Сибирский математический журнал
Январь—февраль, 2011. Том 52, № 1

УДК 512.542

О КОНЕЧНЫХ ГРУППАХ, ИЗОСПЕКТРАЛЬНЫХ ПРОСТЫМ ЛИНЕЙНЫМ И УНИТАРНЫМ ГРУППАМ

А. В. Васильев, М. А. Гречкосеева, А. М. Старолетов

Аннотация. Пусть L — простая линейная или унитарная группа размерности больше трех над конечным полем характеристики p. Рассматривается класс конечных групп, изоспектральных группе L. Известно, что любая группа из этого класса имеет единственный неабелев композиционный фактор. Доказано, что при $L \neq U_4(2), U_5(2)$ этот фактор изоморфен либо L, либо группе лиева типа над полем характеристики, отличной от p.

Ключевые слова: конечная группа, спектр группы, простая группа, линейная группа, унитарная группа, композиционный фактор.

Спектром $\omega(G)$ конечной группы G называется множество порядков ее элементов. Две группы называются *изоспектральными*, если у них одинаковые спектры. Конечная группа L называется *распознаваемой по спектру*, если любая конечная группа G со свойством $\omega(G) = \omega(L)$ изоморфна L. Говорят, что для группы L решена *проблема распознаваемости по спектру*, если известно число $h(L)$ попарно неизоморфных конечных групп, изоспектральных L. Таким образом, распознаваемость группы L эквивалентна равенству $h(L) = 1$. Последние результаты, относящиеся к проблеме распознаваемости по спектру, можно найти в обзорах [1, 2].

При решении проблемы распознаваемости по спектру для конечной группы L естественным образом возникает задача о композиционном строении конечных групп, изоспектральных L. Настоящая работа посвящена изучению данного аспекта проблемы распознаваемости для конечных простых линейных и унитарных групп. Для обозначения этих групп используются матричная нотация из [3] и сокращение $L_n^\varepsilon(q)$, где $\varepsilon \in \{+, -\}$, $L_n^+(q) = L_n(q)$ и $L_n^-(q) = U_n(q)$. Поскольку проблема распознаваемости полностью решена для групп $L_2(q)$ [4, 5], $L_3(q)$ [6–8] и $U_3(q)$ [6, 9], эти группы в работе не рассматриваются.

Теорема 1. *Пусть $L = L_n^\varepsilon(q)$, где $n \geq 4$, $\varepsilon \in \{+, -\}$ и $(n, q) \neq (4, 2)$. Тогда среди неабелевых композиционных факторов конечных групп, изоспектральных L, нет знакопеременных групп.*

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (коды проектов 08–01–00322, 10–01–90007–Бел_а), Совета по грантам Президента РФ (НШ–3669.2010.1 и МК–2136.2010.1), АВЦП Рособразования «Развитие научного потенциала высшей школы» (проект 2.1.1.419), ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракты № 02.740.11.0429, 02.740.11.5191), а также Лаврентьевского гранта для коллективов молодых ученых СО РАН (постановление Президиума СО РАН № 43 от 04.02.2010).

Теорема 2. *Пусть $L = L_n^{\varepsilon}(q)$, где $n \geq 4$, $\varepsilon \in \{+,-\}$ и $(\varepsilon, n, q) \neq (-,5,2)$. Тогда среди неабелевых композиционных факторов конечных групп, изоспектральных L, нет спорадических групп и нет группы Титса ${}^2F_4(2)'$.*

Теорема 3. *Пусть $L = L_n^{\varepsilon}(q)$, где $n \geq 4$, $\varepsilon \in \{+,-\}$, $(\varepsilon, n, q) \neq (-,4,2)$ и q — степень простого числа p. Тогда среди неабелевых композиционных факторов конечных групп, изоспектральных L, нет групп лиева типа над полем характеристики p, отличных от L.*

Отметим, что для симплектических и ортогональных групп аналогичные результаты установлены в [10].

§ 1. Обозначения и предварительные сведения

Обозначения спорадических групп, простых классических групп и простых исключительных групп лиева типа взяты из [3]. Знакопеременная группа степени n обозначается через Alt_n.

Для ненулевого целого числа n через $\pi(n)$ обозначается множество простых делителей числа n; через n_r, где r — простое число, обозначается r-часть числа n, т. е. наибольшая степень числа r, делящая n, и через $n_{r'}$ — r'-часть числа n, т. е. модуль отношения n/n_r. Если n — ненулевое целое число, m — нечетное простое число и $(n,m) = 1$, то через $e(m,n)$ обозначается мультипликативный порядок числа n по модулю m. Для нечетного n положим $e(2,n) = 1$, если $n \equiv 1 \pmod 4$, и $e(2,n) = 2$, если $n \equiv 3 \pmod 4$.

Пусть n — целое число, по модулю большее 1. Простое число r называется *примитивным простым делителем* для $n^i - 1$, если $e(r,n) = i$. Существование примитивных делителей для почти всех пар n и i установлено Жигмонди.

Лемма 1.1 [Жигмонди, 11]. *Пусть n — целое число и $|n| > 1$. Тогда для каждого натурального числа i найдется простое число r такое, что $e(r,n) = i$, за исключением случаев, когда $(n,i) \in \{(2,1),(2,6),(-2,2),(-2,3),(3,1),(-3,2)\}$.*

Далее в статье под записью $r_i(n)$ будет подразумеваться какой-нибудь примитивный делитель для $n^i - 1$, если такие делители существуют. Произведение всех примитивных делителей разности $n^i - 1$ с учетом кратности называется *наибольшим примитивным делителем* и обозначается через $k_i(n)$. Отметим, что свойство примитивности делителя зависит от пары (n,i) и не определяется однозначно числом $n^i - 1$. Например, $k_6(2) = 1$, хотя $k_3(4) = 7$ и $k_6(-2) = 7$, или $k_2(2) = 3$, хотя $k_2(-2) = 1$.

Несложно проверить, что $k_1(n) = |n-1|/2$, если $n \equiv 3 \pmod 4$, и $k_1(n) = |n-1|$ в остальных случаях, а также, что $k_2(n) = |n+1|/2$, если $n \equiv 1 \pmod 4$, и $k_2(n) = |n+1|$ в остальных случаях. Для $i > 2$ из [12] следует, что

$$k_i(n) = \frac{|\Phi_i(n)|}{(r, \Phi_{i_{r'}}(n))}, \qquad (1)$$

где $\Phi_i(x)$ — это i-й круговой многочлен и r — наибольший простой делитель числа i, причем если $i_{r'}$ не делит $r-1$, то $(r, \Phi_{i_{r'}}(n)) = 1$.

Лемма 1.2. *Пусть i — нечетное простое число, q — степень простого числа p и $\varepsilon \in \{+,-\}$. Если $(i, \varepsilon q) \neq (3,-2)$, то $k_i(\varepsilon q) > q^{i-2}/p$. Если к тому же $(i,\varepsilon) \neq (q+1,-)$, то $k_i(\varepsilon q) > q^{i-2}$.*

Доказательство следует из [10, лемма 3.1].

Графом Грюнберга — Кегеля $GK(G)$, или *графом простых чисел*, группы G называется граф с множеством вершин $\pi(G)$, в котором две различные вершины p и q смежны тогда и только тогда, когда $pq \in \omega(G)$. Число компонент связности графа $GK(G)$ обозначается через $s(G)$, а сами компоненты связности — через $\pi_i(G)$, где $1 \le i \le s(G)$. Если G четного порядка, то по умолчанию $2 \in \pi_1(G)$. В соответствии с этим разбиением $\omega_i(G)$ — это подмножество $\pi_i(G)$-чисел в $\omega(G)$ для любого $1 \le i \le s(G)$. Строение конечных групп с несвязным графом простых чисел описано Грюнбергом и Кегелем.

Лемма 1.3 [13]. *Если G — конечная группа со свойством $s(G) > 1$, то выполняется одно из следующих утверждений:*

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 неабелева простая группа S такая, что $S \le \overline{G} = G/K \le \mathrm{Aut}(S)$ для некоторой нильпотентной нормальной подгруппы K из G; более того, K и $\overline{G}/S$ являются $\pi_1(G)$-группами, $s(S) \ge s(G)$ и для любого $1 < i \le s(G)$ существует $1 < j \le s(S)$ такое, что $\omega_i(G) = \omega_j(S)$.*

Конечные простые группы с несвязным графом простых чисел были описаны Уильямсом [13] и А. С. Кондратьевым [14]. Полный список этих групп с исправленными неточностями можно найти в [15, табл. 1a–1c]. Как следует из результатов Уильямса и Кондратьева, если S — простая группа и $s(S) > 1$, то для любого $1 < i \le s(S)$ множество $\omega_i(S)$ имеет единственный максимальный по делимости элемент [16, лемма 4]. В указанных таблицах и в настоящей работе этот максимальный элемент обозначается через $n_i(S)$.

Напомним, что независимым множеством вершин, или *кокликой*, в графе Γ называется подмножество вершин, попарно не смежных между собой в Γ. Будем обозначать через $t(\Gamma)$ неплотность графа Γ, т. е. наибольшее число вершин в его кокликах. Для группы G положим $t(G) = t(GK(G))$. По аналогии для любого простого числа r определим r-неплотность $t(r, G)$ как наибольшее число вершин в кокликах графа $GK(G)$, содержащих вершину r.

Лемма 1.4 [17, 18]. *Пусть L — конечная неабелева простая группа такая, что $t(L) \ge 3$ и $t(2, L) \ge 2$, а G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$. Тогда выполняются следующие утверждения:*

1) *существует неабелева простая группа S такая, что $S \le \overline{G} = G/K \le \mathrm{Aut}(S)$, где K — максимальная нормальная разрешимая подгруппа группы G;*

2) *для каждой коклики ρ вершин графа $GK(G)$, порядок которой больше 2, не более чем одно число из ρ делит произведение $|K| \cdot |\overline{G}/S|$. В частности, $t(S) \ge t(G) - 1$;*

3) *каждое простое число $r \in \pi(G)$, не смежное в $GK(G)$ с числом 2, не делит произведение $|K| \cdot |\overline{G}/S|$, в частности, $t(2, S) \ge t(2, G)$.*

Лемма 1.5. *Пусть G — конечная группа, K — нормальная подгруппа в G и $r \in \pi(K)$. Предположим, что фактор-группа G/K содержит секцию, изоморфную нециклической абелевой p-группе для некоторого нечетного простого числа p, отличного от r. Тогда $rp \in \omega(G)$.*

Доказательство. Пусть R — некоторая силовская r-подгруппа группы K и N — ее нормализатор в G. В силу аргумента Фраттини $G/K \simeq N/(K \cap N)$ и, следовательно, группа N и ее нормальная подгруппа R удовлетворяют условию теоремы. Поэтому можно считать, что $G = N$ и $K = R$. Поскольку $p \neq 2$, группа G/K, содержащая секцию, изоморфную нециклической абелевой p-группе, должна содержать и нециклическую абелеву p-подгруппу. Дальнейшее прямо следует из [19, гл. 5, теорема 3.16].

§ 2. Свойства простых линейных и унитарных групп

Из формул порядков простых линейных и унитарных групп вытекает, что множество простых делителей порядка группы $L_n^\varepsilon(q)$ устроено следующим образом:

$$r \in \pi(L_n^\varepsilon(q)) \text{ тогда и только тогда, когда } e(r, \varepsilon q) \leq n \text{ или } r \text{ делит } q. \qquad (2)$$

Мы будем использовать критерий смежности в графах простых чисел линейных и унитарных групп из [20]. В этой работе при формулировке критерия для унитарных групп используется функция $\nu(x)$, действующая из $\mathbb{N}$ в $\mathbb{N}$ по следующему правилу:

$$\nu(x) = \begin{cases} 2x, & \text{если } x \text{ нечетно}, \\ x/2, & \text{если } x \equiv 2 \pmod 4, \\ x, & \text{если } x \equiv 0 \pmod 4. \end{cases} \qquad (3)$$

Несложно проверить, что

$$\nu(\nu(x)) = x, \qquad (4)$$

$$e(m, -x) = \nu(e(m, x)) \qquad (5)$$

для любого ненулевого целого x и простого m. Используя это замечание, мы объединяем критерии для линейных и унитарных групп в следующих трех леммах.

Лемма 2.1 [20, предложения 2.1, 2.2]. *Пусть $L = L_n^\varepsilon(q)$ — простая группа над полем характеристики p. Пусть r, s — нечетные простые числа из $\pi(L)$, отличные от p. Положим $k = e(r, \varepsilon q)$, $l = e(s, \varepsilon q)$ и предположим, что $2 \leq k \leq l$. Тогда r и s несмежны в $GK(L)$ в том и только в том случае, когда $k + l > n$ и k не делит l.*

Лемма 2.2 [20, предложение 3.1]. *Пусть $L = L_n^\varepsilon(q)$ — простая группа над полем характеристики p. Пусть $r \in \pi(L)$ и $r \neq p$. Тогда r и p несмежны в $GK(L)$ в том и только в том случае, когда выполняется одно из следующих утверждений:*

1) *r нечетно и $e(r, \varepsilon q) > n - 2$;*
2) *$L = L_2(q)$ и $r = 2$;*
3) *$L = L_3^\varepsilon(q)$, $r = 3$ и $(\varepsilon q - 1)_3 = 3$.*

Лемма 2.3 [20, предложения 4.1, 4.2]. *Пусть $L = L_n^\varepsilon(q)$ — простая группа над полем характеристики p. Пусть r — простой делитель числа $\varepsilon q - 1$ и s — нечетное простое число, отличное от p. Положим $k = e(s, \varepsilon q)$. Тогда s и r несмежны в $GK(L)$ в том и только в том случае, когда выполняется одно из следующих утверждений:*

1) *$k = n$, $n_r \leq (\varepsilon q - 1)_r$, и если $n_r = (\varepsilon q - 1)_r$, то $2 < (\varepsilon q - 1)_r$;*
2) *$k = n - 1$ и $(\varepsilon q - 1)_r \leq n_r$.*

Как отмечено во введении, для линейных и унитарных групп размерности меньше четырех проблема распознаваемости уже решена. Кроме того, получен ряд результатов, касающихся групп больших размерностей.

Лемма 2.4. 1. *Если L — одна из простых групп $L_n(2^m)$, где $m \geq 1$, $n \geq 4$; $U_4(2^m)$, где $m > 1$, и G — конечная группа со свойством $\omega(G) = \omega(L)$, то $L \leq G \leq \mathrm{Aut}(L)$.*

2. *Если L — одна из групп $L_4(3)$, $L_5(3)$, $L_6(3)$, $U_6(2)$, $U_4(3)$, $U_4(5)$ и G — конечная группа со свойством $\omega(G) = \omega(L)$, то $L \leq G \leq \mathrm{Aut}(L)$.*

3. *Группа $L = U_4(2)$ изоспектральна группе, имеющей неабелев композиционный фактор, изоморфный $\mathrm{Alt}_5 \simeq L_2(4)$.*

4. *Группа $L = U_5(2)$ изоспектральна группе, имеющей неабелев композиционный фактор, изоморфный спорадической группе Матье M_{11}.*

Доказательство. Полные ссылки на доказательства утверждений 1 и 2 можно найти в [21, 22] и [1] соответственно. Утверждения 3 и 4 доказаны в [23].

Если L — одна из групп, перечисленных в пп. 1 и 2 леммы 2.4, то единственный неабелев композиционный фактор конечной группы, изоспектральной L, изоморфен L. Среди перечисленных групп только группа $L_4(2)$ изоморфна знакопеременной группе, а именно группе Alt_8, и нет ни одной, изоморфной спорадической группе. Значит, если $L \neq L_4(2)$, то заключения теорем 1–3 верны для L. С другой стороны, пп. 3 и 4 леммы 2.4 показывают, что группа $U_4(2)$ не удовлетворяет ни заключению теоремы 1, ни заключению теоремы 3, а группа $U_5(2)$ не удовлетворяет заключению теоремы 2. Кроме того, $\pi(U_4(2)) = \{2, 3, 5\}$, и, используя [3], несложно проверить, что при $L = U_4(2)$ утверждение теоремы 2 верно. Таким образом, при доказательстве теорем 1–3 можно считать, что группа L не содержится в множестве

$$\mathscr{L} = \{L_n(2^m) \mid m \geq 1\} \cup \{U_4(2^m) \mid m \geq 1\} \cup \{L_4(3), L_5(3), L_6(3), U_6(2), U_4(3), U_4(5)\}.$$

Тогда из [20, 24] следует, что $t(L) \geq 3$ и $t(2, L) \geq 2$, поэтому для групп, изоспектральных L, выполнено заключение леммы 1.4.

§ 3. Доказательство теоремы 1

Пусть $L = L_n^\varepsilon(q)$, где $n \geq 4$, $\varepsilon \in \{+, -\}$ и q — степень простого числа p. Пусть G — конечная группа, изоспектральная L, и K — разрешимый радикал группы G. Предположим, что заключение теоремы 1 не выполнено. Тогда $L \notin \mathscr{L}$ и, применяя лемму 1.4, получаем, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$, где $S \simeq \mathrm{Alt}_m$ для некоторого $m \geq 5$.

Допустим, что для группы L нашлось множество M из трех натуральных чисел, удовлетворяющее следующим условиям:

(*) для любого $i \in M$ число $k_i(q)$ отлично от единицы;

(**) примитивные простые делители $r_i(\varepsilon q)$, $r_j(\varepsilon q)$, где $i, j \in M$, несмежны в $GK(L)$ при $i \neq j$.

Рассмотрим числа $k_i(\varepsilon q)$, где i пробегает M. В силу п. 2 леммы 1.4 по крайней мере два из этих трех чисел взаимно просты с $|K| \cdot |\overline{G}/S|$ и лежат в $\omega(S)$. Обозначим их через a и b. Предположим, что существует простой делитель r числа a такой, что $r \leq m/2$. Поскольку все простые делители числа b не смежны с r в $GK(G)$, все они больше, чем $m/2$. Следовательно, либо все простые делители числа a, либо все простые делители числа b больше, чем $m/2$. Обозначим через k то из чисел a и b, для которого это верно.

Пусть r' и r'' — два различных простых делителя числа k. Тогда $r' + r'' > m$, поэтому $r'r'' \notin \omega(S)$ и, значит, $r'r'' \in \omega(L) \setminus \omega(G)$, что невозможно. Пусть k — степень простого числа r, большая r. Тогда $r^2 > (m/2)^2 > m$ и тем самым

$r^2 \in \omega(L) \setminus \omega(G)$; противоречие. Следовательно, k — простое число, и условие $k \in \omega(S)$ влечет неравенство $m \geq k$. Таким образом, $m \geq k_i(\varepsilon q)$ для некоторого $i \in M$.

Идея дальнейшего рассуждения такова. С помощью специального выбора множества M ограничим m снизу через n и q. Затем придем к противоречию, показав, что за некоторыми исключениями, которые будут разобраны отдельно, максимальная степень числа p в $\omega(S)$ будет строго больше максимальной степени числа p в $\omega(L)$. Будем называть максимальную степень числа p в спектре конечной группы *p-периодом* этой группы.

Обозначим p-период группы L через p^l. Как следует из [25, предложение 0.5], число l удовлетворяет неравенствам

$$p^{l-1} + 1 \leq n \leq p^l. \tag{6}$$

Предположим, что $n \geq 17$. Тогда в полуинтервале $(n/2, n]$ найдется по крайней мере три различных простых числа, причем каждое из них, очевидно, не меньше, чем $\max\{(n+1)/2, 11\}$. В силу леммы 2.1 множество M, состоящее из трех таких чисел, удовлетворяет условиям $(*)$ и $(**)$. Поэтому по крайней мере для одного простого числа $i \in M$ число $k_i(\varepsilon q)$ является простым числом, не превосходящим m.

Поскольку $i \geq \max\{(n+1)/2, 11\}$, из леммы 1.2 следует, что

$$m \geq k_i(\varepsilon q) > \max\{q^{\frac{n-3}{2}}/p, q^9/p\}.$$

Поскольку $m > q^9/p > p^7+1$, в группе S есть элемент порядка p^7. Следовательно, $p^7 \in \omega(L)$ и $l \geq 7$. Для $l \geq 7$ выполнено неравенство $l + 2 < (2^{l-1} - 2)/2$, поэтому $l + 2 < (p^{l-1} - 2)/2$. Из (6) следует, что $(p^{l-1} - 2)/2 \leq (n-3)/2$. Таким образом, $l + 2 < (n-3)/2$, и, значит, $m > q^{(n-3)/2}/p > p^{l+2}/p = p^{l+1}$, откуда, $p^{l+1} \in \omega(G) \setminus \omega(L)$; противоречие.

Предположим, что $n \in \{13, 14, 15, 16\}$. Множество $M = \{7, 11, 13\}$ удовлетворяет условиям $(*)$ и $(**)$, поэтому $m \geq \min\{k_7(\varepsilon q), k_{11}(\varepsilon q), k_{13}(\varepsilon q)\}$. Поскольку $q+1$ не может равняться 7, из леммы 1.2 вытекает, что $m > q^5$. Если $q > 2$, то S содержит элемент порядка p^5, а значит, $l \geq 5$. Но тогда $n \geq p^{l-1} + 1 \geq 2^4 + 1 = 17$; противоречие. Если $q = 2$, то $m \geq \min\{k_7(\varepsilon 2), k_{11}(\varepsilon 2), k_{13}(\varepsilon 2)\} = 43$ и, значит, $37 \in \omega(S)$. Однако $e(37, 2) = 36$, откуда $37 \notin \omega(L)$; противоречие.

Пусть $n = 11, 12$. Множество $M = \{7, 9, 11\}$ удовлетворяет условиям $(*)$ и $(**)$. Из равенства $k_9(\varepsilon q) = (q^6 + \varepsilon q^3 + 1)/(3, \varepsilon q - 1)$ и леммы 1.2 несложно вывести, что $m > q^4 + 2$. Поэтому S содержит элемент порядка q^4, а значит, $l \geq 4$. Если $p \neq 2$, то $n \geq p^{l-1} + 1 \geq 3^3 + 1 = 28$, что невозможно. Если $p = 2$, а $q > 2$, то $m > 4^4 + 2$, стало быть, $2^8 \in \omega(G) \setminus \omega(L)$. Если $q = 2$, то $m \geq 19$ и $2 \cdot 13 \in \omega(S)$. Однако $2 \cdot 13 \notin \omega(L)$; противоречие.

Предположим, что $n = 9, 10$. Множество $M = \{7, 8, 9\}$ удовлетворяет условиям $(*)$ и $(**)$. Поэтому $m \geq k_8(\varepsilon q) = (q^4 + 1)/(2, \varepsilon q - 1)$. Если $q > 3$, то сразу получаем противоречие, так как в группе L нет элементов порядка p^3 при $p > 3$ и нет элементов порядка p^6 при $p \in \{2, 3\}$. Если $q = 3$, то $m \geq 42$, откуда $31 \in \omega(S)$. Поскольку $e(31, 3) = 30$, в группе L не может быть элемента порядка 31. Если $q = 2$, то $m \geq 17$ и, как и в предыдущем абзаце, имеем $2 \cdot 13 \in \omega(S) \setminus \omega(L)$, что невозможно.

Пусть $n = 8$. Множество $M = \{5, 7, 8\}$ удовлетворяет условиям $(*)$ и $(**)$. Пусть сначала $p \neq 2$. Тогда $m > q^3$ и, значит, $p^3 \in \omega(S) \setminus \omega(L)$; противоречие. Если $p = 2$, то 2-период группы L равен 8. Чтобы прийти к противоречию нам достаточно показать, что $m > 17$. При $q > 2$ имеем $m \geq \min\{k_5(\varepsilon q), k_7(\varepsilon q), k_8(\varepsilon q) \mid$

$q = 2^m > 2\} > 4^3/2 > 17$, что и требовалось. Осталось рассмотреть случай, когда $q = 2$. Заметим, что в силу леммы 2.2 примитивные делители $r_7(\varepsilon 2)$ и $r_8(\varepsilon 2)$ не смежны с 2 в графе $GK(L)$. Поэтому числа $k_7(\varepsilon 2)$ и $k_8(\varepsilon 2)$ содержатся в $\omega(S)$ и каждое из них является простым числом, лежащим между $m-3$ и m. В частности, $m \geq 43$; противоречие.

Пусть $n = 5, 7$. Тогда, как следует из [15, табл. 1a], граф простых чисел группы L имеет две компоненты связности и $n_2(L) = k_n(\varepsilon q)$. По лемме 1.3 граф $GK(S)$ тоже несвязен и $n_2(L) = n_j(S)$ для некоторого $j > 1$. Значит, $n_2(L)$ — простое число и $m - 2 \leq n_2(L) \leq m$. В частности, $m \geq k_5(\varepsilon q)$. Повторяя рассуждения предыдущего абзаца, получаем противоречие во всех случаях, когда $q > 2$. Группа $L_5(2)$ исключается, так как лежит в $\mathscr{L}$. Рассмотрим группу $L = U_5(2)$. Поскольку $k_5(-2) = 11$ лежит в $\omega(S)$, выполняется неравенство $m \geq 11$. Тогда $7 \in \omega(S) \setminus \omega(L)$.

Пусть $n = 6$. Поскольку $L_6^\varepsilon(2) \in \mathscr{L}$, можно считать, что $q > 2$. Как следует из лемм 2.2 и 2.3, если $p = 2$ или $\varepsilon q \equiv 1 \pmod 4$, то каждый примитивный делитель $r_5(\varepsilon q)$ не смежен с числом 2 в графе $GK(L)$. Тогда в силу п. 3 леммы 1.4 число $k_5(\varepsilon q)$ взаимно просто с произведением $|K| \cdot |\overline{G}/S|$, а значит, является простым числом, удовлетворяющим неравенствам $m-3 \leq k_5(\varepsilon q) \leq m$, что приводит к противоречию.

Таким образом, $\varepsilon q \equiv 3 \pmod 4$. Кроме того, $L_6^\varepsilon(3) \in \mathscr{L}$, поэтому $q \geq 5$. Теперь $r_6(\varepsilon q)$ не смежно с 2 и $k_6(\varepsilon q)$ — простое число, удовлетворяющее неравенствам $m-3 \leq k_6(\varepsilon q) \leq m$. Тогда $m \geq (q^2 - q + 1)/2 \geq 7$, а значит, силовская 3-подгруппа группы S не является циклической. Применяя лемму 1.5, получаем, что число 3 смежно в $GK(G)$ с любым простым делителем $r \neq 3$ числа $|K|$. Если $(\varepsilon q - 1)_3 \leq 3$, то в силу лемм 2.2 и 2.3 примитивный простой делитель $r_5(\varepsilon q)$ не смежен с 3 в $GK(L)$, следовательно, $k_5(\varepsilon q)$ должно быть простым числом с условием $m - 2 \leq k_5(\varepsilon q) \leq m$; противоречие.

Тем самым $(\varepsilon q - 1)_3 \geq 9$. Отсюда, в частности, вытекает, что $k_6(\varepsilon q) = q^2 - \varepsilon q + 1$. Поэтому $m \geq q^2 - \varepsilon q + 1$. Если $q > p$, то $m > p^3$, что приводит к противоречию, так как $p^3 \notin \omega(L)$. Следовательно, $q = p$, и из условий $(\varepsilon q - 1)_3 \geq 9$ и $\varepsilon q \equiv 3 \pmod 4$ вытекает, что $p \geq 19$. В частности, p-период группы L равен p. Если $L = U_6(p)$, то $m \geq p^2 + p + 1$; противоречие. Пусть $L = L_6(p)$. Тогда $m \geq p^2 - p + 1 > 2p$. Поэтому силовская p-подгруппа группы S не является циклической. Применяя лемму 1.5, получаем, что p смежно в $GK(G)$ с любым простым делителем $r \neq p$ числа $|K|$. Значит, ни один из простых делителей числа $k_5(p)$ не может делить порядок группы K, и, следовательно, $k_5(p) \in \omega(S)$. Поскольку $k_5(p) > p^3$, число $k_5(p)$ не может быть простым. Пусть произведение двух простых чисел r_1 и r_2, не обязательно различных, делит $k_5(p)$. Любой простой делитель числа $k_5(p)$ не смежен с p, поэтому $r_1 > m - p > m/2$ и $r_2 > m - p > m/2$. Тогда $r_1 r_2 > m$ и $r_1 + r_2 > m$, следовательно, в S нет элемента порядка $r_1 r_2$; противоречие.

Пусть, наконец, $n = 4$. Поскольку $L \notin \mathscr{L}$, имеем $p > 2$, $q > 3$ и $(\varepsilon, p) \neq (-, 5)$. По леммам 2.2 и 2.3 хотя бы для одного i из пары чисел $3, 4$ каждый примитивный делитель $r_i(\varepsilon q)$ не смежен с 2 в $GK(L)$. Но тогда число $k_i(\varepsilon q)$ простое и $m \geq k_i(\varepsilon q) \geq m - 3$. Если $q > p$, то $m \geq \min\{k_3(\varepsilon q), k_4(\varepsilon q)\} > p^3$, что невозможно, так как p-период группы L не превосходит p^2.

Таким образом, $q = p > 3$, и p-период группы L равен p. Отметим, что $k_4(\varepsilon p) = (p^2 + 1)/2 > 2p$, и так как $(\varepsilon, p) \neq (-, 5)$, то $k_3(\varepsilon p) = (p^2 + \varepsilon p + 1)/(3, \varepsilon p - 1) > 2p$. Поэтому $m > 2p$ и силовская p-подгруппа группы S не является циклической. Следовательно, оба числа $k_3(\varepsilon p)$ и $k_4(\varepsilon p)$ взаимно просты с порядком группы K и лежат в спектре группы S. Повторяя рассуждения из предыдущего абзаца, получаем, что оба этих числа должны быть простыми числами, большими $m-p$ и меньшими m. Если $\varepsilon=+$ и $p\equiv -1 \pmod 3$, то $m\geq p^2+p+1$ и $p^2\in\omega(S)$; противоречие. Если $\varepsilon=-$ и $p\equiv 1 \pmod 3$, то $m\geq p^2-p+1>p+(p^2+1)/2$, что противоречит неравенству $k_4(\varepsilon p)>m-p$. В оставшихся случаях для всех групп, кроме $L=L_4(7)$, выполнено $k_3(\varepsilon p)=(p^2+\varepsilon p+1)/3<(p^2+1)/2-p\leq m-p$, что невозможно. Осталось заметить, что для $L=L_4(7)$ число $k_4(\varepsilon p)=25$ не является простым.

Теорема 1 доказана.

§ 4. Доказательство теоремы 2

Лемма 4.1. *Если $3\leq i\leq 20$, q — степень простого числа, $k_i(q)$ содержится в спектре какой-нибудь спорадической группы или группы Титса ${}^2F_4(2)'$, то тройка $(i,q,k_i(q))$ указана в табл. 1.*

Таблица 1

$q\diagdown i$	3	4	5	6	8	10	12	14	18	20
2	7	5	31	1	17	11	13	43	19	41
3	13	5		7	41					
4	7	17		13		41				
5	31	13		7						
7	19	25		43						
8				19						
9		41								
11				37						

Доказательство. Используя формулу (1), несложно показать, что $k_i(q)\geq(q^2-q+1)/3$ при $i\geq 3$. Согласно [3] порядки элементов спорадических групп не превосходят 119. Значит, $(q^2-q+1)/3\leq 119$, откуда $q\leq 19$. Теперь непосредственные вычисления показывают справедливость леммы.

Пусть $L=L_n^\varepsilon(q)$, где $n\geq 4$, $\varepsilon\in\{+,-\}$ и q — степень простого числа p, и $L\notin\mathscr{L}$. Пусть G — конечная группа, изоспектральная L, и K — разрешимый радикал группы G. По лемме 1.4 имеем $S\leq\overline{G}=G/K\leq\mathrm{Aut}(S)$, где S — неабелева простая группа. Теорема 2 будет вытекать из двух следующих предложений.

Предложение 4.1. *Пусть $L=L_4^\varepsilon(q)$. Тогда S не является ни спорадической группой, ни группой Титса.*

Доказательство. Предположим противное. Группы $L_4^\varepsilon(2^m)$, $L_4(3)$, $U_4(5)$ лежат в $\mathscr{L}$, поэтому q нечетно, больше 3, а также не равно 5 в унитарном случае. По лемме 2.3 все простые делители хотя бы одного из чисел $k_4(\varepsilon q)$ и $k_3(\varepsilon q)$ не смежны с 2 в $GK(L)$, поэтому в силу леммы 1.4 хотя бы одно из этих чисел лежит в $\omega(S)$. Следовательно, $q\leq 11$ по лемме 4.1.

Пусть $q = 11$. Тогда $k_3(\varepsilon 11) \in \omega(S)$. Из леммы 4.1 следует, что $L = U_4(11)$ и $37 \in \omega(S)$. Следовательно, S изоморфна одной из спорадических групп Ly и J_4. В первом случае $67 \in \omega(S) \setminus \omega(L)$, во втором — $43 \in \omega(S) \setminus \omega(L)$; противоречие.

Пусть $q = 9$. Если $L \neq L_4(9)$, то $k_3(\varepsilon 9) \in \omega(S)$, что противоречит лемме 4.1. Если же $L = L_4(9)$, то $41 = r_4(9) \in \omega(S)$. Значит, $S = F_1$ и $47 \in \omega(S) \setminus \omega(L)$; противоречие.

Пусть $q = 7$. Если $\varepsilon = +$, то $\pi(S) \subseteq \pi(L_4(7)) = \{2, 3, 5, 7, 19\}$ и $19 = r_3(7) \in \omega(S)$. Легко убедиться, используя [3], что это невозможно. В случае унитарных групп $\pi(U_4(7)) = \{2, 3, 5, 7, 43\}$, поэтому $S = J_2$. С другой стороны, $5 = r_4(7)$ не смежно с 2 в $GK(L)$, однако $10 \in \omega(J_2)$; противоречие.

Пусть $q = 5$. Тогда $\pi(S) \subseteq \pi(L_4(5)) = \{2, 3, 5, 13, 31\}$, поэтому $S = {}^2F_4(2)'$. С другой стороны, $31 = r_3(5) \in \omega(S)$, однако $31 \notin \omega({}^2F_4(2)')$; противоречие. Предложение доказано.

Предложение 4.2. *Пусть $L = L_n^\varepsilon(q)$, где $n \geq 5$, и S — спорадическая группа или группа Титса. Тогда $L = U_5(2)$ и $S \simeq M_{11}$.*

Доказательство. Заметим, что при $n \neq 6, 10$ в полуинтервале $(n/2, n]$ есть два различных простых числа i и j. В зависимости от четности числа n либо $\{r_i(\varepsilon q), r_j(\varepsilon q), r_n(\varepsilon q)\}$, либо $\{r_i(\varepsilon q), r_j(\varepsilon q), r_{n-1}(\varepsilon q)\}$ — коклика размера 3 в $GK(L)$, поэтому по лемме 1.4 хотя бы одно из чисел $k_i(\varepsilon q)$ и $k_j(\varepsilon q)$ лежит в $\omega(S)$. Значит, найдется простое число i такое, что $i > n/2$ и $k_i(\varepsilon q) \in \omega(S)$.

Если $n = 6$ или $n = 10$, то по лемме 2.1 в $GK(L)$ есть коклика из трех чисел, содержащая $r_3(\varepsilon q)$, $r_5(\varepsilon q)$ для $n = 6$ и $r_5(\varepsilon q)$, $r_7(\varepsilon q)$ для $n = 10$. Значит, в этих случаях найдется простое число i такое, что $i \geq n/2$ и $k_i(\varepsilon q) \in \omega(S)$.

Предположим, что $q \neq 2$.

Пусть $i \geq 7$. Применяя лемму 1.2, получаем, что $k_i(\varepsilon q) > q^{i-2} \geq q^5 \geq 3^5 = 243 > 119$; противоречие.

Пусть $i = 5$. Тогда $k_i(\varepsilon q) > q^{i-2} \geq q^5 \geq 5^3 = 125 > 119$ при $q \geq 5$, поэтому $q = 3$ или $q = 4$. Кроме того, $n \leq 2i = 10$. Из леммы 4.1 находим, что $q = 4$, $\varepsilon = -$ и $41 = k_5(-4) \in \omega(S)$, поэтому $S \simeq F_1$. Если $n \leq 10$, то, как несложно проверить, $31 \in \omega(S) \setminus \omega(L)$. Если $n = 10$, то $109 = r_9(-4)$ не смежно с 2 в $GK(L)$, но не делит порядок группы S.

Пусть $i = 3$ и $L = U_n(q)$. Тогда $q \leq 11$, $q \neq 9$ по лемме 4.1 и, кроме того, $n \leq 2i = 6$. Если $n = 5$, то из лемм 2.3 и 1.4 следует, что $k_5(-q) \in \omega(S)$. Тогда $q = 4$, $k_5(-4) = 41$, поэтому $S \simeq F_1$ и $31 \in \omega(S) \setminus \omega(L)$; противоречие. Значит, $n = 6$. При $q = 11$ из лемм 2.3 и 1.4 получаем, что $k_6(-11) \in \omega(S)$; это противоречит лемме 4.1. Таким образом, $q \leq 7$.

Если $q = 7$, тогда $k_i(q) = k_3(-7) = 43$, поэтому $S \simeq J_4$. В этом случае $37 \in \omega(S) \setminus \omega(L)$; противоречие.

Пусть $q = 5$. Из лемм 2.3 и 1.4 получаем, что $521 = r_5(-5) \in \omega(S)$; противоречие.

Предположим теперь, что $q = 4$. Из лемм 2.2 и 1.4 вытекает, что $41 = r_5(-4) \in \omega(S)$, поэтому $S \simeq F_1$, но тогда $47 \in \omega(S) \setminus \omega(L)$; противоречие.

Значит, $q = 3$. Учитывая, что $\pi(U_6(3)) = \{2, 3, 5, 7, 13, 61\}$, получаем $S \simeq {}^2F_4(2)'$ или $S \simeq J_2$. Пусть $S \simeq {}^2F_4(2)'$. Поскольку $61, 91 \in \omega(G) \setminus \omega(S)$, то 61 и еще хотя бы одно их чисел 7 и 13, обозначим его через r, обязаны лежать в $\omega(K)$. Пусть T — прообраз силовской 5-подгруппы из G/K в G. Тогда T разрешима, следовательно, по теореме Холла имеет холлову $\{5, r, 61\}$-подгруппу H. Числа $5, r, 61$ образуют коклику в графе $GK(G)$, а значит, и в $GK(H)$, что противоречит разрешимости группы H в силу [17, лемма 1.1]. Случай $S \simeq J_2$ рассматривается аналогично, отличие лишь в том, что r в точности равно 13.

Пусть теперь $i = 3$ и $L = L_n(q)$. Тогда $5 \leq n \leq 6$ и $q \leq 7$ по лемме 4.1.

Если $q = 7$, то из лемм 2.3 и 1.4 вытекает, что $k_5(7) \in \omega(S)$; противоречие. Если $q = 5$ и $L = L_5(5)$, то $k_5(5) \in \omega(S)$; противоречие. Если $L = L_6(5)$, то $31 = k_3(5) \in \omega(S)$. Как несложно проверить, используя [3], если 31 делит порядок спорадической группы, то одно из чисел 19 или 37 тоже делит этот порядок, но 19 и 37 не принадлежат $\omega(L_6(5))$; противоречие. Значит, $q = 3$, и из лемм 2.3 и 1.4 вытекает, что $121 = k_5(3) \in \omega(S)$; противоречие.

Осталось рассмотреть случай, когда $q = 2$. Поскольку $L \notin \mathscr{L}$, можно считать, что $L = U_n(2)$ и $n \neq 6$. Если $n \geq 13$, то $i \geq 11$, поэтому $k_i(-2) > 2^9/2 > 119$; противоречие. При $n = 11$, 12 из лемм 2.2 и 1.4 получаем, что $683 = r_{11}(-2) \in \omega(S)$; противоречие. Аналогичным образом при $n = 7, 8$ получаем, что $43 = r_7(-2) \in \omega(G)$, поэтому $S \simeq J_4$, следовательно, $37 \in \omega(G)$; противоречие. Пусть $n = 9, 10$. Из предыдущего рассуждения следует, что $r_7(-2) \notin \omega(S)$, поэтому из п. 2 леммы 1.4 вытекает, что числа $r_5(-2) = 11$, $r_8(-2) = 17$, $r_9(-2) = 19$ лежат в $\omega(S)$. Кроме того, все простые делители порядка S не превосходят 31. Легко проверить, используя [3], что спорадических групп с таким свойствами нет. Значит, $n = 5$. Поскольку $\pi(U_5(2)) = \{2, 3, 5, 11\}$, то S может быть изоморфна только M_{11} или M_{12}. Заметим, что $10 \in \omega(M_{12}) \setminus \omega(U_5(2))$, поэтому $S \simeq M_{11}$.

Предложение и теорема 2 доказаны.

§ 5. Доказательство теоремы 3

Пусть $L = L_n^\varepsilon(q)$, где $n \geq 4$, $\varepsilon \in \{+, -\}$ и $q = p^\alpha$. Пусть G — конечная группа, изоспектральная L, и K — разрешимый радикал группы G. Применяя лемму 1.4 в условиях теоремы 3, получаем, что $S \leq \overline{G} = G/K \leq \operatorname{Aut}(S)$, где S — группа лиева типа над полем характеристики p.

Лемма 5.1. *Если L — одна из групп $U_6(4)$, $U_7(2)$ и $U_7(4)$, то заключение теоремы 3 верно для L.*

Доказательство. Пусть $L = U_6(4)$. Тогда по лемме 2.2 числа $r_6(-4) = 7$ и $r_5(-4) = 41$ не смежны с 2 в $GK(L)$, следовательно, они лежат в $\pi(S)$. Таким образом, $7, 41 \in \pi(S) \subseteq \pi(L) = \{2, 3, 5, 7, 13, 17, 41\}$. В [26, табл. 1] указано множество простых групп, максимальный простой делитель порядка которых равен 41. В этом множестве содержится пять групп лиева типа над полем характеристики 2, но из них только группа $U_6(4)$ содержит 7 в своем спектре.

Если $L = U_7(2)$, то $r_7(-2) = 43$ не смежно с 2 в $GK(L)$. Рассматривая множество простых групп, удовлетворяющих условию $43 \in \pi(S) \subseteq [2; 43]$ из [26, табл. 1], убеждаемся, что оно содержит пять групп лиева типа над полем характеристики 2, но из них только группа $U_7(2)$ не содержит 17 в своем спектре.

Если $L = U_7(4)$, то $r_7(-4) = 113$ не смежно с 2 в $GK(L)$. В [26, табл. 1] указано, что единственная простая группа лиева типа над полем характеристики 2, удовлетворяющая условию $113 \in \pi(S) \subseteq [2; 113]$, — это группа $U_7(4)$.

В любом из рассмотренных случаев $S \simeq L$. Лемма доказана.

Таким образом, можно считать, что L отлична не только от групп из $\mathscr{L}$, но и от $U_6(4)$, $U_7(2)$, $U_7(4)$, в частности, p нечетно, если $\varepsilon = +$ или $n = 4$. Выберем в $\pi(L)$ два простых числа следующим образом. Если $\varepsilon = +$, положим $r_n = r_{n\alpha}(p)$ и $r_{n-1} = r_{(n-1)\alpha}(p)$. Если $\varepsilon = -$, положим $r_n = r_{\nu(n)\alpha}(p)$ и $r_{n-1} = r_{\nu(n-1)\alpha}(p)$, где функция $\nu(x)$ определена в (3). Отметим, что эти примитивные делители существуют в силу ограничений на L и больше 3, так как $n \geq 4$. Применяя формулы (4) и (5), получаем равенства $e(r_n, \varepsilon q) = n$ и $e(r_{n-1}, \varepsilon q) = n-1$. Следовательно, r_n и r_{n-1} не смежны с p в $GK(L)$ по лемме 2.2.

Лемма 5.2. *Группа S не изоморфна $L_2(p)$.*

Доказательство. Предположим, что $S \simeq L_2(p)$. По лемме 2.3 одно из чисел r_n и r_{n-1} не смежно с 2 в $GK(L)$ и, значит, лежит в $\pi(S)$ по лемме 1.4. С другой стороны, каждое из чисел $n\alpha$, $(n-1)\alpha$, $\nu(n)\alpha$, $\nu(n-1)\alpha$ больше 3, а $\pi(S)$ состоит из p и делителей p^2-1; противоречие с определением примитивного делителя. Лемма доказана.

Лемма 5.3. *Если $r \in \pi(L)$ не смежно с p в $GK(L)$, то оно не делит $|K| \cdot |\overline{G}/S|$; в частности, $t(p,S) \geq t(p,L)$.*

Доказательство. Пусть $r \in \pi(L)$, $rp \notin \pi(L)$ и $r \notin \pi(S)$. В силу леммы 1.4 можно считать, что p нечетно. Из леммы 2.2 и условия $n \geq 4$ следует, что $r > 3$.

Предположим, что $r \in \pi(\overline{G}/S)$. Поскольку $r \notin \pi(S)$ и $r > 3$, группа G содержит полевой автоморфизм группы S порядка r. Поскольку в любой группе лиева типа над полем характеристики p централизатор полевого автоморфизма содержит элемент порядка p, получаем, что $rp \in \omega(G)$; противоречие.

Предположим, что $r \in \pi(K)$. По лемме 5.2 группа S отлична от $L_2(p)$, поэтому ее силовская p-подгруппа содержит элементарную абелеву подгруппу порядка p^2. По лемме 1.5 группа G содержит элемент порядка pr; противоречие. Лемма доказана.

Пусть S — группа над полем порядка p^β (в обозначениях из [3]). Обозначим через $e(p,S)$ множество $\{e(r,p^\beta) \mid r \in \pi(S), r \neq p, r > 3, pr \notin \omega(S)\}$. По лемме 5.3 числа r_n и r_{n-1} лежат в $\pi(S)$ и не смежны с p в $GK(S)$, поэтому $e(r_n, p^\beta)$ и $e(r_{n-1}, p^\beta)$ лежат в $e(p,S)$.

Положим $e_n = e(r_n, p^\beta)$ и $e_{n-1} = e(r_{n-1}, p^\beta)$. Поскольку $r_n \in \pi(S)$, число $k_{e_n}(p^\beta)$ делит порядок группы S. Если примитивный делитель $r_{e_n\beta}(p)$ существует, то он делит $k_{e_n}(p^\beta)$, значит, лежит в $\pi(S) \subseteq \pi(L)$. По тем же соображениям если $r_{e_{n-1}\beta}(p)$ существует, то он также лежит в $\pi(L)$.

Пусть $\varepsilon = +$. По определению примитивного делителя $e_{n-1}\beta = a(n-1)\alpha$ для некоторого натурального a. Поскольку $e_{n-1}\beta \geq 3$ и p нечетно, примитивный делитель $r_{e_{n-1}\beta}(p)$ существует и, значит, лежит в $\pi(L)$. Тогда $e(r_{e_{n-1}\beta}(p), q) \leq n$ в силу формулы (2). С другой стороны, $e(r_{e_{n-1}\beta}(p), q) = e(r_{a(n-1)\alpha}(p), p^\alpha) = a(n-1)$. Таким образом, $a(n-1) \leq n$, откуда $a = 1$ и $e_{n-1}\beta = (n-1)\alpha$. По тем же соображениям $e_n\beta = n\alpha$. В частности, $e_n/e_{n-1} = n/(n-1)$.

Пусть теперь $\varepsilon = -$. Тогда $e_n\beta = a\nu(n)\alpha$ и $e_{n-1}\beta = b\nu(n-1)\alpha$ для некоторых натуральных a и b. В силу ограничений на L примитивные делители $r_{e_n\beta}(p)$ и $r_{e_{n-1}\beta}(p)$ существуют и лежат в $\pi(S) \subseteq \pi(L)$. По формуле (2) это означает, что числа $e(r_{e_n\beta}(p), -q)$ и $e(r_{e_{n-1}\beta}(p), -q)$ не превосходят n. С другой стороны, $e(r_{e_n\beta}(p), -q) = \nu(e(r_{e_n\beta}(p), p^\alpha)) = \nu(a\nu(n))$ и $e(r_{e_{n-1}\beta}(p), -q) = \nu(e(r_{e_{n-1}\beta}(p), p^\alpha)) = \nu(b\nu(n-1))$ по (5). Следовательно, $\nu(a\nu(n)) \leq n$ и $\nu(b\nu(n-1)) \leq n$. Рассматривая эти неравенства в зависимости от остатка числа n по модулю 4, получаем, что $a \leq 2$ при $n \equiv 2 \pmod 4$ и $a = 1$ в остальных случаях, $b \leq 2$ при $n \equiv 3 \pmod 4$ и $b = 1$ в остальных случаях. В частности, $e_n/e_{n-1} = a\nu(n)/b\nu(n-1)$, где $a, b \in \{1, 2\}$, $n/4(n-1) \leq e_n/e_{n-1} \leq 4n/(n-1)$ и $e_n/e_{n-1} \neq n/(n-1)$.

Таким образом, при любом значении ε в $e(p,S)$ должны быть два числа e_n и e_{n-1} такие, что отношение e_n/e_{n-1} лежит в множестве

$$R_n = \{2^\gamma n/(n-1) \mid \gamma = -2,-1,0,1,2\},$$

причем $\gamma = 0$ тогда и только тогда, когда $\varepsilon = +$.

Лемма 5.4. *Пусть $n \geq 4$, $m \geq 2$ — натуральные числа и δ — целое число. Если $2^\delta n/(n-1) = m/(m-1)$, то $m = n$ и $\delta = 0$. Если $2^\delta n/(n-1) = (m-1)/m$, то $n = 4$, $m = 3$ и $\delta = -1$.*

Доказательство. Если $\delta < 0$, то $2^\delta n/(n-1) \leq n/(2n-2) < 1 < m/(m-1)$. Если $\delta > 0$, то $2^\delta n/(n-1) \geq 2n/(n-1) > 2 \geq m/(m-1)$. Таким образом, из равенства $2^\delta n/(n-1) = m/(m-1)$ следует, что $\delta = 0$ и тогда $n = m$.

Если $\delta < -1$, то $2^\delta n/(n-1) \leq n/(4n-4) < 1/2 \leq (m-1)/m$. Если $\delta > -1$, то $2^\delta n/(n-1) \geq n/(n-1) > 1 > m-1/m$. Значит, из равенства $2^\delta n/(n-1) = (m-1)/m$ следует, что $\delta = -1$ и $n/(2n-2) = (m-1)/m$. Если n нечетно, то в обеих частях последнего равенства стоят несократимые дроби, поэтому $2n-2-n = 1$, откуда $n = 3$, но это не так. Если n четно, то несократимой дробью будет $(n/2)/(n-1)$, следовательно, $n-1-n/2 = 1$, откуда $n = 4$ и $m = 3$. Лемма доказана.

В качестве следствия леммы 5.4 отметим, что в R_n нет чисел вида 2^δ и $2^\delta(m-1)/m$, где δ — целое число и $m \geq 4$.

Далее последовательно рассматриваются все группы лиева типа. Для нахождения множества $e(p,S)$ используются результаты из [20, § 3].

Предположим, что $S \simeq L_m(p^\beta)$, где $m \geq 3$ или $\beta > 1$. Тогда $e(p,S) = \{m, m-1\}$. Следовательно, $e_n/e_{n-1} = m/(m-1)$ или $e_n/e_{n-1} = (m-1)/m$. Пусть $2^\gamma n/(n-1) = m/(m-1)$. По лемме 5.4 получаем, что $n = m$ и $\gamma = 0$, откуда $\varepsilon = +$. Значит, $S \simeq L$. Пусть $2^\gamma n/(n-1) = (m-1)/m$. Тогда $n = 4$, $m = 3$ и $\gamma = -1$, откуда $\varepsilon = -$ и $a = 1$. Теперь из уравнений $(m-1)\beta = e_n\beta = \nu(n)\alpha = 4\alpha$ следует, что $\beta = 2\alpha$. Значит, $L = U_4(q)$, $S \simeq L_3(q^2)$ и $r_3(q) \in \pi(S) \setminus \pi(L)$; противоречие.

Предположим, что $S \simeq U_m(p^\beta)$, где $m \geq 3$. Тогда $e(p,S) = \{\nu(m), \nu(m-1)\}$. Пусть $2^\gamma n/(n-1) = \nu(m)/\nu(m-1)$. По лемме 5.4 получаем, что $n = m$ и $\gamma \neq 0$, откуда $\varepsilon = -$. Значит, $S \simeq L$. Пусть $2^\gamma n/(n-1) = \nu(m-1)/\nu(m)$. Тогда $m = 3$, откуда $\nu(m-1)/\nu(m) = (m-1)/4m$ и, значит, $\gamma + 2 = -1$; противоречие с тем, что $\gamma \geq -2$.

Предположим, что $S \simeq O_{2m+1}(p^\beta)$ или $S \simeq S_{2m}(p^\beta)$. Тогда $e(p,S) \subseteq \{m, 2m\}$. Таким образом, отношение любых элементов из $e(p,S)$ является степенью числа 2 и не может лежать в R_n; противоречие. По аналогичным соображениям S отлична от групп типов G_2, ${}^3D_4$, ${}^2F_4$ и ${}^2B_2$, поскольку в противном случае $e(p,S)$ совпало бы с одним из множеств $\{3,6\}$, $\{12\}$, $\{6,12\}$ и $\{1,4\}$.

Предположим, что $S \simeq O^+_{2m}(p^\beta)$, где $m \geq 4$. Тогда $e(p,S) = \{2m-2, m-1\}$ при четном m и $e(p,S) = \{2m-2, m\}$ при нечетном m. Отношение e_n/e_{n-1} не может быть равно ни $2(m-1)/m$, ни степени числа 2, поэтому m нечетно и $2^\gamma n/(n-1) = m/(2m-2)$. Тогда $n = m$ и $\gamma = -2$, откуда n нечетно и $\varepsilon = -$. Следовательно, $e_n/e_{n-1} = \nu(n)/b\nu(n-1) = 2n/b\nu(n-1) \geq 2n/(n-1)$ и γ должно быть положительным; противоречие.

Предположим, что $S \simeq O^-_{2m}(p^\beta)$, где $m \geq 4$. Тогда $e(p,S) = \{2m, 2m-2, m-1\}$ при четном m и $e(p,S) = \{2m, 2m-2\}$ при нечетном m. Отношение e_n/e_{n-1} не может быть степенью числа 2 и не может равняться $(m-1)/2m$

или $(m-1)/m$, значит, e_n/e_{n-1} равно одному из чисел $2m/(m-1)$, $m/(m-1)$. Пусть m четно и $2^\gamma n/(n-1) = 2m/(m-1)$. Тогда $n = m$ и $\gamma = 1$, откуда $\varepsilon = -$. Следовательно, n четно и $e_n/e_{n-1} = a\nu(n)/\nu(n-1) = a\nu(n)/2(n-1) \le n/2(n-1)$, поэтому γ должно быть отрицательным; противоречие.

Пусть $2^\gamma n/(n-1) = m/(m-1)$. Тогда $n = m$ и $\gamma = 0$, откуда $\varepsilon = +$. Теперь из уравнений $2m\beta = e_n\beta = n\alpha$, следует, что $\alpha = 2\beta$. Следовательно, $L = L_n(q_0^2)$ и $S \simeq O_{2n}^-(q_0)$, где $q_0^2 = q$. Если n нечетно, то $e\big(r_n(q_0), q_0^2\big) = n$, поэтому по лемме 2.2 число $r_n(q_0)$ не смежно с p в $GK(L)$ и, значит, по лемме 5.3 должно делить порядок группы S, но это неверно. Если n четно, то оба числа $r_{2(n-1)}(q_0)$ и $r_{n-1}(q_0)$ не смежны с p в $GK(L)$, поэтому по лемме 5.3 взаимно просты с $|K| \cdot |\overline{G}/S|$. Это противоречит тому, что в L есть элемент порядка $r_{2(n-1)}(q_0)r_{n-1}(q_0)$, а в группе S нет.

Предположим, что $S \simeq E_8(p^\beta)$. Тогда $e(p,S) = \{30, 24, 20, 15\}$. Отношение e_n/e_{n-1} не является степенью числа 2 и числом вида $2^\delta(m-1)/m$ для $m \ge 4$, поэтому $e_n/e_{n-1} \in \{2/3, 4/3, 5/4, 6/5, 5/8\}$. Если $2^\gamma n/(n-1) = 5/8$, то $n = 5$ и $\gamma = -1$, откуда $\varepsilon = -$. Следовательно, $e_n/e_{n-1} = \nu(n)/\nu(n-1) = 2n/(n-1)$ и $\gamma = 1$; противоречие.

Пусть $2^\gamma n/(n-1) = 2/3$ или $2^\gamma n/(n-1) = 4/3 = 2 \cdot 2/3$. Тогда $n = 4$. Если $\varepsilon = +$, то $e_n/e_{n-1} = 4/3$ и из уравнений $20\beta = e_n\beta = 4\alpha$ следует, что $\alpha = 5\beta$, поэтому $L = L_4\big(q_0^5\big)$ и $S \simeq E_8(q_0)$, где $q_0^5 = q$. Если $\varepsilon = -$, то $e_n/e_{n-1} = \nu(n)/\nu(n-1) = 2/3$ и из уравнений $20\beta = e_n\beta = 4\alpha$ следует, что $\alpha = 5\beta$, поэтому $L = U_4\big(q_0^5\big)$ и $S \simeq E_8(q_0)$, где $q_0^5 = q$. Аналогичным образом если $e_n/e_{n-1} = 5/4$, то $L = L_5\big(q_0^6\big)$ и $S \simeq E_8(q_0)$, где $q_0^6 = q$, а если $2^\gamma n/(n-1) = 6/5$, то $L = L_6\big(q_0^4\big)$ и $S \simeq E_8(q_0)$, где $q_0^4 = q$. В любом из этих случаев $r_{14}(q_0) \in \pi(S) \setminus \pi(L)$.

Предположим, что $S \simeq E_7(p^\beta)$. Тогда $e(p,S) = \{18, 14, 9, 7\}$. Отношение e_n/e_{n-1} не является степенью числа 2, поэтому

$$e_n/e_{n-1} \in \{2^\delta \cdot 9/7, 2^\delta \cdot 7/9 \mid \delta = -1, 0, 1\}.$$

Пусть $2^\gamma n/(n-1) = 2^\delta \cdot 9/7$. Тогда $2^\gamma \cdot 7n = 2^\delta \cdot 9(n-1)$. Если $\gamma \ge \delta$, то $n = 9$ и $2^\gamma \cdot 7 = 2^\delta \cdot 8$, что невозможно. Если $\gamma \le \delta$, то $n - 1 = 7$ и $2^\gamma \cdot 8 = 2^\delta \cdot 9$, что тоже невозможно. Пусть $2^\gamma n/(n-1) = 2^\delta \cdot 7/9$. Тогда $\gamma \le \delta$, откуда $n - 1 = 9$ и $2^\gamma \cdot 10 = 2^\delta \cdot 7$; снова получено противоречие.

Предположим, что $S \simeq E_6(p^\beta)$ или $S \simeq F_4(p^\beta)$. Тогда $\{12, 8\} \subseteq e(p,S) \subseteq \{12, 9, 8\}$. Значит, $e_n/e_{n-1} \in \{9/8, 2/3, 4/3\}$. Пусть $2^\gamma n/(n-1) = 9/8$. Тогда $n = 9$ и $\gamma = 0$, откуда $\varepsilon = +$. Из уравнений $9\beta = e_n\beta = 9\alpha$ получаем, что $\beta = \alpha$, значит, $L = L_9(q)$, $S \simeq E_6(q)$ и $r_{12}(q) \in \pi(S) \setminus \pi(L)$; противоречие.

Пусть $2^\gamma n/(n-1) = 2/3$ или $2^\gamma n/(n-1) = 4/3$. Тогда $n = 4$. Если $\varepsilon = +$, то $e_n/e_{n-1} = 4/3$, значит, S имеет тип E_6. Из уравнений $12\beta = e_n\beta = 4\alpha$ следует, что $\alpha = 3\beta$, поэтому $L = L_4\big(q_0^3\big)$ и $S \simeq E_6(q_0)$, где $q_0^3 = q$. В этом случае $r_8(q_0) \in \pi(S) \setminus \pi(L)$. Если $\varepsilon = -$, то $e_n/e_{n-1} = \nu(n)/\nu(n-1) = 2/3$ и из уравнений $8\beta = e_n\beta = 4\alpha$ следует, что $\alpha = 2\beta$. Значит, $L = U_4\big(q_0^2\big)$ и S изоморфна $E_6(q_0)$ или $F_4(q_0)$, где $q_0^2 = q$, но тогда $r_6(q_0) \in \pi(S) \setminus \pi(L)$.

Предположим, что $S \simeq {}^2E_6(p^\beta)$. Тогда $e(p,S) = \{18, 12, 8\}$ и $e_n/e_{n-1} \in \{2/3, 9/4\}$. Пусть $2^\gamma n/(n-1) = 2/3$. Тогда $n = 4$ и $\varepsilon = -$. Если $e_n = 12$, то $\alpha = 3\beta$ и $L = U_4\big(q_0^3\big)$, $S \simeq {}^2E_6(q_0)$, где $q_0^3 = q$. Если $e_n = 8$, то $\alpha = 2\beta$, поэтому $L = U_4\big(q_0^2\big)$ и $S \simeq {}^2E_6(q_0)$, где $q_0^2 = q$. В любом случае $r_{10}(q_0) \in \pi(S) \setminus \pi(L)$. Пусть $2^\gamma n/(n-1) = 9/4$. Тогда $n = 9$ и $\gamma = -1$, откуда $\varepsilon = -$. Из уравнений $18\beta = e_n\beta = \nu(n)\alpha = 18\alpha$ получаем, что $\alpha = \beta$, поэтому $L = U_9(q)$ и $S \simeq {}^2E_6(q)$. В этом случае $r_{12}(q) \in \pi(S) \setminus \pi(L)$.

Предположим, что $S \simeq {}^2G_2(3^\beta)$, где $\beta \geq 3$ нечетно. Тогда $e(3,S) = \{6,2,1\}$. Поскольку $6 = 8 \cdot 3/4$ и $3 = 4 \cdot 3/4$, отношение e_n/e_{n-1} может быть равно 1/6 или 1/3. Значит, $2^\gamma n/(n-1) = 1/6 = 1/8 \cdot 4/3 = 1/4 \cdot 2/3$ или $2^\gamma n/(n-1) = 1/3 = 1/4 \cdot 4/3 = 1/2 \cdot 2/3$, откуда $n = 4$ и $\gamma < 0$. Следовательно, $\varepsilon = -$. Тогда $e_n/e_{n-1} = \nu(n)/\nu(n-1) = 2/3$; противоречие.

Теорема 3 доказана.

ЛИТЕРАТУРА

1. *Мазуров В. Д.* Группы с заданным спектром // Изв. Уральск. гос. ун-та. Сер. математика и механика. 2005. № 36, вып. 7. С. 119–138.
2. *Grechkoseeva M. A., Shi W. J., Vasilev A. V.* Recognition by spectrum of finite simple groups of Lie type // Front. Math. China. 2008. V. 3, N 2. P. 275–285.
3. *Conway J. H, Curtis R. T., Norton S. P., Parker R. A., Wilson R. A.* Atlas of finite groups. Oxford: Clarendon Press, 1985.
4. *Shi W.* A characteristic property of J_1 and $PSL_2(2^n)$ (in Chinese) // Adv. Math. 1987. V. 16. P. 397–401.
5. *Brandl R., Shi W.* The characterization of $PSL(2,q)$ by its element orders // J. Algebra. 1994. V. 163, N 1. P. 109–114.
6. *Мазуров В. Д., Су М. Ч., Чао Х. П.* Распознавание конечных простых групп $L_3(2^m)$ и $U_3(2^m)$ по порядкам их элементов // Алгебра и логика. 2000. Т. 39, № 5. С. 567–585.
7. *Zavarnitsine A. V.* Recognition of the simple groups $L_3(q)$ by element orders // J. Group Theory. 2004. V. 7, N 1. P. 81–97.
8. *Заварницин А. В.* Веса неприводимых $SL_3(q)$-модулей в характеристике определения // Сиб. мат. журн. 2004. Т. 45, № 2. С. 319–328.
9. *Заварницин А. В.* Распознавание простых групп $U_3(q)$ по порядкам элементов // Алгебра и логика. 2006. Т. 45, № 2. С. 185–202.
10. *Васильев А. В., Гречкосеева М. А., Мазуров В. Д.* О конечных группах, изоспектральных простым симплектическим и ортогональным группам // Сиб. мат. журн. 2009. Т. 50, № 6. С. 1225–1247.
11. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. V. 3. P. 265–284.
12. *Roitman M.* On Zsigmondy primes // Proc. Amer. Math. Soc. 1997. V. 125, N 7. P. 1913–1919.
13. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.
14. *Кондратьев А. С.* О компонентах графа простых чисел конечных простых групп // Мат. сб. 1989. Т. 180, № 6. С. 787–797.
15. *Мазуров В. Д.* Распознавание конечных простых групп $S_4(q)$ по порядкам их элементов // Алгебра и логика. 2002. Т. 41, № 2. С. 166–198.
16. *Кондратьев А. С., Мазуров В. Д.* Распознавание знакопеременных групп простой степени по порядкам их элементов // Сиб. мат. журн. 2000. Т. 41, № 2. С. 360–371.
17. *Васильев А. В.* О связи между строением конечной группы и свойствами ее графа простых чисел // Сиб. мат. журн. 2005. Т. 46, № 3. С. 511–522.
18. *Васильев А. В., Горшков И. Б.* О распознавании конечных простых групп со связным графом простых чисел // Сиб. мат. журн. 2009. Т. 50, № 2. С. 292–299.
19. *Gorenstein D.* Finite groups. New York, etc.: Harper & Row, 1968.
20. *Васильев А. В., Вдовин Е. П.* Критерий смежности в графе простых чисел конечной простой группы // Алгебра и логика. 2005. Т. 44, № 6. С. 682–725.
21. *Васильев А. В., Гречкосеева М. А.* Распознавание по спектру конечных простых линейных групп малой размерности над полями характеристики 2 // Алгебра и логика. 2008. Т. 47, № 5. С. 558–570.
22. *Мазуров В. Д., Чен Г. Ю.* Распознаваемость по спектру конечных простых групп $L_4(2^m)$ и $U_4(2^m)$ // Алгебра и логика. 2008. Т. 47, № 1. С. 83–93.
23. *Мазуров В. Д.* Распознавание конечных групп по множеству порядков их элементов // Алгебра и логика. 1998. Т. 37, № 6. С. 651–666.
24. *Vasil'ev A. V., Vdovin E. P.* Cocliques of maximal size in the prime graph of a finite simple group. Новосибирск, 2009. 33 с. (Препринт/ РАН. Сиб. отд-ние. Ин-т математики; № 225). См. также http://arxiv.org/abs/0905.1164v1.

25. *Testerman D.* A_1-type overgroups of elements of order p in semisimple algebraic groups and the associated finite groups // J. Algebra. 1995. V. 177, N 1. P. 34–76.

26. *Zavarnitsine A. V.* Finite simple groups with narrow prime spectrum // Sib. Electron. Math. Rep. 2009. V. 6. P. 1–12. (http://semr.math.nsc.ru/v6/p1-12.pdf).

Статья поступила 23 марта 2010 г.

Васильев Андрей Викторович, Гречкосеева Мария Александровна,
Старолетов Алексей Михайлович
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090;
Новосибирский гос. университет, ул. Пирогова, 2, Новосибирск 630090
vasand@math.nsc.ru, grechkoseeva@gmail.com, astaroletov@gmail.com