядок элемента ab равен 8, что противоречит п. а.

Следовательно, порядок подгруппы D нечетен. В частности, по 6.1, $D \leq \langle d_0, f^2 \rangle$, где $d_0 = d^{2^s-1}$. Если $1 \neq f_0 \in D \cap \langle f^2 \rangle$, то f_0 централизует подгруппу группы P_0, изоморфную $U_3(2)$ или $U_3(4)$, и G_0 содержит элемент порядка $4k > 4$, что противоречит п. а. Кроме того,

(6.3) $D \cap \langle f^2, d_0^3 \rangle = \langle d_0^3 \rangle \leq P_0$,

поскольку в противном случае D содержит нетривиальный элемент из $\langle f^2 \rangle$.

Теперь предположим, что $G_0 \neq P_0$. По 6.3, $|G_0 : P_0| = 3$ и $(3, 2^s+1) = 3$. Пусть x — 3-элемент в $D \setminus P_0$. По 5.3, $x \in \langle y, z \rangle$, где y порождает силовскую 3-подгруппу из $\langle d_0 \rangle$ и z — элемент порядка 3 в $\langle f \rangle$, который нормализует $\langle y \rangle$. Пусть $x = y_0 z_0$, где $y_0 \in \langle y \rangle, z_0 \in \langle z \rangle$. Если $y_0 \in \langle y^3 \rangle$, то D содержит нетривиальный элемент из $\langle f^2 \rangle$ вопреки 6.3. Поэтому y_0 порождает y. По [34, теор. 12.5.1] порядок элемента x равен порядку элемента y и не может делить $(2^s + 1)/(3, 2^s + 1)$. Поскольку, по 5.1, t и x перестановочны, то порядок элемента tx не делит $2(2^s + 1)/(3, 2^s + 1)$, что противоречит п. а. Лемма доказана.

ЛЕММА 7. *Пусть $P = S_4(q), q = 2^m$. Тогда $\mu(P) = \{4, 2(q-1), 2(q+1), q^2-1, q^2+1\}$.*

ДОКАЗАТЕЛЬСТВО. По [35] централизатор любой инволюции из P является расширением элементарной абелевой 2-группы посредством $L_2(q)$. Это дает множество четных порядков элементов. В силу [36] любой элемент нечетного порядка содержится в максимальном торе группы P, порядок которого равен $q^2 - 1$ или $q^2 + 1$. Абелева подгруппа порядка $q^2 + 1$ действует неприводимо на естественном модуле группы P размерности 4 и поэтому является циклической группой. С другой стороны, P содержит в качестве подгруппы $L_2(q) \times L_2(q)$ и поэтому имеет элемент порядка $q^2 - 1$. Лемма доказана.

ЛЕММА 8. *Пусть P — конечная неабелева группа такая, что $4t \notin \omega(P)$ для всех натуральных чисел $t \geqslant 2$. Тогда граф $GK(P)$ несвязен и $P, \mu_i, i = 1, 2, \ldots$, такие, как в следующей таблице.*

Простые группы P с $4t \notin \omega(P)$ для $t > 1$

P	μ_1	μ_2	μ_3	μ_4
A_6	4	3	5	
A_7	4, 6	5	7	
A_8	4, 6, 15	7		
J_1	6, 10, 15	7	11	19
$L_2(2^s)$, $s \geqslant 2$	2	$2^s - 1$	$2^s + 1$	
$L_2(p^s)$, p простое $3 < p^s \equiv 3\varepsilon\,(mod 8)$ $\varepsilon = \pm 1$	$(p^s + \varepsilon)/2$	p	$(p^s - \varepsilon)/2$	
${}^2G_2(3^{2s+1})$, $s \geqslant 1$	$6, (3^{2s+1} + 1)/2, 3^{2s+1} - 1$	$3^{2s+1} + 3^{s+1} + 1$	$3^{2s+1} - 3^{s+1} + 1$	
$L_3(2)$	4	3	7	
$L_3(4)$	4	3	5	7
$L_3(2^m)$, $m = 2s \geqslant 4$	$4, 2(2^m - 1)/3, 2^m - 1, (2^{2m} - 1)/3$	$(2^{2m} + 2^m + 1)/3$		
$L_3(2^m)$ $m = 2s + 1 \geqslant 3$	$4, 2(2^m - 1), 2^{2m} - 1$	$2^2 m + 2^m + 1$		
$U_3(2^m)$, $m = 2s \geqslant 2$	$4, 2(2^m + 1), 2^{2m} - 1$	$2^2 m - 2^m + 1$		
$U_3(2^m)$ $m = 2s + 1 \geqslant 3$	$4, 2(2^m + 1)/3, 2^m + 1, (2^{2m} - 1)/3$			
$S_4(2^m)$, $m \geqslant 2$	$4, 2(2^m + 1), 2(2^m - 1), 2^{2m} - 1$	$2^{2m} + 1$		
${}^2B_2(2^{2m+1})$, $m \geqslant 1$	4	$(2^{2m+1} - 1)$	$2^{2m+1} + 2^{2m+1} + 1$	$2^{2m+1} - 2^{2m+1} + 1$

ДОКАЗАТЕЛЬСТВО. Если $4 \notin \mu(P)$, то силовская 2-подгруппа из P является элементарной абелевой, и группа P изоморфна $L_2(2^m)$, $m \geqslant 2$, $L_2(q)$, $q = 8s \pm 3$, ${}^2G_2(3^{2s+1})$, $s \geqslant 1$, или J_1. Множество $\omega(P)$ можно найти так, как это осуществлено в [37] и [38] для случаев $P = {}^2G_2(3^{2s+1})$ и $P = J_1$ соответственно. В остальных случаях оно хорошо известно. Поэтому можно считать, что $4 \in \mu(P)$.

Множество $\omega(P)$ для $P = {}^2B_2(2^{2s+1})$ определил Сузуки [39]. Поскольку A_n содержится в A_{n+1} и в A_9 имеется элемент порядка 12, то $6 \leqslant n \leqslant 8$ в случае $P = A_n$.

Пусть группа P изоморфна $L_n(q)$. Если $n = 2$, то q нечетно, и P содержит элементы порядков $(q-1)/2$ и $(q+1)/2$. Одно из этих чисел делится на 4, и поэтому $(q-1)/2 = 4$ или $(q+1)/2 = 4$. Следовательно, $q = 9$ или $q = 7$ и в этом случае группа P изоморфна A_6 или $L_3(2)$. Если $n \geqslant 3$ и число q нечетно, то по [40] P содержит элемент порядка 8. Пусть число q четно. Для $n = 3$ заключение следует из леммы 5. Пусть $n = 4$. Тогда $P \simeq SL_4(q)$ содержит подгруппу H, изоморфную $GL_3(q)$, в которой найдется элемент порядка 4 и которая при $q > 2$ имеет нетривиальный центр. Поэтому $P = L_4(2) \simeq A_8$, и заключение следует из [38]. Наконец, если $n \geqslant 5$, то P содержит элемент порядка $2^r \geqslant 8$, прообраз которого в $SL_n(q)$ представляется жордановой клеткой размерности n, что неверно.

Пусть группа P изоморфна $U_n(q)$, $n \geqslant 3$. Если q нечетно, то по [40] в P найдется элемент порядка 8. Поэтому q четно. При $n = 3$ заключение следует из леммы 6. Если $n \geqslant 4$, то P содержит подгруппу, изоморфную $GU_3(q)$, в которой существует элемент порядка 4 и порядок центра равен $q+1$. Значит, для любого числа $n \geqslant 4$ группа $U_n(q)$ содержит элемент порядка $4(q+1)$.

Пусть группа P изоморфна $S_{2n}(q)$, $n \geqslant 2$. Тогда P содержит в качестве подгруппы центральное произведение групп $Sp_2(q)$ и $Sp_{2n-2}(q)$, в котором, очевидно, имеется элемент порядка $4t$, $t > 1$, если q нечетно или $n > 2$. Поэтому $P = S_4(2^m)$, и заключение следует из леммы 7.

Поскольку любая простая ортогональная группа размерности $n > 6$ содержит в качестве секции $(n-2)$-мерную ортогональную группу того же типа над тем же полем и $O_5(q) \simeq S_4(q)$, $O_7(2^m) \simeq S_6(2^m)$, $O_6^+(q) \simeq L_4(q)$, $O_6^-(q) \simeq U_4(q)$, то P не может быть ортогональной группой.

По [41, табл. OA8] выполняется

$$L_3(q) \prec G_2(q) \prec {}^3D_4(q) \prec F_4(q) \prec E_6^*(q) \prec E_7(q) \prec E_8(q),$$

и по [38] имеют место

$$U_3(3) \simeq G_2'(2) \prec G_2(2^m),\ L_3(3) \prec {}^2F_4(2) \prec {}^2F_4(2^s),$$

где $A \prec B$ означает, что группа A изоморфна фактор-группе подгруппы группы B, а $E_6^*(q)$ обозначает любую из групп $E_6(q)$ и ${}^2E_6(q)$. Поэтому группа P не может быть изоморфна ни одной из исключительных групп, отличных от ${}^2B_2(q)$ и ${}^2G_2(q)$.

Наконец, если P спорадическая, то по [38], $P \simeq J_1$. Лемма доказана.

ЛЕММА 9. *Пусть G — конечная группа, для которой $\omega(G) = \omega(L)$, где группа L изоморфна $L_3(2^m)$, $m \geqslant 3$, или $U_3(2^m)$, $m \geqslant 2$. Тогда G удовлетворяет п.* в, г *или* д *заключения леммы* 1.

ДОКАЗАТЕЛЬСТВО. По лемме 8, G удовлетворяет заключению леммы 1. Предположим, что G — группа Фробениуса с ядром F и дополнением C. Тогда $\pi(F)$ совпадает с одной из компонент связности графа $GK(L)$. Если порядок группы F четен, то по лемме 2 группа F нильпотентна, и поэтому период ее равен 4. Следовательно, $\pi_1(L) = \{2\}$, что неверно. Поэтому порядок группы F нечетен, порядок группы C четен и по лемме 2 силовская 2-подгруппа T группы C является группой кватернионов порядка 8 или циклической группой порядка 4.

Предположим, T — группа кватернионов порядка 8. Так как T нормализует некоторую силовскую p-подгруппу из $O(C)$ для любого нечетного простого числа p, которая по лемме 2 является циклической, и в G нет элементов порядка $4p$, то подгруппа $O(C)$ тривиальна, и по лемме 2, $\pi_1(G) = \pi(C) \subseteq \{2, 3, 5\}$.

Из леммы 8 вытекает, что $m = 2$ и L изоморфна $U_3(4)$. В этом случае C содержит элемент порядка 15, что противоречит лемме 2.

Итак, T — циклическая группа порядка 4 и $O(C)$ — нормальное 2-дополнение в C. Поскольку в C нет элементов порядка $4t$ для $t > 1$, порождающий элемент группы T инвертирует $O(C)$, и группа $O(C)$ абелева. По лемме 2, группа $O(C)$ циклическая и $\mu_1(G) = \mu(C) = \{4, 2|C|\}$. Это невозможно по лемме 8.

Теперь предположим, что G удовлетворяет п. б. Если порядок группы C четен, то по лемме 3, G содержит элемент порядка $4t > 4$, что неверно. Если число $|C|$ нечетно, то по леммам 5 и 6, A является 2-группой, и поэтому C — циклическая группа порядка $2^{2m} - 1$, тогда, по лемме 3, G содержит элемент порядка $2(2^{2m} - 1)$. Это противоречит леммам 5 и 6, лемма доказана.

ЛЕММА 10. *Пусть G — конечная группа, для которой $\omega(G) = \omega(L)$, где группа L — это $L_3(2^m)$, $m \geqslant 3$, или $U_3(2^m)$, $m > 1$. Тогда G является расширением $\pi_1(L)$-группы посредством L.*

ДОКАЗАТЕЛЬСТВО. По леммам 8, 9 и 1

(10.1) *существует группа P в таблице такая, что P — композиционный фактор группы G, $\mu_2(L) = \mu_j(P)$ для некоторого числа $j > 1$ и $\mu_2(L)$ состоит из единственного числа $u(m, \delta) = (2^{2m}+\delta 2^m+1)/(3, 2^m-\delta)$, где $\delta = 1$ для $L = L_3(2^m)$ и $\delta = -1$ для $L = U_3(2^m)$. Далее, $\mu(P) \subseteq \omega(L)$.*

Поскольку $u(m, \delta) \geqslant 19$ и в силу п. (10.1), P не изоморфна ни одной из групп A_6, A_7, A_8, $L_3(2)$, $L_3(4)$ и J_1.

В дальнейшем будем использовать следующее замечание:

(10.2) *если*

$$(2^{a_1} - 1) \cdots (2^{a_r} - 1) = (2^{b_1} - 1) \cdots (2^{b_t} - 1),$$

где $a_1, ..., a_r, b_1, ..., b_t$ — натуральные числа и $a = \max\{a_1, ..., a_r\} > 6$, то $a = b$, где $b = \max\{b_1, ..., b_t\}$.

Действительно, по лемме 4, существует примитивный простой делитель числа $2^a - 1$, делящий $2^{b_i} - 1$ для некоторого числа i. Следовательно, $a \leqslant b$. Поэтому существует примитивный простой делитель числа $2^b - 1$, делящий $2^j - 1$ для некоторого j. Следовательно, $a \geqslant b$.

Предположим, что группа P изоморфна $L_2(2^s)$. Тогда

$$u(m,\delta) = 2^s \pm 1. \tag{1}$$

После простых преобразований получаем одно из следующих равенств:

$$(2^{3m}-1) = (2^s-1)(3,2^m-1)(2^m-1),\ m \geqslant 3; \tag{2}$$

$$(2^{3m}-1)(2^s-1) = (2^{2s}-1)(3,2^m-1)(2^m-1),\ m \geqslant 3; \tag{3}$$

$$(2^{6m}-1)(2^m-1) = (2^s-1)(2^{2m}-1)(3,2^m+1)(2^{3m}-1),\ m \geqslant 2; \tag{4}$$

$$(2^{6m}-1)(2^m-1)(2^s-1) = (2^{2s}-1)(2^{2m}-1)(3,2^m+1)(2^{3m}-1),\ m \geqslant 2. \tag{5}$$

Если верно (2), то по (10.2), $3m = s$, и из (1) получаем $(2^{2m}+2^m+1)/(3,2^m-1) = 2^{3m}-1$, что невозможно для $m > 1$. Если верно (3), то по 10.2, $3m = 2s = 6k$ для некоторого натурального числа k, и из (1) получаем $2^{4k}+2^{2k}+1 = 3(2^{3k}+1)$, что невозможно. Если же выполняется (4), то $6m = s$ и $(2^{2m}-2^m+1)/(3,2^m+1) = 2^{6m}-1$, что невозможно. Если верно (5), то $3m = s$ и $(2^{2m}-2^m+1)/(3,2^m+1) = 2^{3m}+1$, что снова невозможно.

Предположим, что P изоморфна $L_2(p^s)$, $p^s > 3$, $p^s \equiv \pm 3 \pmod 8$. Тогда $u(m,\delta) = p$ или $u(m,\delta) = (q\pm 1)/2$, $q = p^s$. Если $u(m,\delta) = p$, то, согласно 10.1, число $(q^2-1)/4$ делит $2(2^{2m}-1)$. В частности, $(u(m,\delta)^2-1)/4 = (p^2-1)/4 \leqslant (q^2-1)/4 \leqslant 2(2^{2m}-1)$, а это невозможно при $m > 1$. Если $u(m,\delta) = (q-\varepsilon)/2, \varepsilon = \pm 1$, то, аналогично, $u(m,\delta)+\varepsilon$ делит $2(2m-\delta)$. Это возможно только тогда, когда $m = 3$, $\delta = -1$, $\varepsilon = 1$, но в этом случае $q = 39$ не является степенью простого числа.

Предположим, что группа P изоморфна ${}^2G_2(3^{2s+1})$, $s \geqslant 1$. Тогда

$$u(m,\delta) = 3^{2s+1} + \varepsilon 3^{s+1} + 1,\ \varepsilon = \pm 1. \tag{6}$$

Положим $x = 2^m$, $y = 3^s$ и заметим, что $(x,3y) = 1$. Если $(2^m-\delta,3) = 1$, то $x(x+\delta) = 3y(y+\varepsilon)$, и поэтому x делит $y+\varepsilon$, $3y$ делит $x+\delta$. В частности, $x \leqslant y+1$, $3y \leqslant x+1$. Это невозможно для $m \geqslant 2$.

Если $(2^m-\delta,3) = 3$, то после простых преобразований равенства (6) получаем:

$$(2^m + \delta\varepsilon 3^{s+1} + 2\delta)(2^m - \delta\varepsilon 3^{s+1} - \delta) = 0.$$

Поскольку первый сомножитель левой части нечетен, мы имеем одно из следующих условий:

$$3^{s+1} = 2^m - 1, \quad \delta = 1, \quad \varepsilon = 1; \tag{7}$$

$$3^{s+1} = -2^m + 1, \quad \delta = 1, \quad \varepsilon = -1; \tag{8}$$

$$3^{s+1} = -2^m - 1, \quad \delta = -1, \quad \varepsilon = 1; \tag{9}$$

$$3^{s+1} = 2^m + 1, \quad \delta = -1, \quad \varepsilon = -1. \tag{10}$$

По лемме 4, равенство (7) выполняется только при $m = 2$, $s = 1$, что не имеет места. Очевидно, равенства (8) и (9) невозможны. Предположим, что выполняется равенство (10). Если $m > 3$, то по лемме 4 существует примитивный простой делитель q числа $2^{2m} - 1$. По определению, q не делит $2^2 - 1 = 3$, но q делит $(2^{2m} - 1)/(2^m - 1) = 3^{s+1}$. Это противоречие показывает, что $m \leqslant 3$. Поэтому $m = 3$, $s = 1$, $L = U_3(8)$, $P = {}^2G_2(3^3)$. Это невозможно, поскольку $\omega({}^2G_2(3^3)) \ni 37 \notin \omega(U_3(8))$.

Предположим, группа P изоморфна $S_4(2^s)$, $s > 1$. Тогда $u(m,\delta) = 2^{2s} + 1$, и поэтому выполняется одно из следующих условий:

$$(2^{3m} - 1)(2^{2s} - 1) = (2^{4s} - 1)(2^m - 1)(2^m - 1, 3), \ \delta = 1; \tag{11}$$

$$(2^{6m} - 1)(2^m - 1)(2^{2s} - 1) = (2^{4s} - 1)(2^{3m} - 1)(2^{2m} - 1)(2^m - 1, 3),$$
$$\delta = -1. \tag{12}$$

По (10.2) либо $\delta = 1$, $3m = 4s$, либо $\delta = -1, 6m = 4s$. В первом случае левая часть равенства (11) меньше правой части, а во втором случае левая часть равенства (12) больше правой части.

Пусть группа P изоморфна ${}^2B_2(2^{2s+1})$, $s \geqslant 1$. Тогда верно одно из следующих соотношений:

$$u(m,\delta) = 2^{2s+1} - 1;$$

$$u(m,\delta) = 2^{2s+1} + \varepsilon 2^s + 1, \ \varepsilon = \pm 1.$$

Легко проверить, что ни одно из них не может быть выполнено.

Предположим, группа P изоморфна $L_3(2^s)$, $s \geqslant 3$, или $U_3(2^s)$, $s \geqslant 2$. Тогда $u(m,\delta) = u(s,\varepsilon)$, где $\varepsilon = 1$ для $P = L_3(2^s)$ и $\varepsilon = -1$ для $P = U_3(2^s)$.

Легко проверить, что это равенство выполняется только при $m = s$ и $\delta = \varepsilon$. Поэтому группа P изоморфна L. По леммам 9, 5б и 6б, G является расширением разрешимой $\pi_1(G)$-группы посредством L. Поскольку $\pi_1(G) = \pi_1(L)$, лемма доказана.

Основные результаты

ТЕОРЕМА 1. *Пусть G — конечная группа, для которой $\omega(G) = \omega(L)$, где $L = L_3(2^m)$, $m \geqslant 1$, или $L = U_3(2^m)$, $m \geqslant 2$. Тогда G изоморфна L.*

ДОКАЗАТЕЛЬСТВО. Этот факт известен для группы L, равной $L_3(2)$ или $L_3(4)$ (см. введение). Поэтому можно считать, что $m \geqslant 3$ для $L = L_3(2^m)$. По лемме 10 фактор-группа G/A изоморфна L для некоторой нормальной $\pi_1(L)$-подгруппы A. Докажем, что $A = 1$. Для этого, не нарушая общности, можно считать, что A — элементарная абелева p-группа.

Предположим, что $A \neq 1$. Поскольку граф $GK(G)$ несвязен, то $C_G(A) \neq G$. Так как группа L проста, то $C_G(A) = A$, и G индуцирует при сопряжении в A группу автоморфизмов, изоморфную L. Если $L = L_3(2^m)$, где число m четно, или $L = U_3(2^m)$, где m нечетно, то L содержит подгруппу H, изоморфную $U_3(2)$, которая является группой Фробениуса с ядром порядка 9 и кватернионным дополнением C порядка 8. Итак, если $p = 2$, то по лемме 2.2, G содержит элемент порядка $8 \notin \omega(L)$.

Если порядок A нечетен, то $A_0 = C_A(t) \neq 1$ для некоторой инволюции t из C, и четверная группа $C/\langle t \rangle$ действует на A_0. Поскольку некоторая инволюция из $C/\langle t \rangle$ централизует в A_0 нетривиальный элемент, G содержит элемент порядка $4p$ вопреки предположению. Поэтому можно предполагать, что число m нечетно, если $L = L_3(2^m)$, и m четно, если $L = U_3(2^m)$. В частности, в L нет элементов порядка 6. Поскольку L содержит подгруппу Фробениуса с циклическим ядром порядка $2^{2m} \pm 2^m + 1$ и дополнением порядка 3, порядок группы A нечетен по лемме 2.2.

Так как центр Z силовской 2-подгруппы из G нециклический, существует инволюция $z \in Z$, для которой $C_A(z) \neq 1$ и силовская 2-подгруппа из $C_G(z)$ действует на $C_A(t)$. Если $x^2 = z$, то x не может централизовать нетривиальный элемент в $C_A(z)$, и поэтому x инвертирует $C_A(z)$. По 5.1, 5.2, 6.1, 6.2 существуют два элемента x, y такие, что $x^2 = y^2 = z$ и xy — элемент порядка 4. Поскольку xy централизует $C_A(z)$, G содержит элемент порядка $4p$ для некоторого числа $p > 1$. Это последнее противоречие завершает доказательство теоремы.

В отличие от групп $L_3(2^m)$ и $U_3(2^m)$, для простых симплектических групп $S_4(q)$ верно следующее

ПРЕДЛОЖЕНИЕ. *Для любого целого числа $m \geqslant 2$ существует расширение E элементарной 2-группы посредством $L_2(2^{2m})$, для которого $\omega(E) = \omega(S_4(2^m))$.*

ДОКАЗАТЕЛЬСТВО. Пусть N — естественный модуль для $L = SL_2(2^{2m}) = L_2(2^{2m})$ над полем F порядка 2^{2m} и пусть $V = N \otimes N^\sigma$, где σ — автоморфизм порядка 2 поля F. Тогда для любого элемента $h \in L$ порядка $t \neq 2$ характеристические корни преобразования h пространства V равны $\lambda\lambda^{2^s}$, $\lambda^{-1}\lambda^{2^s}$, $\lambda\lambda^{-2^s}$, $\lambda^{-1}\lambda^{-2^s}$, где λ — примитивный корень степени t из единицы. Поэтому V тогда и только тогда содержит собственный вектор для h с собственным значением 1, когда t делит $2^m - 1$ или $2^m + 1$. Поскольку $\mu(L) = \{2, 2^{2m} - 1, 2^{2m} + 1\}$, для естественного полупрямого произведения E модуля V на L имеет место равенство

$$\mu(E) = \{4, 2(2^m + 1), 2(2^m - 1), 2^{2m} - 1, 2^{2m} + 1\}.$$

По лемме 8, $\omega(E) = \omega(S_4(2^m))$. Предложение доказано.

ТЕОРЕМА 2. *Пусть G — конечная простая неабелева группа такая, что $4t \notin \omega(G)$ для всех натуральных чисел $t > 1$. Тогда верно одно из двух следующих утверждений:*

а) *группа G изоморфна A_7; A_8; J_1; $L_2(2^m)$, $m > 1$; $L_2(q)$, q — степень простого числа, $3 < q \equiv \pm 3 (\mathrm{mod}\, 8)$; ${}^2G_2(3^{2m+1})$, $m > 1$; ${}^2B_2(2^{2m+1})$, $m \geqslant 1$; $L_3(2^m)$, $m \geqslant 1$, или $U_3(2^m)$, $m > 1$, и G распознаваема по $\omega(G)$;*

б) *группа G изоморфна A_6 или $S_4(2^m)$, $m > 1$, и существует бесконечно много попарно неизоморфных групп H таких, что $\omega(H) = \omega(G)$.*

ДОКАЗАТЕЛЬСТВО. По лемме 8, G изоморфна одной из групп заключения теоремы. Распознаваемость групп из п. а, отличных от $L_3(2^m)$, $m \geqslant 1$, и $U_3(2^m)$, $m > 1$, доказана Р. Брандлом, Ч. Прэгер и В. Ши (см. введение). Группы $L_3(2^m)$, $m \geqslant 1$ и $U_3(2^m)$, $m > 1$, распознаваемы по теореме 1. Заключение известно также и для A_6 (см. [23]). Наконец, если группа G изоморфна $S_4(2^m)$, $m > 1$, то по предложению существует группа H такая, что $\omega(H) = \omega(G)$ и H содержит нетривиальную разрешимую подгруппу. По [42, лемма 1] существует бесконечно много таких групп H. Теорема доказана.

ЗАМЕЧАНИЕ. Недавно Ж. Ан и В. Ши [43] доказали распознаваемость групп $L_3(2^m)$, $m \not\equiv 0 \pmod 6$ и $U_3(2^m)$, $m \not\equiv 3 \pmod 6$, и высказали гипотезу, что число неабелевых простых нераспознаваемых групп конечно. Теорема 2, в частности, опровергает эту гипотезу.

М. Ч. Су и Ч. П. Чао выражают свою благодарность профессору Вуджи Ши за руководство и помощь.

ЛИТЕРАТУРА

1. *W. Shi*, A characteristic property of A_5 (in Chinese), J. Southwest-China Teachers University, **3** (1986), 11—14.

2. *W. Shi*, A characteristic property of $PSL_2(7)$, J. Aust. Math. Soc., Ser. A, **36**, N 3 (1984), 354—356.

3. *W. Shi*, A characterization of some projective special linear groups (in Chinese), J. Southwest-China Teachers Univ., Ser. B2, 1985, 2—10.

4. *W. Shi*, A characteristic property of J_1 and $PSL_2(2^n)$ (in Chinese), Adv. Math., Beijing, **16** (1987), 397—401.

5. *R. Brandl, W. Shi*, The characterization of $PSL(2,q)$ by its element orders, J. Algebra, **163**, N 1 (1994), 109—114.

6. *W. Shi*, A characterization of Suzuki simple groups, Proc. Am. Math. Soc., **114**, N 3 (1992), 589—591.

7. *R. Brandl, W. Shi*, A characterization of finite simple groups with abelian Sylow 2-subgroups, Ric. Mat., **42**, N 1 (1993), 193—198.

8. *H. W. Deng, W. J. Shi*, The characterization of Ree groups ${}^2F_4(q)$ by their element orders, J. Algebra, **217**, N 1 (1999), 180—187.

9. *W. Shi*, A characterization of some projective special linear groups, J. Math. Res. Expo., **5** (1985), 191—200.

10. *F. J. Liu*, A characteristic property of projective special linear group $L_3(8)$ [in Chinese], J. Southwest-China Normal Univ., **22**, N 2 (1997), 131—134.

11. *S. Lipschutz, W. Shi*, Finite groups whose element orders do not exceed twenty, Prog. Nat. Sci., **10**, N 1 (2000), 11—21.

12. *M. R. Aleeva*, On recognizability of groups $U_3(q), q$ odd, Маломерная топология и комбинаторная теория групп, Тез. докл. междунар. конф. Челябинск, 1999, 12.

13. *W. Shi*, A characterization of the finite simple group $U_4(3)$, An. Univ. Timiş., Ser. Ştiinţe Mat., **30**, N 2—3 (1992), 319—323.

14. *W. Shi, H. L. Li*, A characteristic property of M_{12} and $PSU(6,2)$ (in Chinese), Acta Math. Sin., **32**, N 6 (1989), 758—764.

15. *W. Shi, C. Y. Tang*, A characterization of some orthogonal groups, Prog. Nat. Sci., **7**, N 2 (1997), 155—162.

16. *W. Shi*, A characteristic property of Mathieu groups [in Chinese], Chin. Ann. Math., Ser. A, **9**, N 5 (1988), 575—580.

17. *W. Shi*, A characterization of the Conway simple group Co_2, J. Math. Res. Expo., **9** (1989), 171—172.

18. *W. Shi*, A characterization of the Higman-Sims group, Houston J. Math., **16**, N 4 (1990), 597—602.

19. *H. L. Li, W. Shi*, A characteristic property of some sporadic simple groups [in Chinese], Chin. Ann. Math, Ser. A, **14**, N 2 (1993), 144—151.

20. *W. Shi*, The characterization of the sporadic simple groups by their element orders, Algebra Colloq., **1**, N 2 (1994), 159—166.

21. *W. Shi*, A characteristic property of A_8, Acta Math. Sin., New Ser., **3** (1987), 92—96.

22. *R. Brandl, W. Shi*, Finite groups whose element orders are consecutive integers, J. Algebra, **143**, N 2 (1991), 388—400.

23. *C. E. Praeger, W. Shi*, A characterization of some alternating and symmetric groups, Commun. Algebra, **22**, N 5 (1994), 1507—1530.

24. *В. Д. Мазуров*, Характеризации конечных групп множествами порядков их элементов, Алгебра и логика, **36**, N 1 (1997), 37—53.

25. *А. В. Заварницин*, Порядки элементов в накрытиях групп $L_n(q)$ и распознаваемость знакопеременной группы A_{16}, Новосибирск, ГНИУ Ин-т дискрет. матем. информ., препринт N 48, 2000.

26. *А. С. Кондратьев, В. Д. Мазуров*, Распознавание знакопеременных групп простой степени по порядкам их элементов, Сиб. матем. ж., **41**, N 2 (2000), 360—371.

27. *А. В. Заварницин*, Распознавание по множеству порядков элементов знакопеременных групп степени $r+1$ и $r+2$ для простого r, Новосибирск, ГНИУ Ин-т дискр. матем. информ., препринт N 47, 2000.

28. *J. S. Williams*, Prime graph components of finite groups, J. Algebra, **69**, N 2 (1981), 487—513.

29. *J. G. Thompson*, Normal p-complements for finite groups, Math. Z., **72**, N 2 (1960), 332—354.

30. *H. Zassenhaus*, Kennzeichnung endlicher linearen Gruppen als Permutationsgruppen, Abh. Math. Semin. Univ. Hamb., **11** (1936), 17—40.

31. *H. Zassenhaus*, Über endliche Fastkörper, Abh. Math. Semin. Univ. Hamb., **11** (1936), 187—220.

32. *K. Zsigmondy*, Zur Theorie der Potenzreste, Monatsh. Math. Phys., **3** (1892), 265—284.

33. *J. Diedonne*, La géométrie des groupes classiques, Berlin, Springer-Verlag, 1955.

34. *М. Холл*, Теория групп, М., ИЛ, 1962.

35. *M. Aschbacher, G. M. Seitz*, Involutions in Chevalley groups groups over fields of even order, Nagoya Math. J., **63**, N 1 (1976), 1—91.

36. *R. Carter*, Centralizers of semisimple elements in finite classical groups, Proc. Lond. Math. Soc., III. Ser., **42**, N 1 (1981), 1—41.

37. *H. N. Ward*, On Ree's series of simple groups, Trans. Am. Math. Soc., **121**, N 1 (1966), 62—89.

38. *J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker, R. A. Wilson*, Atlas of finite groups, Oxford, Clarendon Press, 1995.

39. *M. Suzuki*, On a class of doubly transitive groups, Ann. Math. (2), **75**, N 1 (1962), 105—145.

40. *R. W. Carter, P. Fong*, The Sylow 2-subgroups of the finite classical groups, J. Algebra, **1**, N 2 (1964), 139–151.

41. *E. Stensholt*, Certain embeddings among finite simple groups of Lie type, J. Algebra, **53**, N 1 (1978), 136–185.

42. *В. Д. Мазуров*, Распознавание конечных групп по множеству порядков их элементов, Алгебра и логика, **37**, N 6 (1998), 651–666.

43. *J. B. An, W. J. Shi*, The characterization of finite simple groups with no elements of order six, Commun. Algebra, **28**, N 7 (2000), 3351–3358.

Адреса авторов:

Поступило 29 октября 1998 г.

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

M. C. XU and H. P. CAO
Department of Mathematics,
Sichuan University,
610000, Chengdu,
CHINA.