Сибирский математический журнал
Ноябрь—декабрь, 2009. Том 50, № 6

УДК 512.542

О КОНЕЧНЫХ ГРУППАХ, ИЗОСПЕКТРАЛЬНЫХ ПРОСТЫМ СИМПЛЕКТИЧЕСКИМ И ОРТОГОНАЛЬНЫМ ГРУППАМ

А. В. Васильев,
М. А. Гречкосеева, В. Д. Мазуров

Аннотация. *Спектром конечной группы* называется множество порядков ее элементов. Две группы называются *изоспектральными*, если они имеют одинаковые спектры. Рассматривается класс конечных групп, изоспектральных простым симплектическим и ортогональным группам над полем произвольной положительной характеристики p. Как известно, группа из этого класса имеет единственный неабелев композиционный фактор. Доказано, что этот фактор не может быть изоморфен знакопеременной или спорадической группе. Также рассмотрен случай, когда этот фактор изоморфен группе лиева типа над полем той же характеристики p.

Ключевые слова: конечная группа, спектр группы, простая группа, симплектическая группа, ортогональная группа, композиционные факторы.

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. В более общем смысле группа L — *группа с решенной проблемой распознаваемости по спектру*, если известно число (с точностью до изоморфизма) конечных групп, изоспектральных L. Последние результаты, относящиеся к проблеме распознаваемости по спектру, можно найти в обзоре В. Д. Мазурова [1].

Настоящая работа посвящена изучению проблемы распознаваемости для конечных простых симплектических и ортогональных групп. В данном классе проблема решена для групп $B_2(q)$ [2, 3], $B_3(2)$ [4, 5], $B_3(3)$ [5], $B_{2^m}(2)$ [6, 7], $C_3(3)$ [2], $D_4(2)$ [4, 5], $D_4(3)$ [5], $D_5(2)$ [8], ${}^2D_4(2)$ [5], ${}^2D_p(3)$ [9], ${}^2D_{2^m+1}(2)$ [7], ${}^2D_{2^m+1}(3)$ [10], где $m \geq 2$ и p — простое нечетное число. Кроме того, для нескольких серий симплектических и ортогональных групп доказана квазираспознаваемость по спектру (см. [7, 11, 12]). Конечная неабелева простая группа L называется *квазираспознаваемой по спектру*, если любая конечная группа G со свойством $\omega(G) = \omega(L)$ имеет единственный неабелев композиционный фактор и этот фактор изоморфен L.

Результаты работы дают ограничения на композиционное строение конечной группы, изоспектральной простой симплектической или ортогональной группе.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 08–01–00322), Совета по грантам президента РФ (коды проектов НШ–344.2008.1 и МК–377.2008.1) и АВЦП Рособразования «Развитие научного потенциала высшей школы» (проект 2.1.1.419).

Теорема 1. *Пусть L — одна из простых групп $B_n(q)$, где $n \geq 2$ и $(n,q) \neq (2,3)$, $C_n(q)$, где $n \geq 3$, и $D_n(q)$, ${}^2D_n(q)$, где $n \geq 4$. Тогда среди неабелевых композиционных факторов конечных групп, изоспектральных L, нет знакопеременных групп.*

Теорема 2. *Пусть L — одна из простых групп $B_n(q)$, где $n \geq 2$ и $(n,q) \neq (2,3)$, $C_n(q)$, где $n \geq 3$, и $D_n(q)$, ${}^2D_n(q)$, где $n \geq 4$. Тогда среди неабелевых композиционных факторов конечных групп, изоспектральных L, нет спорадических групп и нет группы Титса ${}^2F_4(2)'$.*

Теорема 3. *Пусть q — степень простого числа p, L — одна из простых групп $B_n(q)$, где $n \geq 2$ и $(n,q) \neq (2,3)$, $C_n(q)$, где $n \geq 3$, и $D_n(q)$, ${}^2D_n(q)$, где $n \geq 4$, G — конечная группа со свойством $\omega(G) = \omega(L)$. Предположим, что среди неабелевых композиционных факторов группы G есть фактор S, изоморфный группе лиева типа над полем характеристики p.*

(1) *Если $L = B_2(q)$, где $q > 3$, то $S \in \{A_1(q^2), B_2(q)\}$.*
(2) *Если $L \in \{B_3(q), C_3(q), D_4(q)\}$, то $S \in \{A_1(q^3), B_3(q), C_3(q), D_4(q), G_2(q)\}$.*
(3) *Если $n \geq 4$ и $L \in \{B_n(q), C_n(q), {}^2D_n(q)\}$, то $S \in \{B_n(q), C_n(q), {}^2D_n(q)\}$.*
(4) *Если $n \geq 6$ четно и $L = D_n(q)$, то $S \in \{B_{n-1}(q), C_{n-1}(q), D_n(q)\}$.*
(5) *Если $n \geq 5$ нечетно и $L = D_n(q)$, то $S \simeq L$.*

Отметим, что выбор симплектических и ортогональных групп в качестве объекта исследования обусловлен, в частности, вопросом 12.39 из «Коуровской тетради» [13], в котором речь идет о справедливости гипотезы Ши, впервые сформулированной в [14]. Гипотеза Ши состоит в том, что любая конечная простая группа однозначно характеризуется своим спектром и порядком в классе конечных групп. К настоящему моменту она доказана для всех простых групп, исключая симплектические и некоторые ортогональные группы (см. [15]).

§ 1. Предварительные сведения

В обозначениях спорадических групп и простых групп лиева типа мы следуем [16]. При этом если группа лиева типа L обозначается как ${}^tX_n(q)$ [16, с. xiv, xv], мы говорим, что L — *группа ранга n над полем порядка q*. В частности, ранг скрученной группы считается равным рангу ее нескрученного аналога. Знакопеременная группа степени n обозначается через Alt_n.

Для натурального числа n через $\pi(n)$ обозначается множество простых делителей числа n, через n_r, где r — простое число, — r-часть числа n, т. е. наибольшая степень числа r, делящая n, и через $n_{r'}$ — r'-часть числа n, т. е. отношение n/n_r. Если n и $m > 2$ — взаимно простые натуральные числа, 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 $n > 1$. Простое число r называется *примитивным простым делителем* для разности $n^i - 1$, если $e(r,n) = i$. Существование примитивных делителей для почти всех пар n и i установлено Жигмонди.

Лемма 1.1 [17]. *Пусть $n > 1$ — натуральное число. Тогда для каждого натурального числа i найдется простое число r, для которого $e(r,n) = i$, исключая случаи $n = 2$ и $i = 1$, $n = 3$ и $i = 1$, $n = 2$ и $i = 6$.*

Далее в статье под записью $r_i(n)$ будет подразумеваться какой-нибудь примитивный делитель разности $n^i - 1$, 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, $k_6(2) = 1$, $k_3(4) = 7$, $k_2(8) = 9$ и $k_1(64) = 63$.

Несложно проверить, что $k_1(n) = n - 1$, если $n \not\equiv 3 \pmod 4$, и $k_1(n) = (n-1)/2$, если $n \equiv 3 \pmod 4$, а также, что $k_2(n) = (n+1)/(2, n-1)$, если $n \not\equiv 3 \pmod 4$, и $k_2(n) = n + 1$, если $n \equiv 3 \pmod 4$. Как следует из [18], для $i > 2$

$$k_i(n) = \Phi_i(n)/(r, \Phi_{i_{r'}}(n)),$$

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 $(r, \Phi_{i_{r'}}(n)) = 1$.

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 $1 \leq i \leq s(G)$. 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 $1 \leq i \leq s(G)$. Строение конечных групп с несвязным графом простых чисел описано Грюнбергом и Кегелем.

Лемма 1.2 [19]. *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 $S \leq \overline{G} = G/K \leq \operatorname{Aut} S$ для некоторой нильпотентной нормальной подгруппы K из G; более того, K и $\overline{G}/S$ являются $\pi_1(G)$-группами, $s(S) \geq s(G)$ и для любого $1 < i \leq s(G)$ существует $1 < j \leq s(S)$ такое, что $\omega_i(G) = \omega_j(S)$.*

Конечные простые группы с несвязным графом простых чисел были описаны Уильямсом [19] и А. С. Кондратьевым [20]. Полный список этих групп с исправленными неточностями можно найти в [2, табл. 1a–1c]. Как следует из результатов Уильямса и Кондратьева, если S — простая группа и $s(S) > 1$, то для любого $1 < i \leq s(S)$ множество $\omega_i(S)$ имеет единственный максимальный по делимости элемент [21, 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. В [22, 23] для каждой конечной неабелевой простой группы указан критерий смежности в ее графе простых чисел и найдены все коклики максимального размера в этом графе.

Лемма 1.3 [24, 25]. *Пусть L — конечная неабелева простая группа такая, что $t(L) \geq 3$ и $t(2, L) \geq 2$, а G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$. Тогда выполняются следующие утверждения.*

(1) *Существует неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \operatorname{Aut} S$, где K — максимальная нормальная разрешимая подгруппа группы G.*

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

(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, $t(2, S) \geq t(2, G)$.*

Если Γ — граф простых чисел и π — некоторое множество простых чисел, то через $\Gamma \setminus \pi$ обозначается максимальный подграф графа Γ, все вершины которого не лежат в π. Отметим, что из п. (2) леммы 1.3 кроме неравенства $t(S) \geq t(G) - 1$ следует неравенство $t(GK(S) \setminus \pi) \geq t(GK(G) \setminus \pi) - 1$ для любого множества простых чисел π.

Лемма 1.4. *Пусть G — конечная группа, K — нормальная r-подгруппа в G и G/K — нециклическая абелева p-группа, где r и p — различные простые числа. Тогда $rp \in \omega(G)$.*

Доказательство. Прямое следствие из [26, гл. 5, теорема 3.16].

§ 2. Конечные группы, изоспектральные симплектическим и ортогональным группам

Лемма 2.1. *Пусть L — одна из простых групп $B_n(q)$, где $n \geq 2$, $(n, q) \neq (2, 3)$, $C_n(q)$, где $n \geq 3$, $D_n(q)$, ${}^2D_n(q)$, где $n \geq 4$, и G — конечная группа со свойством $\omega(G) = \omega(L)$. Тогда существует простая неабелева группа S такая, что*

$$S \leq \overline{G} = G/K \leq \operatorname{Aut} S,$$

где K — разрешимый радикал группы G, причем G, K и S удовлетворяют пп. (2) и (3) леммы 1.3.

Доказательство. Если $n > 2$ и $L \neq D_4(2)$, то, как следует из [22], группа L удовлетворяет условиям $t(L) \geq 3$ и $t(2, L) \geq 2$, поэтому утверждение вытекает из леммы 1.3. Пусть $n = 2$ или $L = D_4(2)$. Тогда группа L имеет несвязный граф простых чисел, поэтому требуемое следует из теоремы Грюнберга — Кегеля и основного результата [27], а также из того факта, что в этом случае $t(L) = 2$. Лемма доказана.

Критерий смежности в графах простых чисел симплектических и ортогональных групп сформулирован в [22, предложения 3.1, 4.3, 4.4] и [23, предложения 2.4, 2.5]. В формулировке используется функция $\eta : \mathbb{N} \to \mathbb{N}$, определенная по правилу

$$\eta(n) = \begin{cases} n, & \text{если } n \text{ нечетно;} \\ n/2, & \text{если } n \text{ четно.} \end{cases}$$

Лемма 2.2. *Пусть L, G, S и K такие же, как в лемме 2.1.*

(1) *Предположим, что $L = B_n(q)$ или $L = C_n(q)$, где $n \geq 3$ и $(n, q) \neq (3, 2)$. Если существует i такое, что $n/2 < \eta(i) \leq n$ и $k_i(q) \notin \omega(S)$, то для любого $j \neq i$ такого, что $n/2 \leq \eta(j) \leq n$, число $k_j(q)$ взаимно просто с $|K| \cdot |\overline{G}/S|$ и лежит в $\omega(S)$.*

(2) *Предположим, что $L = D_n(q)$, где $n \geq 4$ и $(n, q) \neq (4, 2)$. Если существует $i \neq 2n$ такое, что $n/2 < \eta(i) \leq n$ и $k_i(q) \notin \omega(S)$, то для любого $j \notin \{i, 2n\}$ такого, что $n/2 \leq \eta(j) \leq n$, число $k_j(q)$ взаимно просто с $|K| \cdot |\overline{G}/S|$ и лежит в $\omega(S)$.*

(3) *Предположим, что $L = {}^2D_n(q)$, где $n \geq 4$ и $(n,q) \neq (4,2), (5,2)$. Если существует $i \neq n$ такое, что $n/2 < \eta(i) \leq n$ и $k_i(q) \notin \omega(S)$, то для любого $j \notin \{i,n\}$ такого, что $n/2 \leq \eta(j) \leq n$, число $k_j(q)$ взаимно просто с $|K| \cdot |\overline{G}/S|$ и лежит в $\omega(S)$.*

Доказательство. Поскольку $k_i(q) \notin \omega(S)$, некоторое $r_i = r_i(q)$ делит $|K| \cdot |\overline{G}/S|$. Пусть $r_j = r_j(q)$ — произвольный примитивный делитель разности $q^j - 1$.

(1) Положим $r = r_{2n}(q)$, если $2n \notin \{i,j\}$. Если $2n \in \{i,j\}$ и $2(n-1) \notin \{i,j\}$, положим $r = r_{2(n-1)}(q)$. Если же $\{i,j\} = \{2n, 2(n-1)\}$, то положим $r = r_n(q)$ для нечетного n и $r = r_{n-1}(q)$ для четного n. Если $(n,q) \neq (4,2)$, то требуемые примитивные делители существуют. В силу [23, предложение 2.4] числа r_i, r_j, r попарно не смежны в $GK(G)$, поэтому из п. (2) леммы 1.3 следует, что r_j не делит $|K| \cdot |\overline{G}/S|$. Значит, $k_j(q) \in \omega(S)$.

Пусть $(n,q) = (4,2)$. По теореме Грюнберга — Кегеля $n_2(L) = k_8(q)$ лежит в $\omega(K)$. Поскольку $k_6(q) = 1$, можно считать, что $i = 3$ и $j = 2$. Числа $r_3(q)$, $r_2(q)$ и $r_8(q)$ образуют коклику в $GK(G)$, поэтому $r_2(q)$ не делит $|K| \cdot |\overline{G}/S|$. Значит, $k_2(q) \in \omega(S)$.

(2) Пусть n четно. Положим $r = r_{2(n-1)}(q)$, если $2(n-1) \notin \{i,j\}$, и $r = r_{n-1}(q)$, если $2(n-1) \in \{i,j\}$ и $n-1 \notin \{i,j\}$. Если же $\{i,j\} = \{2(n-1), n-1\}$, то положим $r = r_n(q)$. Поскольку $(n,q) \neq (4,2)$, требуемые делители существуют.

Пусть n нечетно. Положим $r = r_{2(n-1)}(q)$, если $2(n-1) \notin \{i,j\}$, и $r = r_n(q)$, если $2(n-1) \in \{i,j\}$ и $n \notin \{i,j\}$. Если же $\{i,j\} = \{2(n-1), n\}$, то положим $r = r_{2(n-2)}(q)$ для $n > 5$ и $r = r_{n-2}(q)$ для $n = 5$. Поскольку $n \geq 5$, требуемые делители существуют.

В силу [23, предложение 2.5] указанное число r и числа r_i, r_j попарно не смежны в $GK(G)$, поэтому r_j не делит $|K| \cdot |\overline{G}/S|$. Значит, $k_j(q) \in \omega(S)$.

(3) Положим $r = r_{2n}(q)$, если $2n \notin \{i,j\}$, и $r = r_{2(n-1)}(q)$, если $2n \in \{i,j\}$ и $2(n-1) \notin \{i,j\}$. Если же $\{i,j\} = \{2n, 2(n-1)\}$, то положим $r = r_{2(n-2)}(q)$. Поскольку $(n,q) \notin \{(4,2), (5,2)\}$, требуемые делители существуют. В силу [23, предложение 2.5] числа r_i, r_j, r попарно не смежны в $GK(G)$, поэтому r_j не делит $|K| \cdot |\overline{G}/S|$. Значит, $k_j(q) \in \omega(S)$. Лемма доказана.

Как отмечено во введении, для ряда симплектических и ортогональных групп уже решена проблема распознаваемости или доказана квазираспознаваемость. Из полученных ранее результатов мы используем только результаты, касающиеся нескольких групп малых порядков. Эти группы перечислены в следующей лемме. Отметим, что для всех этих групп утверждения теорем 1–3 верны, поэтому при доказательстве их можно не рассматривать.

Лемма 2.3. *Пусть L — одна из простых групп $B_n(q)$, $C_n(q)$, $D_n(q)$, ${}^2D_n(q)$, и G — конечная группа со свойством $\omega(G) = \omega(L)$.*

(1) *Если $L = B_3(2)$, то $G \simeq B_3(2)$ или $G \simeq D_4(2)$* [2, 5].

(2) *Если $L = B_3(3)$, то $G \simeq B_3(3)$ или $G \simeq D_4(3)$* [5].

(3) *Если $L = B_4(2)$, то G имеет единственный неабелев композиционный фактор S и $S \in \{B_4(2), {}^2D_4(2)\}$* [6].

(4) *Если $L = B_4(3)$, то G имеет единственный неабелев композиционный фактор S и $S \in \{B_4(3), {}^2D_4(3)\}$* [11].

(5) *Если $L = C_3(3)$, то $G \simeq C_3(3)$* [4].

(6) *Если $L = C_4(3)$, то G имеет единственный неабелев композиционный фактор S и $S \in \{C_4(3), {}^2D_4(3)\}$* [11].

(7) *Если* $L = D_4(2)$, *то* $G \simeq B_3(2)$ *или* $G \simeq D_4(2)$ [2, 5].
(8) *Если* $L = D_4(3)$, *то* $G \simeq B_3(3)$ *или* $G \simeq D_4(3)$ [5].
(9) *Если* $L = D_5(2)$, *то* $G \simeq D_5(2)$ [8].
(10) *Если* $L = {}^2D_4(2)$, *то* $G \simeq {}^2D_4(2)$ [5].
(11) *Если* $L = {}^2D_4(3)$, *то* G *имеет единственный неабелев композиционный фактор* S *и* $S \simeq {}^2D_4(3)$ [11].
(12) *Если* $L = {}^2D_4(4)$, *то* G *имеет единственный неабелев композиционный фактор* S *и* $S \simeq {}^2D_4(4)$ [7].
(13) *Если* $L = {}^2D_5(2)$, *то* $G \simeq {}^2D_5(2)$ [4].

Лемма 2.4. *Если* $L \in \{B_3(4), D_4(4)\}$, *то для* L *выполнено утверждение теоремы* 3.

Доказательство. Пусть G — конечная группа со свойством $\omega(G) = \omega(L)$. По лемме 2.1 выполнено $S \leq \overline{G} = G/K \leq \operatorname{Aut} S$, где K — разрешимый радикал группы G. Числа 7 и 13 лежат в $\pi(L)$ и не смежны с 2 в $GK(L)$, следовательно, они лежат в $\pi(S)$, при этом $\pi(S) \subseteq \pi(L) = \{2, 3, 5, 7, 13, 17\}$. Как показывает [28, табл. 1], среди групп лиева типа над полем характеристики 2 этим условиям удовлетворяют только группы $A_1(64)$, $A_2(16)$, $B_2(8)$, $B_3(4)$, $D_4(4)$, $G_2(4)$, $F_4(2)$, ${}^3D_4(2)$ и $Sz(8)$. Группа $A_2(16)$ содержит элемент порядка 91, а группы $B_2(8)$, $F_4(2)$, ${}^3D_4(2)$ содержат элемент порядка 14. Значит, для доказательства леммы достаточно показать, что $S \not\simeq Sz(8)$.

Предположим, что $S \simeq Sz(8)$. Тогда $17 \notin \pi(\operatorname{Aut} S)$ и, значит, $17 \in \pi(K)$. В группе S есть подгруппа Фробениуса с ядром порядка 2^6 и циклическим дополнением порядка 7 (см. [16]). Используя [29, лемма 3], заключаем, что $17 \cdot 7 \in \omega(G)$, но $17 \cdot 7 \notin \omega(L)$; противоречие.

§ 3. Доказательство теоремы 1

Пусть L — одна из групп, указанных в условии теоремы 1, и q — степень простого числа p. Пусть G — конечная группа, изоспектральная L. Предположим, от противного, что среди неабелевых композиционных факторов группы G есть знакопеременная группа. Тогда по лемме 2.1 имеем $S \leq \overline{G} = G/K \leq \operatorname{Aut} S$, где K — разрешимый радикал группы G и $S \simeq \mathrm{Alt}_m$ для $m \geq 5$.

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

(1) для любого $i \in M$ выполнено неравенство $n/2 < \eta(i) \leq n$, причем $i \neq 2n$, если $L = D_n(q)$, и $i \neq n$, если $L = {}^2D_n(q)$;

(2) для любого $i \in M$ число $k_i(q)$ отлично от единицы.

Рассмотрим числа $k_i(q)$, где i пробегает M. В силу леммы 2.2 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 $r^2 > (m/2)^2 > m$, следовательно, $r^2 \in \omega(L) \setminus \omega(G)$; противоречие. Тем самым k — простое число и условие $k \in \omega(S)$ влечет неравенство $m \geq k$. Таким образом, $m \geq k_i(q)$ для некоторого $i \in M$.

Идея дальнейшего рассуждения такова. С помощью специального выбора множества M мы ограничим m снизу через n и q. Затем придем к противоречию, показав, что за некоторыми исключениями, которые будут разобраны отдельно, p-период группы S будет строго больше p-периода группы L.

Лемма 3.1. *Пусть i — нечетное простое число и q — степень простого числа p. Тогда $k_i(q) > q^{i-2}$. Если $(i,q) \neq (3,2)$, то $k_{2i}(q) > q^{i-2}/p$, и если $i \neq q+1$, то $k_{2i}(q) > q^{i-2}$.*

Доказательство. Поскольку $k_i(q) = (q^i-1)/(q-1)(i,q-1)$, получаем, что

$$k_i(q) \geq \frac{q^i-1}{(q-1)^2} = \frac{q^{i-1}+\dots+1}{q-1} > \frac{q^{i-1}}{q} = q^{i-2}.$$

Предположим, что $q > 2$. Тогда $(q+1)^2 < 2q^2 \leq pq^2$, поэтому из равенства $k_{2i}(q) = (q^i+1)/(q+1)(i,q+1)$ следует, что

$$k_{2i}(q) \geq \frac{q^i+1}{(q+1)^2} > \frac{q^i}{pq^2} = \frac{q^{i-2}}{p},$$

и при условии $i \neq q+1$ — что

$$k_{2i}(q) \geq 2\frac{q^i+1}{(q+1)^2} > \frac{q^i}{q^2} = q^{i-2}.$$

Пусть $q = 2$. Тогда $i \neq 3$ и, значит, $(i,q+1) = 1$. Таким образом, $k_{2i}(q) = (2^i+1)/3 > 2^{i-2}$. Лемма доказана.

Случай $L = B_n(q)$ или $L = C_n(q)$, где $n \geq 3$.

Обозначим p-период группы L через p^l. Как следует из [30, предложение 0.5], число l удовлетворяет неравенствам

$$(p^{l-1}+1)/2 \leq n < (p^l+1)/2. \qquad (*)$$

Предположим, что $n \geq 11$. Обозначим через i наибольшее простое число из промежутка $(n/2, n]$. Поскольку $n \geq 11$, в этом промежутке найдется по крайней мере два различных простых числа, значит, $i \geq (n+5)/2$. Положим

$$k_i = k_i(q) = \frac{q^i-1}{(q-1)(i,q-1)} \quad \text{и} \quad k_{2i} = k_{2i}(q) = \frac{q^i+1}{(q+1)(i,q+1)}.$$

Обозначим через j единственную степень числа 2, лежащую в $(n/2, n]$. Положим

$$k_{2j} = k_{2j}(q) = \frac{q^j+1}{(2,q-1)}.$$

Поскольку множество $M = \{i, 2i, 2j\}$ удовлетворяет условиям (1) и (2), по крайней мере одно из чисел k_i, k_{2i}, k_{2j} является простым числом, не превосходящим m. Значит, $m \geq \min\{k_i, k_{2i}, k_{2j}\}$.

Поскольку $i \geq \max\{(n+5)/2, 11\}$, по лемме 3.1 получаем, что каждое из чисел k_i и k_{2i} больше, чем $\max\{q^{(n+1)/2}/p, q^9/p\}$. Кроме того, $j \geq \max\{(n+1)/2, 8\}$, поэтому $k_j > \max\{q^{(n+1)/2}/p, q^8/p\}$. Таким образом,

$$m \geq \min\{k_i, k_{2i}, k_{2j}\} > \max\{q^{\frac{n+1}{2}}/p, q^8/p\}.$$

Поскольку $m > q^8/p \geq p^6+1$, в группе S есть элемент порядка p^6. Следовательно, $p^6 \in \omega(L)$ и $l \geq 6$. Для $l \geq 6$ выполнено неравенство $l+2 < (2^{l-1}+3)/4$, поэтому $l+2<(p^{l-1}+3)/4$. Из $(*)$ следует, что $(p^{l-1}+3)/4 \leq (n+1)/2$. Таким образом, $l+2<(n+1)/2$, и, значит, $m>q^{(n+1)/2}/p>p^{l+2}/p=p^{l+1}$, откуда $p^{l+1}\in\omega(G)\setminus\omega(L)$; противоречие.

Предположим, что $n=9,10$. Множество $M=\{9,18,16\}$ удовлетворяет условиям (1) и (2), поэтому $m\geq\min\{k_9,k_{18},k_{16}\}$. Следовательно, $m>q^6/q$ при $q\neq 2$, и $m\geq 19$ при $q=2$. Если $p\neq 2$, то $m>p^5$, а значит, $l\geq 5$. Но тогда $n\geq(p^{l-1}+1)/2\geq(3^4+1)/2=41$; противоречие. Если $p=2$ и $q>2$, то $m>4^6/4=1024$, а значит, $2^9\in\omega(G)\setminus\omega(L)$. Пусть, наконец, $q=2$. Если $n=9$, то в силу равенства $e(73,2)=9$ число 73 лежит в $\pi(L)$ и не смежно с 2 в $GK(L)$, откуда в силу п. (3) леммы 1.3 следует, что $73\in\omega(S)$ и, значит, $m\geq 73$. Аналогично если $n=10$, то 41 не смежно с 2 в графе простых чисел группы L и поэтому лежит в $\omega(S)$, откуда $m\geq 41$. В обоих случаях $29\in\omega(G)\setminus\omega(L)$; противоречие.

Предположим, что $n=8$. Тогда $GK(L)$ имеет две компоненты связности, и $n_2(L)=(q^8+1)/(2,q-1)$. По теореме Грюнберга — Кегеля граф $GK(S)$ тоже несвязен и $n_2(L)=n_2(S)$, откуда $m\geq(q^8+1)/(2,q-1)$. Тогда $m>q^7+1$, откуда $l\geq 7$ и $n\geq(p^6+1)/2\geq(2^6+1)/2>32$; противоречие.

Предположим, что $n=5,6,7$. Множество $M=\{5,10,8\}$ удовлетворяет условиям (1) и (2), поэтому $m>q^3$, если $q\neq 4$, и $m\geq 41$, если $q=4$. При $p>3$ выполняется цепочка неравенств $n\geq(p^2+1)/2\geq(5^2+1)/2=13$, что невозможно. Если $p\in\{2,3\}$, $q>p$ и $q\neq 4$, то $m>q^3\geq p^6$, откуда $n\geq(p^5+1)/2\geq(2^5+1)/2>16$. Если $q=3$, то $m>27$, а если $q=4$, то $m\geq 41$. В обоих случаях $19\in\omega(S)$. Поскольку $e(19,2)=e(19,3)=18$, число 19 может делить порядок L только при $n\geq 9$; противоречие.

Пусть $q=2$. Если $n=5$, то 31 не смежно с 2 в $GK(L)$, следовательно, лежит в $\omega(S)$. Аналогично если $n=7$, то 127 не смежно с 2 в $GK(L)$. В обоих случаях $m\geq 31$, поэтому $19\in\omega(S)\setminus\omega(L)$; противоречие. Пусть $n=6$. В этом случае 13 не смежно с 2 в $GK(L)$, значит, 13 взаимно просто с числом $|K|\cdot|\overline{G}/S|$ и лежит в $\omega(S)$. Следовательно, $13\leq m\leq 16$. Поскольку 65 и 31 лежат в $\omega(L)$, но не лежат в $\omega(\operatorname{Aut}S)$, порядок разрешимого радикала K делится на 5 и 31. Обозначим через T полный прообраз силовской 11-подгруппы группы $\overline{G}$ в G. Группа T разрешима, а значит, по [24, предложение 1] ее граф простых чисел не может содержать коклики из трех или более элементов. Поскольку $\sigma=\{5,11,31\}\subseteq\pi(T)$, по крайней мере два простых числа из σ смежны в $GK(T)$, а значит, и в $GK(G)=GK(L)$. Получаем противоречие, так как в L нет элементов порядков $5\cdot 11, 5\cdot 31, 11\cdot 31$.

Предположим, что $n=4$. По лемме 2.3 можно считать, что $q>3$. Граф $GK(L)$ имеет две компоненты связности, и $n_2(L)=(q^4+1)/(2,q-1)$. По теореме Грюнберга — Кегеля граф $GK(S)$ тоже несвязен и $n_2(L)=n_2(S)$, откуда $m\geq(q^4+1)/(2,q-1)$. Если $q>p$, то $m\geq(q^4+1)/(2,q-1)>q^4/p\geq p^7$, откуда $n\geq(p^6+1)/2\geq(2^6+1)/2>32$; противоречие. Если $q=p>3$, то $m>p^3$, следовательно, $n\geq(p^2+1)/2\geq 5$, что невозможно.

Предположим, что $n=3$. По лемме 2.3 можно считать, что $q>3$, и тогда множество $M=\{3,6,4\}$ удовлетворяет условиям (1) и (2).

Пусть $q=2^\alpha>2$. Поскольку 2-период группы L равен 8, имеем $m\leq 17$. Если степень α нечетна, то $m\geq\min\{k_3,k_4,k_6\}=k_6=(q^2-q+1)/3\geq(8^2-8+1)/3=19$; противоречие. Если степень α четна, то $m\geq\min\{k_3,k_4,k_6\}=k_3=(q^2+q+1)/3$. При $q>4$ имеем $m\geq 91$. Осталось рассмотреть группу $C_3(4)$. Поскольку число $k_6=13$ не смежно с 2 в $GK(L)$, оно лежит в $\omega(S)$. Значит,

$m \geq 13$. Тогда $11 \in \omega(S) \setminus \omega(L)$; противоречие.

Пусть $q = 3^\alpha > 3$. Тогда 3-период группы L равен 9, а значит, $m \leq 26$. С другой стороны, $m \geq \min\{k_3, k_4, k_6\} = k_4 = (q^2+1)/2 \geq 41$; противоречие.

Пусть $q = p^\alpha$, где $p \notin \{2,3\}$. В этом случае $\min\{k_3, k_4, k_6\} = (q^2+\varepsilon q+1)/3$, где $q \equiv \varepsilon 1 \pmod 3$. Если $p > 5$, то p-период группы L равен p, и если $p = 5$, то он равен 5^2. Если $q > p > 5$, то $m \geq (p^4 - p^2 + 1)/3 > p^2$, что невозможно. Если $q = 5^\alpha > 5$, то $m \geq (5^4 + 5^2 + 1)/3 > 5^3$; противоречие. Таким образом, можно считать, что $q = p$. Рассмотрим четыре возможных случая в зависимости от остатка числа p по модулю 12.

Если $p \equiv 11 \pmod{12}$, то каждый простой делитель r числа $k_3 = p^2+p+1$ не смежен с 2 в $GK(L)$. Тогда r взаимно прост с $|K| \cdot |\overline{G}/S|$ и $r \in \omega(S)$. Это возможно, только если $r = k_3$ — простое число и $m - 3 \leq k_3 \leq m$. Получаем, что $p^2 \in \omega(S) \setminus \omega(L)$.

Если $p \equiv 1 \pmod{12}$, то $p \geq 13$ и каждый простой делитель r числа $k_6 = p^2-p+1$ не смежен с 2 в $GK(L)$. Тогда r взаимно прост с $|K|\cdot|\overline{G}/S|$ и $r \in \omega(S)$. Это возможно, только если $r = k_6$ — простое число и $m-3 \leq k_6 \leq m$. Пусть s — простой делитель числа $k_3 = (p^2+p+1)/3$. Тогда $sp \notin \omega(L)$. Однако при $p \geq 13$ выполняются неравенства $s+p \leq (p^2+p+1)/3+p = (p^2+4p+1)/3 < p^2-p+1 \leq m$. Значит, $sp \in \omega(S) \setminus \omega(L)$.

Если $p \equiv 7 \pmod{12}$, то $p \geq 7$ и каждый простой делитель r числа $k_3 = (p^2+p+1)/3$ не смежен с 2 в $GK(L)$. Тогда r взаимно прост с $|K| \cdot |\overline{G}/S|$ и $r \in \omega(S)$. Это возможно, только если $r = k_3$ — простое число и $m - 3 \leq k_3 \leq m$. Поскольку $p \geq 7$, получаем, что $m > 2p$ и, следовательно, силовская p-подгруппа группы S содержит элементарную абелеву подгруппу порядка p^2. Значит, по лемме 1.4 любой простой делитель числа $|K|$, отличный от p, смежен с p в $GK(G)$. Каждый простой делитель числа $k_6 = p^2 - p + 1$ не смежен с p в $GK(L)$, поэтому $k_6 = p^2 - p + 1 \in \omega(S)$. Поскольку $k_6 > k_3 + 3 \geq m$, число k_6 должно быть составным. Значит, найдется простой делитель s этого числа, не превосходящий $\sqrt{p^2 - p + 1}$. Имеем $s + p \leq \sqrt{p^2 - p + 1} + p < 2p < m$; противоречие.

Если $p \equiv 5 \pmod{12}$, то каждый простой делитель r числа $k_6 = (p^2-p+1)/3$ не смежен с 2 в $GK(L)$. Значит, r взаимно прост с $|K| \cdot |\overline{G}/S|$ и $r \in \omega(S)$. Это возможно, только если $r = k_6$ — простое число и $m-3 \leq k_6 \leq m$. Предположим, что $p \neq 5$, а значит, $p \geq 17$. Тогда $m > 2p$ и, следовательно, силовская p-подгруппа группы S содержит элементарную абелеву подгруппу порядка p^2. Значит, по лемме 1.4 любой простой делитель числа $|K|$, отличный от p, смежен с p в $GK(G)$. Каждый простой делитель числа $k_3 = p^2 + p + 1$ не смежен с p в $GK(L)$, поэтому $k_3 = p^2 + p + 1 \in \omega(S)$. Поскольку $k_3 > k_6 + 3 \geq m$, число k_3 должно быть составным. Значит, найдется простой делитель s этого числа, не превосходящий $\sqrt{p^2 + p + 1}$. Имеем $s + p \leq \sqrt{p^2 + p + 1} + p < 2p + 1 < m$; противоречие. Пусть, наконец, $p = 5$. Тогда $7 \leq m \leq 10$. Значит, $31 = k_3$ не делит порядок группы $\operatorname{Aut} S$. Следовательно, $31 \in \omega(K)$. Однако S содержит элементарную абелеву подгруппу порядка 3^2, откуда по лемме 1.4 получаем, что $31 \cdot 3 \in \omega(G) \setminus \omega(L)$.

Случай $L = D_n(q)$ или $L = {}^2D_n(q)$, где $n \geq 4$.

В силу [30, предложение 0.5] если p-период группы L равен p^l, то выполняются неравенства $(p^{l-1}+3)/2 \leq n < (p^l+3)/2$. В частности, $n \geq (p^{l-1}+3)/2 > (p^{l-1}+1)/2$. Это означает, что при равных p-периодах у группы типа D_n или ${}^2D_n$ лиев ранг не меньше, чем у группы типа B_n или C_n.

Предположим, что $n \geq 12$. Обозначим через i наибольшее простое число из интервала $(n/2, n)$. Поскольку при $n \geq 12$ в этом интервале найдется по крайней мере два различных простых числа, $i \geq (n+5)/2$. Положим

$$k_i = k_i(q) = \frac{q^i - 1}{(q-1)(i, q-1)} \quad \text{и} \quad k_{2i} = k_{2i}(q) = \frac{q^i + 1}{(q+1)(i, q+1)}.$$

Обозначим через j такую степень числа 2, что $j \in (n/2, n]$, за одним исключением: если $L = D_n(q)$, а n является степенью числа 2, то через j обозначим $n/2$. Положим

$$k_{2j} = k_{2j}(q) = \frac{q^j + 1}{(2, q-1)}.$$

Поскольку трехэлементное множество $M = \{i, 2i, 2j\}$ удовлетворяет условиям (1) и (2), по крайней мере одно из чисел k_i, k_{2i}, k_{2j} является простым числом, не превосходящим m. Значит, $m \geq \min\{k_i, k_{2i}, k_{2j}\}$.

В силу того, что $i \geq \max\{(n+5)/2, 11\}$, а $j \geq \max\{(n+1)/2, 8\}$, имеем

$$\min\{k_i, k_{2i}, k_{2j}\} > \max\{q^{\frac{n+1}{2}}/p, q^8/p\}.$$

Рассуждая так же, как в случае групп типов B_n и C_n, получаем, что $l + 2 < (n+1)/2$, откуда $m \geq q^{(n+1)/2}/p > q^{l+2}/p \geq p^{l+1}$. Но тогда $p^{l+1} \in \omega(G) \setminus \omega(L)$; противоречие.

Предположим, что $n = 10, 11$. Поскольку множество $M = \{9, 18, 16\}$ удовлетворяет условиям (1) и (2), доказательство аналогично доказательству для групп $B_n(q)$ и $C_n(q)$ при $n = 9, 10$. Действительно, все оценки остаются в силе, поэтому во всех случаях, кроме $q = 2$, сразу получаем, что p-период группы L строго меньше p-периода группы S, а это невозможно. Пусть $q = 2$. В графах простых чисел групп ${}^2D_{10}(2)$, ${}^2D_{11}(2)$ и $D_{11}(2)$ число 41 не смежно с 2, поэтому для этих групп $m \geq 41$. В группе $D_{10}(2)$ число 73 не смежно с 2, а значит, $m \geq 73$. Во всех случаях $29 \in \omega(G) \setminus \omega(L)$; противоречие.

Предположим, что $n = 9$. Множество $M = \{7, 14, 16\}$ удовлетворяет условиям (1) и (2), поэтому $m \geq \min\{k_7, k_9, k_{16}\} > q^5/p$. Если $p \neq 2$, то $p^4 \in \omega(L)$, откуда $n \geq (p^3 + 3)/2 \geq (3^3 + 3)/2 = 15$; противоречие. Если $p = 2$ и $q > 2$, то $p^8 \in \omega(L)$, откуда $n \geq (2^7 + 3)/2 > 9$; противоречие. Если $q = 2$, то 257 не смежно с 2 в $GK(L)$, поэтому $m \geq 257$. Значит, $2^8 \in \omega(L)$ и $n \geq (2^7 + 3)/2 > 9$; противоречие.

Поскольку граф простых чисел группы $L = {}^2D_8(q)$ имеет две компоненты связности и $n_2(L) = (q^8 + 1)/(2, q-1)$, этот случай разбирается полностью аналогично случаю групп $B_8(q)$ и $C_8(q)$.

Предположим, что $n = 6, 7$ при $L = {}^2D_n(q)$ и $n = 6, 7, 8$ при $L = D_n(q)$. Тогда множество $M = \{5, 10, 8\}$ удовлетворяет условиям (1) и (2), поэтому, если $q \neq 2$, доказательство проводится так же, как в случае групп $B_n(q)$ и $C_n(q)$ при $n = 5, 6, 7$. Пусть $q = 2$. В графе $GK(L)$ число 2 не смежно с числом 31, если $L = D_6(2)$ или $L = {}^2D_6(2)$, с числом 127, если $L = D_7(2)$ или $L = D_8(2)$, и с числом 43, если $L = {}^2D_7(2)$. Отсюда вытекает, что $m \geq 31$. Но тогда $19 \in \omega(S) \setminus \omega(L)$; противоречие.

Предположим, что $n = 5$. В силу леммы 2.3 можно считать, что $q > 2$. Положим

$$i = \begin{cases} 5, & \text{если } L = D_5(q), \\ 10, & \text{если } L = {}^2D_5(q), \end{cases} \qquad j = \begin{cases} 3, & \text{если } (3, q-1) = 1, \\ 6 & \text{в остальных случаях} \end{cases}$$

и рассмотрим числа $k_8 = k_8(q)$, $k_i = k_i(q)$ и $k_j = k_j(q)$.

Трехэлементное множество $M = \{8, i, j\}$ удовлетворяет условиям (1) и (2), поэтому $m \geq q^2 - q + 1$. Поскольку при $q > 2$ выполняется неравенство $q^2 - q + 1 > 2p$, силовская p-подгруппа группы S содержит элементарную абелеву p-подгруппу порядка p^2. Следовательно, по лемме 1.4 любой простой делитель числа $|K|$, отличный от p, смежен с p в графе $GK(G)$. Любой простой делитель чисел k_8 и k_i не смежен с p в $GK(L)$, поэтому k_8 и k_i лежат в $\omega(S)$. Значит, по крайней мере одно из этих чисел должно быть простым числом, лежащим между $m/2$ и m. Обозначим это число через k. Имеем $m \geq k \geq \min\{k_8, k_i\}$. Следовательно, $m > p^3$, если $q \neq 4$, и $m \geq 41$, если $q = 4$. Если $p > 3$, то p-период группы L не превосходит p^2, что сразу приводит нас к противоречию. Если $p = 3$, то 3-период группы L равен 3^3, что снова приводит к противоречию при $q > 3$. Наконец, если $p = 2$, то 2-период группы L равен 2^4, и мы снова получаем противоречие при $q > 4$. Таким образом, нам осталось рассмотреть группы $D_5(q)$ и ${}^2D_5(q)$, где $q = 3, 4$. В этом случае $m > 27$ и, значит, $19 \in \omega(S) \setminus \omega(L)$, что невозможно.

Граф простых чисел группы $L = {}^2D_4(q)$ имеет две компоненты связности и $n_2(L) = (q^4 + 1)/2$. Поэтому рассуждение, приводящее к противоречию, дословно повторяет рассуждение для групп $B_4(q)$ и $C_4(q)$.

Осталось разобрать случай $L = D_4(q)$. По лемме 2.3 можно считать, что $q > 3$. Тогда, как и в случае $L = B_3(q)$ или $L = C_3(q)$, множество $M = \{3, 6, 4\}$ удовлетворяет условиям (1) и (2). Дальнейшее рассуждение полностью совпадает с рассуждением для групп $B_3(q)$ и $C_3(q)$, включая детальный разбор четырех случаев по модулю 12 при $q = p > 3$.

Случай $L = B_2(q)$, где $q > 3$.

Граф простых чисел группы L имеет две компоненты связности. Обозначим через k число $n_2(L) = (q^2 + 1)/(2, q - 1)$. По теореме Грюнберга — Кегеля получаем, что k — простое число и $m - 2 \leq k \leq m$.

Предположим сначала, что $q > p$. Тогда $m \geq (p^4 + 1)/(2, p - 1) > p^3 + 1$. Однако p-период группы L равен p при $p > 3$ и p^2 при $p \in \{2, 3\}$. Получаем, что $p^3 \in \omega(S) \setminus \omega(L)$.

Таким образом, $q = p \geq 5$. В этом случае любой простой делитель порядка группы L, не делящий k, либо равен p, либо делит $p - 1$, либо делит $p + 1$. В любом случае, он не превосходит $p + 1$. С другой стороны, $2(p + 1) < (p^2 + 1)/2 = k$ и $p + 1 \geq 6$, поэтому в интервале $(p + 1, k)$ содержится по крайней мере одно простое число r. Получаем противоречие, так как $r \in \omega(S) \setminus \omega(L)$.

Теорема 1 доказана.

§ 4. Доказательство теоремы 2

Пусть L — одна из групп, указанных в условии теоремы 2, и q — степень простого числа p. Пусть G — конечная группа, изоспектральная L. Допустим, что утверждение теоремы неверно. Тогда по лемме 2.1 имеем $S \leq \overline{G} = G/K \leq \operatorname{Aut} S$, где K — разрешимый радикал группы G и S — спорадическая группа или группа Титса. Отметим, что все элементы $\omega(S)$ не превосходят 119.

Предположим, что $L = B_2(q)$. Тогда граф $GK(L)$ несвязен, и по теореме Грюнберга — Кегеля число $u = (q^2 + 1)/(2, q - 1)$ принадлежит спектру группы

S. Как следует из [3, 31],

$$\mu(L) = \begin{cases} \left\{ \frac{q^2+1}{(2,q-1)}, \frac{q^2-1}{(2,q-1)}, p(q+1), p(q-1) \right\}, & \text{если } p > 3, \\ \left\{ \frac{q^2+1}{(2,q-1)}, \frac{q^2-1}{(2,q-1)}, p(q+1), p(q-1), p^2 \right\}, & \text{если } p \in \{2,3\}. \end{cases}$$

Оба числа $p(q+1)/3$ и $p(q-1)/2$ меньше, чем u; если $p = 2$, то $p^2 < u$; если $p = 3$, то $q > 3$ и $p^2 < u$. Таким образом,

(1) $(q^2+1)/(2, q-1) \in \omega(S)$;

(2) одно из чисел $(q^2+1)/(2, q-1)$, $p(q+1)$, $p(q+1)/2$, $p(q-1)$ является наибольшим элементом множества $\omega(S)$.

В силу условия $(q^2+1)/(2, q-1) \leq 119$ получаем, что $q \leq 13$. Индивидуальная проверка для каждого $q \leq 13$ показывает, что ни одна из спорадических групп, ни группа Титса условиям (1) и (2) не удовлетворяют. Таким образом, $n > 2$.

Предположим, что $n \geq 12$. Так же, как в доказательстве теоремы 1 для случая $L \in \{D_n(q), {}^2D_n(q)\}$, выберем тройку $\{k_i(q), k_{2i}(q), k_{2j}(q)\}$. По лемме 2.2 по крайней мере два из этих трех чисел принадлежат спектру группы S. Тривиальные оценки показывают, что при $n \geq 12$ все числа из тройки больше 119, поэтому ни одно из них не может принадлежать $\omega(S)$; противоречие.

Предположим, что $n = 11$. Так же, как в доказательстве теоремы 1, показываем, что два из чисел $k_9(q)$, $k_{18}(q)$, $k_{16}(q)$ принадлежат $\omega(S)$. При $q > 2$ оба числа $k_9(q)$ и $k_{16}(q)$ больше 119, поэтому $q = 2$. Так как $k_9(2) = 73$ и $k_{16}(2) = 257$, ни одно из этих чисел не может содержаться в $\omega(S)$; противоречие.

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, причем простые делители числа $k_i(q)$ не смежны с 2 в графе простых чисел этой группы, то тройка $(i, q, k_i(q))$ содержится в табл. 1.*

Таблица 1

	i									
q	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			43						
8				19						
9		41								
11				37						

Доказательство. Так как $119 \geq k_i(q) \geq (q^2-q+1)/3$, получаем, что $q \leq 19$. Теперь непосредственные вычисления показывают справедливость леммы.

Предположим, что $3 \leq n \leq 10$. В силу критерия смежности с числом 2 и леммы 1.3 в множестве $\{n-1, n, 2n-2, 2n\}$ найдется хотя бы одно i такое, что простые делители $k_i(q)$ не смежны с 2 в $GK(L)$ и, значит, $k_i(q) \in \omega(S)$. Тогда из леммы 4.1 следует, что $q \leq 11$. При таких значениях q в $\pi(L)$ нет чисел 23, 59 и 67, поэтому S отлична от F_1, F_2, LyS, Fi'_{24}, Fi_{23}, J_4, M_{24}, M_{23} и групп Конвея. Следовательно, в S нет элементов порядка 37, 41 и 43, откуда $q \leq 8$.

Для всех групп L с $3 \leq n \leq 10$ и $q \leq 8$, кроме групп, перечисленных в лемме 2.3, проводится проверка по следующей схеме.

Пусть $L = B_5(2)$. Тогда по лемме 1.3 числа $k_5(2) = 31$ и $k_{10}(2) = 11$ принадлежат $\omega(S)$, при этом $\pi(S) \subseteq \pi(L) = \{2, 3, 5, 7, 11, 17, 31\}$. Как показывает табл. 1 в [28], ни одна из спорадических групп S таким условиям не удовлетворяет.

Подобная проверка оставляет в качестве возможных лишь пары (L, S) из множества $\{(B_6(2), Suz), (B_6(2), Fi_{22}), (D_4(5), J_2)\}$. Случай $L = B_6(2)$ невозможен, поскольку 13, 17, 31 составляют коклику в графе $GK(L)$ и, следовательно, одно из чисел 17, 31 должно принадлежать либо спектру Suz, либо спектру Fi_{22}, что неверно. Аналогично в случае $L = D_4(5)$ коклику составляют числа 7, 13, 31, поэтому одно из чисел 13, 31 должно принадлежать спектру $S = J_2$, что неверно.

Теорема 2 доказана.

§ 5. Доказательство теоремы 3

Пусть L — одна из групп, указанных в условии теоремы 3, $q = p^\alpha$ и G — конечная группа, изоспектральная L. По лемме 2.1 и условию теоремы имеем $S \leq G/K \leq \mathrm{Aut}(S)$, где S — простая неабелева группа, изоморфная группе лиева типа над полем характеристики p. Поскольку утверждение теоремы выполнено для групп L, перечисленных в леммах 2.3 и 2.4, эти группы далее не рассматриваются. При доказательстве используются критерии смежности в графе простых чисел из [22, 23], табл. 4–7 из [22] и табл. 2–4 из [23].

Лемма 5.1. *Предположим, что $S \not\simeq A_1(p)$. Тогда любое число r из $\pi(L)$, не смежное с p в $GK(L)$, взаимно просто с $|K| \cdot |\overline{G}/S|$; в частности, $t(p, S) \geq t(p, L)$.*

Доказательство. Пусть L — одна из групп $B_n(q)$ и $C_n(q)$, где n четно. Тогда r не смежно не только с p, но и с 2 в $GK(L)$, и заключение леммы следует из п. (3) леммы 1.3.

Предположим теперь, что L отлична от групп $B_n(q)$ и $C_n(q)$, где n четно. Тогда в графе $GK(G)$ есть коклика размера три вида $\{r, s, p\}$. Как несложно проверить, каждое из чисел r и s больше 3. Предположим, что $r \notin \pi(S)$. Тогда $r \in \pi(\overline{G}/S)$ или $r \in \pi(K)$. Кроме того, из п. (2) леммы 1.3 следует, что $s, p \notin \pi(K) \cup \pi(\overline{G}/S)$.

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

Пусть $r \in \pi(K)$. Как и в предыдущем случае, покажем, что $rp \in \omega(G)$, и получим противоречие. Пусть R — силовская r-подгруппа группы K и $N = N_G(R)$. Тогда в силу аргумента Фраттини $N/(N \cap K) \simeq G/K \simeq S$, поэтому без ограничения общности можно считать, что R нормальна в G и силовская p-подгруппа P группы G действует на ней сопряжением. Поскольку $p \notin \pi(K) \cup \pi(\overline{G}/S)$, группа P изоморфна силовской p-подгруппе группы S. По условию S отлична от $A_1(p)$, поэтому ее силовская p-подгруппа содержит элементарную абелеву подгруппу порядка p^2. Для группы $A_1(p^\beta)$, где $\beta > 1$, это подгруппа элементарной абелевой силовской p-подгруппы; для остальных групп Шевалле эта подгруппа порождается корневым элементом, соответствующим самому высокому корню системы корней, и любым другим неединичным корневым элементом, соответствующим положительному корню. Для скрученных групп эта подгруппа несложно строится на основе [32, предложение 13.6.3]. Таким образом, абелева нециклическая группа действует на группе R. По лемме 1.4 группа G содержит элемент порядка pr. Лемма доказана.

Лемма 5.2. *Если S изоморфна группе типа A_1, то либо $L = B_2(q)$, $q > 3$, и $S \simeq A_1(q^2)$, либо $L \in \{B_3(q), C_3(q), D_4(q)\}$ и $S \simeq A_1(q^3)$.*

Доказательство. Пусть $S \simeq A_1(p^\beta)$. Тогда $t(GK(S) \setminus \{p\}) = 2$, поэтому $t(GK(L) \setminus \{p\}) \leq 3$. Следовательно, $L \in \{B_2(q), B_3(q), C_3(q), D_4(q)\}$.

Если $L = B_2(q)$, то $GK(L)$ несвязен. По теореме Грюберга — Кегеля получаем, что $(q^2+1)/(2,p-1) = (p^\beta \pm 1)/(2,p-1)$, откуда $p^\beta = q^2$. Значит, в этом случае $S \simeq A_1(q^2)$.

Предположим, что $L \in \{B_3(q), C_3(q), D_4(q)\}$. По лемме 2.3 можно считать, что $q > 3$, поэтому определены $r_6 = r_{6\alpha}(p)$ и $r_3 = r_{3\alpha}(p)$, и $\{p, r_3, r_6\}$ — коклика в $GK(L)$.

Пусть $\beta > 1$. По лемме 5.1 число r_6 лежит в $\pi(S)$. Значит, r_6 делит $p^{2\beta}-1$, откуда 6α делит 2β. Если $2\beta > 6\alpha$, то $r_{2\beta}(q) \in \pi(S) \setminus \pi(L)$. Таким образом, $2\beta = 6\alpha$ и $S \simeq A_1(q^3)$.

Пусть $\beta = 1$. По лемме 1.3 хотя бы одно из чисел r_6 и r_3 лежит в $\pi(S)$, следовательно, делит p^2-1; противоречие с определением примитивного делителя. Лемма доказана.

Лемма 5.3. *Пусть S — группа над полем порядка p^β.*

(1) *Если $r_i(p^\beta) \in \pi(S)$, то $i\beta \leq 2n\alpha$ при $L \neq D_n(q)$ и $i\beta \leq 2(n-1)\alpha$ при $L = D_n(q)$.*

(2) *Если $(i\beta, p) \neq (6,2)$ и $k_{i\beta}(p) \in \omega(S)$, то $i\beta$ делит $2j\alpha$, где $j \in \{1,\dots,n\}$ при $L \neq D_n(q)$ и $j \in \{1,\dots,n-1\}$ при $L = D_n(q)$.*

Доказательство. (1) Допустим, что $L \neq D_n(q)$ и $i\beta > 2n\alpha$. Тогда $i\beta > 6$ при $p = 2$, поэтому существует $r = r_{i\beta}(p)$. По условию $r_i(p^\beta)$ делит порядок группы S. Значит, $k_i(p^\beta)$ делит порядок группы S. Следовательно, r делит порядок группы S. Таким образом, $r \in \pi(L)$, и требуемое следует из определения примитивного делителя. Случай $L = D_n(q)$ рассматривается аналогично.

(2) Если $i\beta \leq 2$, то требуемое выполнено. Если $i\beta > 2$, то $k_{i\beta}(p) \neq 1$, и заключение следует из определения примитивного делителя. Лемма доказана.

В дальнейшем S — группа над полем порядка p^β. В силу леммы 5.2 можно считать, что S не является группой типа A_1.

Обозначим через $e(p,S)$ и $e(p,S)'$ множества

$$\{e(r,p^\beta) \mid r \in \pi(S) \setminus \{p\}, pr \notin \omega(S)\}$$

и

$$\{e(r,p^\beta) \mid r \in \pi(S) \setminus \{2,3,p\}, pr \notin \omega(S)\}$$

соответственно. Отметим, что для всех групп S, кроме групп типа A_2 и ${}^2A_2$, множества $e(p,S)$ и $e(p,S)'$ совпадают. В силу п. (1) леммы 5.3 для любого e из $e(p,S)$ выполнено неравенство $e\beta \leq 2n\alpha$.

Предположим, что L — одна из групп $B_n(q)$ и $C_n(q)$, где n четно. Множество простых чисел, не смежных с p в $GK(L)$, совпадает с множеством чисел, не смежных с 2 в $GK(L)$, и равно множеству делителей числа $k_{2n}(q)$. Выберем среди этих делителей число r_{2n}, удовлетворяющее не только условию $e(r_{2n}, p^\alpha) = 2n$, но и более сильному условию $e(r_{2n}, p) = 2n\alpha$. Другими словами, r_{2n} имеет вид $r_{2n\alpha}(p)$. Поскольку $L \neq B_3(2)$, такое число существует. По лемме 5.1 число r_{2n} лежит в $\pi(S)$. Кроме того, $r_{2n} > 3$. Значит, если $e = e(r_{2n}, p^\beta)$, то $e \in e(p,S)'$. По определению примитивного делителя $e\beta$ делится на $2n\alpha$. С другой стороны, $e\beta \leq 2n\alpha$ в силу п. (1) леммы 5.3. Таким образом, получаем уравнение $e\beta = 2n\alpha$, где e — максимальный элемент в $e(p,S)'$.

Предположим, что L — одна из групп $B_n(q)$ и $C_n(q)$, где n нечетно. Тогда $t(p,L) = 3$. Поскольку $L \notin \{B_3(2), B_3(4)\}$, существуют примитивные простые делители $r_{2n} = r_{2n\alpha}(p)$ и $r_n = r_{n\alpha}(p)$. Оба этих числа не смежны с p в $GK(L)$, поэтому по лемме 5.1 делят порядок группы S. Положим $e_2 = e(r_{2n}, p^\beta)$ и $e_1 = e(r_n, p^\beta)$. Тогда $e_2, e_1 \in e(p, S)'$, причем если S отлична от групп Ри и Сузуки, то $e_2 \neq e_1$. По определению примитивного делителя $e_2\beta$ делится на $2n\alpha$. С другой стороны, $e_2\beta \leq 2n\alpha$. Значит, $e_2\beta = 2n\alpha$. Точно так же $e_1\beta$ делится на $n\alpha$ и $e_1\beta \leq 2n\alpha$, откуда $e_1\beta \in \{n\alpha, 2n\alpha\}$. Таким образом, получаем уравнение $2n\alpha = e_2\beta$, где e_2 — максимальный элемент в $e(p, S)'$, и условие $n\alpha \in \{e_1\beta, e_1\beta/2\}$, где e_1 — некоторый элемент в $e(p, S)'$. Если S отлична от групп Ри и Сузуки, то условие превращается в уравнение $n\alpha = e_1\beta$, в частности, $e_2/e_1 = 2$.

Предположим, что $L = D_n(q)$, где n четно. Поскольку $L \notin \{D_4(2), D_4(4)\}$, существуют примитивные простые делители $r_{2(n-1)} = r_{2(n-1)\alpha}(p)$ и $r_{n-1} = r_{(n-1)\alpha}(p)$. Повторяя предыдущее рассуждение и полагая $e_2 = e(r_{2(n-1)}, p^\beta)$, $e_1 = e(r_{n-1}, p^\beta)$, получаем, что $e_2, e_1 \in e(p, S)'$ и $e_2\beta = 2(n-1)\alpha$. Более того, если S отлична от групп Ри и Сузуки, то $e_1\beta = (n-1)\alpha$, в частности, $e_2/e_1 = 2$.

Предположим, что $L = D_n(q)$, где n нечетно. Тогда существуют примитивные простые делители $r_{2(n-1)} = r_{2(n-1)\alpha}(p)$ и $r_n = r_{n\alpha}(p)$. Полагая $e_2 = e(r_{2(n-1)}, p^\beta)$ и $e_1 = e(r_n, p^\beta)$, получаем, что $e_2, e_1 \in e(p, S)'$ и $e_2\beta = 2(n-1)\alpha$. Кроме того, $e_1\beta$ делится на $n\alpha$ и не превосходит $2(n-1)\alpha$. Значит, $e_1\beta = n\alpha$, в частности, $e_2/e_1 = 2(n-1)/n < 2$.

Предположим, что $L = {}^2D_n(q)$, где n нечетно. Тогда существуют примитивные простые делители $r_{2n} = r_{2n\alpha}(p)$ и $r_{2(n-1)} = r_{2(n-1)\alpha}(p)$. Полагая $e_2 = e(r_{2n}, p^\beta)$ и $e_1 = e(r_{2(n-1)}, p^\beta)$, получаем, что $e_2, e_1 \in e(p, S)'$ и $e_2\beta = 2n\alpha$. Кроме того, $e_1\beta$ делится на $2(n-1)\alpha$ и не превосходит $2n\alpha$. Значит, $e_1\beta = 2(n-1)\alpha$, в частности, $e_2/e_1 = n/(n-1) < 2$.

Предположим, наконец, что $L = {}^2D_n(q)$, где n четно. Тогда $t(p, L) = 4$. По лемме 5.1 получаем, что $t(p, S) \geq 4$. Значит, S изоморфна одной из групп ${}^2D_m(p^\beta)$, где m четно, $E_8(p^\beta)$, $E_7(p^\beta)$, $E_6(p^\beta)$ или одной из групп Ри и Сузуки. Поскольку $L \notin \{{}^2D_4(2), {}^2D_4(4)\}$, существуют делители $r_{2n} = r_{2n\alpha}(p)$, $r_{2(n-1)} = r_{2(n-1)\alpha}(p)$ и $r_n = r_{(n-1)\alpha}(p)$. Положим $e_2 = e(r_{2n}, p^\beta)$, $e_1 = e(r_{2(n-1)}, p^\beta)$ и $e_0 = e(r_n, p^\beta)$. Тогда $\{e_2, e_1, e_0\} \subseteq e(p, S)'$, причем $e_2\beta = 2n\alpha$ и $e_1\beta = 2(n-1)\alpha$, в частности, $e_2/e_1 = n/(n-1) < 2$.

Дальнейшее доказательство состоит в последовательном рассмотрении в качестве S всех простых групп лиева типа. Если есть пп. (а) и (б), то в п. (а) рассматривается случай $L = B_n(q)$ или $L = C_n(q)$, где n четно, а в п. (б) — оставшиеся случаи.

1. Пусть $S \simeq A_{m-1}(p^\beta)$, где $m \geq 3$. Тогда $e(p, S) = \{m, m-1\}$ при $m \neq 3$ и $m \in e(p, S)' \subseteq \{m, m-1\}$ при $m = 3$.

(а) Напомним, что e — максимальный элемент в $e(p, S)'$ и $e\beta = 2n\alpha$. Значит, $e = m$ и $m\beta = 2n\alpha$. В частности, $(m-1)\beta > 2$.

Допустим, что $m > n$. Тогда $\beta < 2\alpha$ и тем самым

$$2(n-1)\alpha < (m-1)\beta < 2n\alpha.$$

Следовательно, $(m-1)\beta$ не делит ни одного из чисел $2i\alpha$, где $i \in \{1, 2, \ldots, n\}$. С другой стороны, в S есть циклический тор порядка $(p^{(m-1)\beta} - 1)/(m, p^\beta - 1)$ (см., например, [33, теорема 2.1]), и, значит, $k_{(m-1)\beta}(p) \in \omega(S)$. Получаем противоречие с п. (2) леммы 5.3, если пара $((m-1)\beta, p)$ не равна $(6, 2)$. Пусть $((m-1)\beta, p) = (6, 2)$. С учетом уравнения $m\beta = 2n\alpha$ получаем, что $m = 4$,

$\beta = 2$ и $n = 2$, $\alpha = 2$. Таким образом, $S \simeq A_3(4)$ и $L = B_2(4)$. В этом случае $7 \in \omega(S) \setminus \omega(L)$, что невозможно.

Пусть $m \leq n$. Тогда $n \geq 4$ и, поскольку $L \neq B_4(2)$, в $GK(L)$ есть коклика размера 4, не содержащая ни p, ни 2, ни 3 [23, табл. 3]. Другими словами, $t(GK(L) \setminus \{p, 2, 3\}) \geq 4$. По п. (2) леммы 1.3 выполнено $t(GK(S) \setminus \{p, 2, 3\}) \geq 3$, откуда в силу [23, табл. 2] следует, что $m \geq 5$. Таким образом, $n \geq m \geq 5$. Тогда $t(L) - 1 \geq (3n + 2)/4 - 1 > (m + 1)/2 \geq t(S)$, что невозможно.

(б) Напомним, что $e_2, e_1 \in e(p, S)'$ и $e_2 > e_1$. Значит, $e_2/e_1 = m/(m - 1)$. Если $e_2/e_1 = 2$, то $m = 2$; противоречие. Если $e_2/e_1 = 2(n - 1)/n$, где $n \geq 5$ нечетно, то $m = 2(n - 1)/(n - 2)$, откуда $n = 3$; противоречие.

Пусть $e_2/e_1 = n/(n - 1)$, где $n \geq 5$ нечетно. Тогда $m = n$ и $\beta = 2\alpha$. Значит, $L = {}^2D_n(q)$ и $S \simeq A_{n-1}(q^2)$. В этом случае $r_n(q) \in \pi(S) \setminus \pi(L)$; противоречие.

2. Пусть $S \simeq {}^2A_{m-1}(p^\beta)$, где $m \geq 3$. Тогда $e(p, S)'$ — одно из множеств $\{2m - 2, m\}$, $\{2m - 2, m/2\}$ при четном m и одно из множеств $\{2m, m - 1\}$, $\{2m, (m - 1)/2\}$ при нечетном $m \neq 3$. Если $m = 3$, то $2m \in e(p, S)' \subseteq \{2m, (m - 1)/2\}$.

(а) Поскольку e — максимальный элемент в $e(p, S)'$, получаем, что $2(m - 1)\beta = 2n\alpha$ при четном m и $2m\beta = 2n\alpha$ при нечетном m.

Рассмотрим случай четного m. Пусть $m - 1 > n$. Тогда $\beta < \alpha$ и, значит, $n\alpha < m\beta < (n + 1)\alpha$. Следовательно, $m\beta$ не делит ни одного из чисел $2i\alpha$, где $i \in \{1, 2, \dots, n\}$. С другой стороны, $k_{m\beta}(p) \in \pi(S)$. Если $((m - 1)\beta, p) \neq (6, 2)$, получаем противоречие с п. (2) леммы 5.3. Если $m\beta = 6$, то $m = 6$, $\beta = 1$, откуда $n = 5$, но n четно; противоречие.

Пусть $m - 1 \leq n$. Так как $m \geq 4$, то $n \geq 4$. Значит, $t(GK(L) \setminus \{2, 3, p\}) \geq 4$, следовательно, $t(GK(S) \setminus \{2, 3, p\}) \geq 3$, откуда $m \geq 5$. Учитывая четность m, получаем, что $n \geq m \geq 6$. Как и в случае линейных групп, эти неравенства приводят к тому, что $t(S) < t(L) - 1$; противоречие.

Теперь рассмотрим случай, когда m нечетно. Пусть $m > n$. Тогда $\beta < \alpha$ и, значит, выполнены неравенства

$$(n-1)\alpha < (m-1)\beta < n\alpha,\ 2(n-1)\alpha < 2(m-1)\beta < 2n\alpha,\ 2n\alpha \leq 4(n-1)\alpha < 4(m-1)\beta.$$

С другой стороны, $k_{(m-1)\beta} \in \omega(S)$, и поскольку $m\beta = n\alpha$ четно, то β четно, так что $(m - 1)\beta \neq 6$. По п. (2) леммы 5.3 некоторое кратное числа $(m - 1)\beta$ совпадает с $2i\alpha$, где $i \in \{1, \dots, n\}$. В силу предыдущих неравенств этим кратным может быть только $3(m-1)\beta$ и оно равно $2n\alpha$, поскольку превосходит $2(n-1)\alpha$. Следовательно, $2n\alpha = 3(m - 1)\beta > 3(n - 1)\alpha$. Значит, $n = 2$, $m = 3$ и $\beta = 3\alpha/2$. Таким образом, $L = B_2(q)$ и $S \simeq {}^2A_2(q^{2/3})$. Графы простых чисел групп $B_2(q)$ и ${}^2A_2(q^{2/3})$ имеют по две компоненты связности, и по теореме Грюнберга — Кегеля выполнено равенство

$$\frac{q^2 + 1}{(2, q - 1)} = n_2(B_2(q)) = n_2({}^2A_2(q^{2/3})) = \frac{q^2 + 1}{(q^{2/3} + 1)(3, q^{2/3} + 1)};$$

противоречие.

Пусть $m \leq n$. Тогда $n \geq 4$ и $t(GK(L) \setminus \{2, 3, p\}) \geq 4$, следовательно, $t(GK(S) \setminus \{2, 3, p\}) \geq 3$, откуда $m \geq 5$ и $n \geq 6$. Тогда $t(L) - 1 > t(S)$; противоречие.

(б) Напомним, что $e_2, e_1 \in e(p, S)'$ и $e_2/e_1 \leq 2$. Поскольку $2(m - 1)/m < 2$ и каждое из чисел $2m/(m - 1)$, $4(m - 1)/m$, $4m/(m - 1)$ больше двух, $e_2/e_1 = 2(m - 1)/m$ и m четно. Если $e_2/e_1 = 2(n - 1)/n$, где n нечетно, то $m = n$;

противоречие с четностью числа m. Если $e_2/e_1 = n/(n-1)$, где $n \geq 4$ нечетно, то $m = 2(n-1)/(n-2)$, откуда $n = 3$; противоречие.

3. Пусть $S \simeq B_m(p^\beta)$ или $S \simeq C_m(p^\beta)$. Если m четно, то $e(p,S) = \{2m\}$. Если m нечетно, то $e(p,S) = \{2m, m\}$.

(а) Имеем $e = 2m$ и $m\beta = n\alpha$. Этот уравнение будет рассмотрено в п. (б).

(б) Поскольку $t(p,S) \geq t(p,L) > 2$, число m нечетно и $e(p,S) = \{2m, m\}$. Следовательно, $e_2/e_1 = 2$ и, значит, либо $L = D_n(q)$, где n четно, либо $L \in \{B_n(q), C_n(q)\}$, где n нечетно.

Предположим, что $L = D_n(q)$, где n четно. Тогда $m\beta = (n-1)\alpha$. Заметим, что $k_{2(m-1)\beta}(p) \in \omega(S)$, причем, поскольку m нечетно, $2(m-1)\beta \neq 6$.

Пусть $m > n-1$. Тогда $\beta < \alpha$, тем самым

$$n\alpha \leq 2(n-2)\alpha < 2(m-1)\beta < 2(n-1)\alpha;$$

противоречие с п. (2) леммы 5.3. Значит, $m \leq n-1$. Кроме того, из неравенства

$$(3m+5)/4 \geq t(S) \geq t(L) - 1 \geq (3n-2)/4 - 1$$

следует, что $m \geq n-3$. Таким образом, $m \in \{n-1, n-2, n-3\}$. Более того, так как n четно и m нечетно, $m \in \{n-1, n-3\}$.

Пусть $m = n-3$. Тогда $n \geq 6$ и $(n-3)\beta = (n-1)\alpha$. Обозначим $\beta/(n-1) = \alpha/(n-3)$ через γ. По п. (2) леммы 5.3 число $2(m-1)\beta = 2(n-4)(n-1)\gamma$ должно делить $2i\alpha = 2i(n-3)\gamma$ для некоторого $1 \leq i \leq n-1$. Это возможно только при $i = n-1$. Значит, $n-4$ делит $n-3$, что при $n \geq 6$ невозможно.

Если $m = n-1$, то $\beta = \alpha$ и $S \in \{B_{n-1}(q), C_{n-1}(q)\}$, как и утверждается в п. (4) доказываемой теоремы.

Предположим, что $L \in \{B_n(q), C_n(q)\}$, где n нечетно. Тогда $m\beta = n\alpha$. Таким образом, в случае $L \in \{B_n(q), C_n(q)\}$ при любом n выполнено равенство $m\beta = n\alpha$, причем если n нечетно, то и m нечетно. Будем вести рассуждения одновременно для четных и нечетных n, предположив пока, что $(2(m-1)\beta, p) \neq (6, 2)$.

Пусть $m > n$. Тогда $\beta < \alpha$ и, значит,

$$n\alpha \leq 2(n-1)\alpha < 2(m-1)\beta < 2n\alpha.$$

Следовательно, $2(m-1)\beta$ не делит ни одного из чисел $2i\alpha$, где $i \in \{1, 2, \dots, n\}$. С другой стороны, $k_{2(m-1)\beta}(p) \in \omega(S)$; противоречие. Значит, $m \leq n$. Из неравенства $(3m+5)/4 \geq t(S) \geq t(L) - 1 \geq (3n+2)/4 - 1$ следует, что $m \geq n-2$. Таким образом, $m \in \{n, n-1, n-2\}$.

Пусть $m = n-1$. Тогда $n \geq 3$ и $(n-1)\beta = n\alpha$. Обозначим $\beta/n = \alpha/(n-1)$ через γ. По п. (2) леммы 5.3 число $2(m-1)\beta = 2(n-2)n\gamma$ должно делить $2i\alpha = 2i(n-1)\gamma$ для некоторого $i \in \{1, 2, \dots, n\}$. Это возможно только при $i = n$. Значит, $n-2$ делит $n-1$, откуда $n = 3$. Тогда m нечетно, но $m = 2$; противоречие.

Пусть $m = n-2$. Тогда $n \geq 4$ и $(n-2)\beta = n\alpha$. Повторяя предыдущее рассуждение с показателем $2(m-1)\beta$, приходим к тому, что $n = 4$, $m = 2$ и $\beta = 2\alpha$. Таким образом, $L \in \{B_4(q), C_4(q)\}$ и $S \simeq B_2(q^2)$. Тогда $t(S) = 2$, неплотность же группы L при $q > 2$ равна 4; противоречие.

Если $m = n$, то $\alpha = \beta$ и $S \in \{B_n(q), C_n(q)\}$, как и утверждается в п. (3) доказываемой теоремы.

Осталось рассмотреть случай, когда $(2(m-1)\beta, p) = (6, 2)$. В этом случае либо $m = 2$ и $\beta = 3$, либо $m = 4$ и $\beta = 1$. Значит, n четно. Теперь из уравнения

$m\beta = n\alpha$ следует, что либо $S \simeq L$, как и требуется, либо $S \simeq B_4(2)$ и $L = B_2(4)$. Последнее невозможно, так как $7 \in \omega(B_4(2)) \setminus \omega(B_2(4))$.

4. Пусть $S \simeq D_m(p^\beta)$. Тогда $e(p,S) = \{2m-2, m-1\}$ при четном m и $e(p,S) = \{2m-2, m\}$ при нечетном m.

(а) Имеем $e = 2m-2$ и, значит, $(m-1)\beta = n\alpha$. Это уравнение будет рассмотрено в п. (б).

(б) Пусть m нечетно. Тогда $e_2/e_1 = 2(m-1)/m < 2$, поэтому либо $e_2/e_1 = n/(n-1)$, либо $e_2/e_1 = 2(n-1)/n$. В первом случае $m = 2(n-1)/(n-2) < 4$, что невозможно; во втором случае $L \simeq D_n(q)$ и $m = n$, $\beta = \alpha$, тем самым $S \simeq L$, как и требуется. Таким образом, можно считать, что m четно и $e_2/e_1 = 2$, поэтому либо $L = D_n(q)$, где n четно, либо $L \in \{B_n(q), C_n(q)\}$, где n нечетно.

Предположим, что $L = D_n(q)$, где n четно. Тогда $(m-1)\beta = (n-1)\alpha$. Заметим, что $k_{2(m-2)\beta}(p) \in \omega(S)$, причем, поскольку m четно, $2(m-2)\beta \neq 6$.

Пусть $m > n$. Тогда $\beta < \alpha$ и

$$n\alpha \leq 2(n-2)\alpha < 2(m-2)\beta < 2(n-1)\alpha;$$

противоречие с п. (2) леммы 5.3. Таким образом, $m \leq n$. С другой стороны, из неравенства

$$(3m+1)/4 \geq t(S) \geq t(L) - 1 \geq (3n-2)/4 - 1$$

следует, что $m \geq n-2$. Таким образом, $m \in \{n, n-1, n-2\}$. Более того, так n и m четны, $m \in \{n, n-2\}$.

Пусть $m = n-2$. Тогда $n \geq 6$ и $(n-3)\beta = (n-1)\alpha$. Обозначим $\beta/(n-1) = \alpha/(n-3)$ через γ. По п. (2) леммы 5.3 число $2(m-2)\beta = 2(n-4)(n-1)\gamma$ должно делить $2i\alpha = 2i(n-3)\gamma$ для некоторого $1 \leq i \leq n-1$. Это возможно только при $i = n-1$. Значит, $n-4$ делит $n-3$, что при $n \geq 6$ невозможно.

Если $m = n$, то $\beta = \alpha$ и, значит, $S \simeq L$, как и требуется.

Предположим, что $L \in \{B_n(q), C_n(q)\}$, где n нечетно. Тогда $(m-1)\beta = n\alpha$. Значит, в случае $L \in \{B_n(q), C_n(q)\}$ при любом n выполнено равенство $(m-1)\beta = n\alpha$. При этом если n нечетно, то m четно. Будем вести рассуждения одновременно для четных и нечетных n, предположив пока, что $(2(m-2)\beta, p) \neq (6,2)$.

Пусть $m-1 > n$. Тогда $\beta < \alpha$ и тем самым

$$n\alpha \leq 2(n-1)\alpha < 2(m-2)\beta < 2n\alpha;$$

противоречие с п. (2) леммы 5.3. Таким образом, $m-1 \leq n$. Кроме того, из неравенства

$$(3m+1)/4 \geq t(S) \geq t(L) - 1 \geq (3n+2)/4 - 1$$

следует, что $m \geq n-1$. Таким образом, $m \in \{n+1, n, n-1\}$.

Пусть $m = n$. Тогда $n \geq 4$ и $(n-1)\beta = n\alpha$. Обозначим $\beta/n = \alpha/(n-1)$ через γ. По п. (2) леммы 5.3 число $2(m-2)\beta = 2(n-2)n\gamma$ должно делить $2i\alpha = 2i(n-1)\gamma$ для некоторого $1 \leq i \leq n$. Это возможно только при $i = n$. Значит, $n-2$ делит $n-1$, откуда $n = 3$, однако $n \geq 4$; противоречие.

Пусть $m = n-1$. Тогда $n \geq 5$ и $(n-2)\beta = n\alpha$. Повторяя рассуждение с показателем $2(m-2)\beta$, приходим к тому, что $n = 4$ и $m = 3$; противоречие.

Пусть $m = n+1$. Тогда $\alpha = \beta$ и, значит, $S \simeq D_{n+1}(q)$. Если $n = 3$, то $S \simeq D_4(q)$ и $L \in \{B_3(q), C_3(q)\}$, как и утверждается в п. (2) доказываемой теоремы. Для $n > 3$ покажем, что $\pi(S) \nsubseteq \pi(L)$, тем самым будет достигнуто противоречие. Если n четно, то $r_{n+1}(q) \in \pi(S) \setminus \pi(L)$. Пусть $n \geq 5$ нечетно и

$S \not\simeq D_8(2)$. Тогда в группе S есть элемент порядка $r_{n+3}(q)r_{n-1}(q)$. С другой стороны, $\eta(n+3)+\eta(n-1)=n+1>n$ и $1<\eta(n+3)/\eta(n-1)=(n+3)/(n-1)\leq 2$, поэтому в силу критерия смежности [23, предложение 2.4] имеем $r_{n+3}(q)r_{n-1}(q)\notin\omega(L)$. Если $S\simeq D_8(2)$, то $L\simeq B_7(2)$ и $99\in\omega(S)\setminus\omega(L)$ (см. [33]).

Осталось рассмотреть случай, когда $(2(m-2)\beta,p)=(6,2)$. В этом случае $m=5$ и $\beta=1$ и $S\simeq D_5(2)$. Из уравнения $(m-1)\beta=n\alpha$ следует, что $L\in\{B_2(4),B_4(2)\}$. Поскольку $31\in\pi(S)\setminus\pi(L)$, получаем противоречие.

5. Пусть $S\simeq {}^2D_m(p^\beta)$. Тогда $e(p,S)=\{2m,2m-2,m-1\}$ при четном m и $e(p,S)=\{2m,2m-2\}$ при нечетном m.

(а) Имеем $e=2m$ и $m\beta=n\alpha$. Повторяя соответствующее рассуждение из п. 3(б), приходим к тому, что либо $L\in\{B_n(q),C_n(q)\}$, как и утверждается в п. (3) теоремы, либо $L=B_2(4)$ и $S\simeq {}^2D_4(2)$. В последнем случае $7\in\omega(S)\setminus\omega(L)$, что невозможно.

(б) Поскольку e_2 — максимальный элемент в $e(p,S)$, имеем $e_2=2m$. Кроме того, $e_2/e_1\neq 2m/(m-1)$, поскольку $e_2/e_1\leq 2$. Значит, $e_2/e_1=m/(m-1)<2$. Если $e_2/e_1=2(n-1)/n$, то $m=2(n-1)/(n-2)<3$, что невозможно. Если $e_2/e_1=n/(n-1)$, то $L={}^2D_n(q)$, $m=n$, $\beta=\alpha$ и $S\simeq L$, как и требуется.

6. Пусть $S\simeq E_8(p^\beta)$. Тогда $e(p,S)=\{30,24,20,15\}$. Кроме того, из неравенства $(3n-2)/4\leq t(L)\leq t(S)+1=13$ следует, что $n\leq 18$.

(а) Поскольку $e=30$, получаем, что $15\beta=n\alpha$. Это уравнение будет рассмотрено в п. (б).

(б) Пусть $e_2/e_1=30/24=5/4$. Тогда $e_2/e_1=n/(n-1)$ и $30\beta=2n\alpha$, откуда $n=5$ и $3\beta=\alpha$. Получаем, что $S\simeq E_8(q^{1/3})$ и $L={}^2D_5(q)$. В этом случае, $r_{5\alpha}(p)\in\omega(S)\setminus\omega(L)$; противоречие. Если $e_2/e_1=30/20$, то уравнение $e_2/e_1=n/n-1$ не имеет решений, больших 3, а уравнение $e_2/e_1=2(n-1)/n$ не имеет нечетных решений, больших 3, но в этих случаях $n\geq 4$. Значит, $e_1=15$ и $e_2/e_1=2$.

Предположим, что $L\in\{B_n(q),C_n(q)\}$, где n нечетно. Тогда $15\beta=n\alpha$. Таким образом, это уравнение выполнено независимо от четности n. Из него следует, что $24\beta=8n\alpha/5$ и $20\beta=4n\alpha/3$. По п. (2) леммы 5.3 найдутся $i,j\in\{1,\dots,n\}$ такие, что $8n\alpha/5\mid 2i\alpha$ и $4n\alpha/3\mid 2j\alpha$, поэтому n делится на 5 и на 3. Значит, $n=15$ и $\beta=\alpha$.

Предположим, что $L=D_n(q)$, где n четно. Тогда $15\beta=(n-1)\alpha$. Аналогично предыдущему случаю получаем, что $n-1$ делится на 5 и на 3. Значит, $n=16$ и $\beta=\alpha$.

Таким образом, $L\in\{B_{15}(q),C_{15}(q),D_{16}(q)\}$ и $S\simeq E_8(q)$. По лемме 2.2 хотя бы одно из чисел $r_{13}(q)$ и $r_{26}(q)$ должно принадлежать $\omega(S)$, но это неверно.

7. Пусть $S\simeq E_7(p^\beta)$. Тогда $e(p,S)=\{18,14,9,7\}$. Кроме того, из неравенства $(3n-2)/4\leq t(L)\leq t(S)+1=9$ следует, что $n\leq 12$. В п. (а) получаем, что $e=18$ и $9\beta=n\alpha$. В п. (б), как несложно проверить, $e_2/e_1\notin\{18/14,18/7\}$, поэтому $e_1=9$ и $e_2/e_1=2$.

Предположим, что $L\in\{B_n(q),C_n(q)\}$. Тогда $9\beta=n\alpha$. Значит, $14\beta=14n\alpha/9$. Следовательно, найдется $i\in\{1,\dots,n\}$ такое, что $14n\alpha/9\mid 2i\alpha$. Поскольку i должно делиться на 7 и $n\leq 12$, то $i=7$. Тогда $n=9$ и $\beta=\alpha$.

Предположим, что $L=D_n(q)$, где n четно. Тогда $9\beta=(n-1)\alpha$. Так же, как в предыдущем случае, получаем, что $n-1=9$ и $\beta=\alpha$.

Таким образом, $L\in\{B_9(q),\ C_9(q),D_{10}(q)\}$ и $S\simeq E_7(q)$. Тогда $r=r_{16}(q)\in\pi(L)\setminus\pi(S)$. Отметим, что $r\geq 17$ и r не смежен в $GK(G)$ ни с одним из чисел

$r_5(q)$, $r_9(q)$ и $r_{18}(q)$.

Пусть $r \in \pi(\overline{G}/S)$. Тогда G содержит полевой автоморфизм группы S порядка r. Централизатор этого автоморфизма в группе S содержит элемент порядка q_0^5-1, где $q = q_0^r$. В силу взаимной простоты чисел r и 5 если $s = r_5(q_0)$, то $e(s,q) = 5$, поэтому $rs \in \omega(G) \setminus \omega(L)$; противоречие.

Пусть $r \in \pi(K)$. Числа r, $r_9(q)$ и $r_{18}(q)$ образуют коклику в $GK(G)$, поэтому $r_9(q), r_{18}(q) \in \pi(S)\setminus\pi(K)$. Кроме того, окрестности вершин $r_9(q)$ и $r_{18}(q)$ в графе $GK(G)$ не пересекаются. В группе S есть подгруппа, изоморфная группе типа $A_6(q)$, следовательно, есть подгруппа, изоморфная $GL_6(q)$. Значит, в S есть подгруппа Фробениуса с ядром порядка q^5 и циклическим дополнением порядка q^5-1. По [29, лемма 3] получаем, что $r(q^5-1) \in \omega(G) \setminus \omega(L)$; противоречие.

8. Пусть S изоморфна одной из групп $E_6(p^\beta)$, $F_4(p^\beta)$ и ${}^3D_4(p^\beta)$. Тогда

$$\{12\} \subseteq e(p,S) \subseteq \{12,9,8\}.$$

Из неравенства $(3n-2)/4 \le t(L) \le t(S)+1 \le 6$ следует, что $n \le 8$.

(а) Поскольку $e = 12$, получаем, что $6\beta = n\alpha$. Тогда $9\beta = 3n\alpha/2$ и $8\beta = 4n\alpha/3$. Найдутся $i,j \in \{1,\dots,n\}$ такие, что $3n\alpha/2 \mid 2i\alpha$ и $4n\alpha/3 \mid 2j\alpha$, поэтому n делится на 4 и на 3; противоречие.

(б) Как несложно проверить, $e_2/e_1 \ne 12/8$. Следовательно, $e_2/e_1 = 12/9$. Тогда $e_2/e_1 = n/(n-1)$ и $6\beta = n\alpha$, откуда $n = 4$ и $\beta = 2\alpha/3$. Значит, $S \simeq E_6(q^{2/3})$ и $L = {}^2D_4(q)$. В этом случае $r_{5\beta}(p) \in \pi(S) \setminus \pi(L)$; противоречие.

9. Пусть $S \simeq {}^2E_6(p^\beta)$. Тогда $e(p,S) = \{18,12,8\}$. Как и в предыдущем случае, $n \le 8$.

(а) Поскольку $e = 18$, получаем, что $9\beta = n\alpha$. Тогда $12\beta = 4n\alpha/3$ и $8\beta = 8n\alpha/9$. Найдутся $i,j \in \{1,\dots,n\}$ такие, что $4n\alpha/3 \mid 2i\alpha$ и $8n\alpha/9 \mid 2j\alpha$, что при $n \le 8$ невозможно.

(б) Как несложно проверить, e_2/e_1 не может лежать в $\{18/12, 18/8\}$.

10. Пусть $S \simeq G_2(p^\beta)$. Тогда $e(p,S) = \{6,3\}$. Значит, $e = 6$ и $e_2/e_1 = 2$. Из неравенства $(3n-2)/4 \le t(L) \le t(S)+1 = 4$ следует, что $n \le 6$.

Предположим, что $L \in \{B_n(q), C_n(q)\}$. Тогда $3\beta = n\alpha$. Если $n = 2,4$, то граф $GK(L)$ несвязен. По теореме Грюнберга — Кегеля получаем уравнение

$$(q^n+1)/(2,q-1) = p^{2\beta} \pm p^\beta + 1,$$

откуда либо $2^{n\alpha} = 2^\beta(2^\beta \pm 1)$, либо $q^n = 2p^{2\beta} \pm 2p^\beta + 1$; оба эти равенства невозможны. Если $n \ge 5$ и $(n,q) \ne (5,2)$, то $t(GK(L)) \ge 5$; противоречие с тем, что $t(GK(S)) = 3$. Если $(n,q) = (5,2)$, то $n\alpha$ не делится на 3; противоречие с уравнением $3\beta = n\alpha$. Если $n = 3$, то $\beta = \alpha$ и $S \simeq G_2(q)$, как и утверждается в п. (2) доказываемой теоремы.

Предположим, что $L = D_n(q)$, где n четно. Тогда $3\beta = (n-1)\alpha$. Если $n = 4$, то $S \simeq G_2(q)$, как и утверждается в п. (2).

Пусть $n = 6$. Тогда $\beta = 5\alpha/3$. В частности, $\alpha \ge 3$. По лемме 2.2 хотя бы одно из чисел $k_8(q) = (q^4+1)/(2,q-1)$ и $k_3(q) = (q^2+q+1)/(3,q-1)$ должно лежать в $\omega(S)$, но ни одно из этих чисел не делит $|S|_{p'} = (q^{10}-1)(q^{10/3}-1)$; противоречие.

Осталось рассмотреть случай, когда S — простая группа Ри или Сузуки. В этих группах в отличие от предыдущих не смежные между собой и не смежные с p в $GK(S)$ числа r могут иметь одинаковые показатели $e(r,p^\beta)$, поэтому e_2 и e_1 могут быть равны.

11. Пусть $S \simeq {}^2F_4(2^\beta)$, где $\beta \geq 3$ нечетно. Тогда $e(2,S) = \{12,6\}$. Значит, $e = e_2 = 12$ и $e_2/e_1 \in \{2,1\}$.

Предположим, что $L = D_n(q)$, где n нечетно. Тогда $e_2/e_1 = 2(n-1)/n$; противоречие, так как при $n \geq 4$ имеем $1 < 2(n-1)/n < 2$. Аналогичным образом доказывается, что $L \neq {}^2D_n(q)$.

Предположим, что $L = B_n(q)$. Тогда $6\beta = n\alpha$. Из неравенства $t(L) \leq t(S) + 1 \leq 6$ следует, что $n \leq 7$.

Пусть $n \in \{2,4\}$. Тогда граф $GK(L)$ несвязен и по теореме Грюнберга — Кегеля получаем равенство

$$2^{n\alpha} + 1 = n_2(L) = 2^{2\beta} \pm 2^{(3\beta+1)/2} + 2^\beta \pm 2^{(\beta+1)/2} + 1,$$

откуда $2^{6\beta} = 2^{(\beta+1)/2}(2^{(3\beta-1)/2} \pm 2^\beta + 2^{(\beta-1)/2} \pm 1)$; противоречие.

Если $n = 3$, то $\beta = \alpha/2$, в частности, α четно. Значит, $S \simeq {}^2F_4(q^{1/2})$ и $L = B_3(q)$. По лемме 2.2 хотя бы одно из чисел $k_2(q) = q^2 + 1$ и $k_3(q) = (q^2+q+1)/3$ должно лежать в $\omega(S)$, но ни одно из этих чисел не делит $|S|_{2'} = (q^3+1)(q^2-1)(q^{3/2}+1)(q^{1/2}-1)$; противоречие.

Пусть $n \in \{5,6,7\}$. По лемме 2.2 хотя бы одно из чисел $r_{(n-1)\alpha}(2)$ и $r_{2(n-1)\alpha}(2)$ должно лежать в $\omega(S)$, но, как несложно проверить, это неверно.

Предположим, что $L = D_n(q)$, где n четно. Тогда $6\beta = (n-1)\alpha$. Из неравенства $t(L) \leq t(S)+1 \leq 6$ следует, что $n \leq 8$. Случай $L = D_4(q)$ аналогичен случаю $L = B_3(q)$, а случай $L \in \{D_6(q), D_8(q)\}$ — случаю $L \in \{B_5(q), B_7(q)\}$.

12. Пусть $S \simeq {}^2B_2(2^\beta)$, где $\beta \geq 3$ нечетно. Тогда $e(2,S) = \{4,1\}$. Значит, $e = e_2 = 4$ и $e_2/e_1 \in \{4,1\}$. Так же, как и в предыдущем случае, показывается, что $L \neq D_n(q)$, где n нечетно, и $L \neq {}^2D_n(q)$.

Предположим, что $L = B_n(q)$. Тогда $2\beta = n\alpha$. Из неравенства $t(L) \leq t(S) + 1 \leq 5$ следует, что $n \leq 6$. Если $n \in \{5,6\}$, то $t(GK(L) \setminus \{2\}) = 5$, а $t(GK(S) \setminus \{2\}) = 3$; противоречие.

Пусть $n \in \{2,4\}$. Тогда граф $GK(L)$ несвязен и по теореме Грюнберга–Кегеля получаем одно из равенств

$$2^{n\alpha} + 1 = 2^\beta - 1,$$

$$2^{n\alpha} + 1 = 2^\beta \pm 2^{(\beta+1)/2} + 1.$$

Первое равенство очевидно невозможно; второе приводит к равенству $2^{2\beta} = 2^{(\beta+1)/2}(2^{(\beta-1)/2} \pm 1)$, которое тоже неверно.

Пусть $n = 3$. Тогда $\beta = 3\alpha/2$, в частности, α четно. Значит, $S \simeq {}^2B_2(q^{3/2})$ и $L = B_3(q)$. По лемме 2.2 хотя бы одно из чисел $k_4(q) = q^2 + 1$ и $k_3(q) = (q^2+q+1)/3$ должно лежать в $\omega(S)$. Поскольку $q > 4$ в силу лемм 2.3 и 2.4, ни одно из этих чисел не делит $|S|_{2'} = (q^3+1)(q^{3/2}-1)$; противоречие.

Предположим, что $L = D_n(q)$, где n четно. Тогда $2\beta = (n-1)\alpha$. Из неравенства $t(L) \leq t(S)+1 \leq 5$ следует, что $n \leq 6$. Случай $L = D_4(q)$ аналогичен случаю $L = B_3(q)$.

Пусть $n = 6$. Тогда $\beta = 5\alpha/2$. Значит, $S \simeq {}^2B_2(q^{5/2})$ и $L = B_3(q)$. По лемме 2.2 хотя бы одно из чисел $k_8(q) = q^4+1$ и $k_5(q) = (q^5-1)/(q-1)$ должно лежать в $\omega(S)$, но ни одно из них не делит $|S|_{2'} = (q^5+1)(q^{5/2}-1)$; противоречие.

13. Пусть $S \simeq {}^2G_2(3^\beta)$, где $\beta \geq 3$ нечетно. Тогда $e(3,S) = \{6,2,1\}$. Значит, $e = e_2 = 6$ и $e_2/e_1 \in \{6,3,2,1\}$. Так же, как и в предыдущих случаях, показывается, что $L \neq D_n(q)$, где n нечетно, и $L \neq {}^2D_n(q)$.

Предположим, что $L \in \{B_n(q), C_n(q)\}$. Тогда $3\beta = n\alpha$. Из $t(L) \le t(S) + 1 \le 6$ следует, что $n \le 7$. Если $n = 7$, то $t(GK(L) \setminus \{3\}) = 6$, а $t(GK(S) \setminus \{3\}) = 4$; противоречие.

Пусть $n \in \{2, 4\}$. Тогда граф $GK(L)$ несвязен и по теореме Грюнберга — Кегеля получаем равенство

$$\frac{3^{n\alpha} + 1}{2} = 3^{\beta} \pm 3^{(\beta+1)/2} + 1,$$

откуда $3^{3\beta} = 2 \cdot 3^{\beta} \pm 2 \cdot 3^{(\beta+1)/2} + 1$; противоречие.

Пусть $n \in \{3, 5, 6\}$. Тогда $S \simeq {}^2G_2(q^{n/3})$. По лемме 2.2 хотя бы одно из чисел $k_{2(n-1)}(q)$ и $k_n(q)$ должно лежать в $\omega(S)$, но ни одно из них не делит $|S|_{3'} = (q^n + 1)(q^{n/3} - 1)$; противоречие.

Предположим, что $L = D_n(q)$, где n четно. Тогда $2\beta = (n - 1)\alpha$. Из неравенства $t(L) \le t(S) + 1 \le 6$ следует, что $n \le 8$. Случай $L = D_8(q)$ аналогичен случаю $L \in \{B_7(q), C_7(q)\}$, а случай $L \in \{D_6(q), D_4(q)\}$ — случаю $L \in \{B_5(q), B_3(q), C_5(q), C_3(q)\}$.

Теорема 3 доказана.

ЛИТЕРАТУРА

1. *Мазуров В. Д.* Группы с заданным спектром // Изв. Уральск. гос. ун-та. Сер. математика и механика. Вып. 7. 2005. № 36. С. 119–138.
2. *Мазуров В. Д.* Распознавание конечных простых групп $S_4(q)$ по порядкам их элементов // Алгебра и логика. 2002. Т. 41, № 2. С. 166–198.
3. *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.
4. *Мазуров В. Д.* Характеризация конечных групп множествами порядков их элементов // Алгебра и логика. 1997. Т. 36, № 1. С. 37–53.
5. *Shi W., Tang C. Y.* A characterization of some orthogonal groups // Progr. Nat. Sci. 1997. V. 7, N 2. P. 155–162.
6. *Mazurov V. D., Moghaddamfar A. R.* The recognition of the simple group $S_8(2)$ by its spectrum // Algebra Colloq. 2006. V. 13, N 4. P. 643–646.
7. *Васильев А. В., Гречкосеева М. А.* О распознаваемости конечных простых ортогональных групп размерности 2^m, $2^m + 1$ и $2^m + 2$ над полем характеристики 2 // Сиб. мат. журн. 2004. Т. 45, № 3. С. 510–526.
8. *Гречкосеева М. А.* Распознаваемость группы $O^+_{10}(2)$ по ее спектру // Сиб. мат. журн. 2003. Т. 44, № 4. С. 737–741.
9. *Алексеева О. А., Кондратьев А. С.* Распознаваемость по спектру групп ${}^2D_p(3)$ для нечетного простого числа p // Тр. Ин-та математики и механики УрО РАН. 2008. Т. 14, № 4. С. 3–11.
10. *Kondrat'ev A. S.* Recognition by spectrum of the groups ${}^2D_{2^m+1}(3)$ // Sci. China, Ser. A. 2009. V. 52, N 2. P. 293–300.
11. *Васильев А. В., Горшков И. Б., Гречкосеева М. А., Кондратьев А. С., Старолетов А. М.* О распознаваемости по спектру конечных простых групп типов B_n, C_n и ${}^2D_n$ при $n = 2^k$ // Тр. Ин-та математики и механики УрО РАН. 2009. Т. 15, № 2. С. 58–73.
12. *Алексеева О. А., Кондратьев А. С.* О распознаваемости по спектру некоторых конечных простых ортогональных групп // Тр. Ин-та математики и механики УрО РАН. 2009. Т. 15, № 1. С. 30–43.
13. *Коуровская тетрадь.* Нерешенные вопросы теории групп / сост. В. Д. Мазуров, Е. И. Хухро. 16-е изд. Новосибирск: Ин-т математики СО РАН, 2006.
14. *Shi W.* A new characterization of the sporadic simple groups // Group theory. Proc. of the 1987 Singapore group theory conf. Berlin; New York: Walter de Gruyter, 1989. P. 531–540.
15. *Xu M., Shi W.* Pure quantitative characterization of finite simple groups ${}^2D_n(q)$ и $D_l(q)$ (l odd) // Algebra Colloq. 2003. V. 10, N 3. P. 427–443.
16. *Conway J. H, Curtis R. T., Norton S. P., Parker R. A., Wilson R. A.* Atlas of finite groups. Oxford: Clarendon Press, 1985.

17. *Zsigmondy K.* Zür Theorie der Potenzreste // Monatsh. Math. Phys. 1892. Bd 3. S. 265–284.
18. *Roitman M.* On Zsigmondy primes // Proc. Amer. Math. Soc. 1997. V. 125, N 7. P. 1913–1919.
19. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.
20. *Кондратьев А. С.* О компонентах графа простых чисел конечных простых групп // Мат. сб. 1989. Т. 180, № 6. С. 787–797.
21. *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.
22. *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.
23. *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.
24. *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.
25. *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.
26. *Gorenstein D.* Finite Groups. New York etc.: Harper & Row, 1968.
27. *Алеева М. Р.* О конечных простых группах с множеством порядков элементов, как у группы Фробениуса или двойной группы Фробениуса // Мат. заметки. 2003. Т. 73, № 3. С. 323–339.
28. *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.
29. *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.
30. *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.
31. *Srinivasan B.* The characters of the finite symplectic group $Sp(4,q)$ // Trans. Amer. Math. Soc. 1968. V. 131, N 2. P. 488–525.
32. *Carter R. W.* Simple groups of Lie type. London etc.: John Wiley and Sons, 1972. (Pure Appl. Math., A Wiley-Interscience Publ.; 28).
33. *Бутурлакин А. А., Гречкосеева М. А.* Циклическое строение максимальных торов в конечных классических группах // Алгебра и логика. 2007. Т. 46, № 2. С. 129–156.

Статья поступила 4 августа 2009 г.

Васильев Андрей Викторович, Гречкосеева Мария Александровна,
Мазуров Виктор Данилович
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
vasand@math.nsc.ru, grechkoseeva@gmail.org, mazurov@math.nsc.ru