Сибирский математический журнал
Июль—август, 2016. Том 57, № 4

УДК 512.542

О СПЕКТРАХ ПОЧТИ ПРОСТЫХ ГРУПП С СИМПЛЕКТИЧЕСКИМ ИЛИ ОРТОГОНАЛЬНЫМ ЦОКОЛЕМ

М. А. Гречкосеева

Аннотация. Конечные группы называются *изоспектральными*, если у них одинаковые множества порядков элементов. Рассматриваются почти простые группы H с цоколем S, где S — конечная простая симплектическая или ортогональная группа над полем нечетной характеристики. Показано, что если H изоспектральна S, то H/S является 2-группой. Найден критерий изоспектральности H и S в случае, когда S — симплектическая группа или ортогональная группа нечетной размерности.

DOI 10.17377/smzh.2016.57.402

Ключевые слова: почти простая группа, порядки элементов, распознаваемость по спектру.

1. Введение

Спектром $\omega(G)$ конечной группы G называется множество порядков ее элементов. Как недавно было показано, если G — конечная группа и $\omega(G) = \omega(S)$, где S — конечная простая классическая группа размерности больше 60, то G — почти простая группа с цоколем, изоморфным S (см. [1]). Таким образом, возникает естественный вопрос о том, какие почти простые группы с классическим цоколем S имеют такой же спектр, как S (ср. [2, вопрос 17.36]). Этот вопрос решен в случае, когда S — одна из групп $L_2(q)$ [3], $L_3(q)$ [4, 5] и $U_3(q)$ [4, 6], а также когда S — группа над полем характеристики 2 [7–10]. В настоящей работе рассматривается случай, когда S — симплектическая или ортогональная группа над полем нечетной характеристики. Основными результатами работы являются две следующие теоремы.

Теорема 1. *Пусть S — простая группа $S_{2n}(q)$ или $O_{2n+1}(q)$, где $n \geq 2$ и q — степень нечетного простого числа p, и $S < H \leq \operatorname{Aut} S$. Тогда $\omega(H) = \omega(S)$ в том и только в том случае, когда H является расширением S посредством полевого автоморфизма, H/S — 2-группа и $2n-1$ не является степенью числа p.*

Теорема 2. *Пусть S — простая группа $O^{\varepsilon}_{2n}(q)$, где $n \geq 4$, q нечетно и $\varepsilon \in \{+,-\}$. Если $S < H \leq \operatorname{Aut} S$ и $\omega(H) = \omega(S)$, то H/S является 2-группой.*

Отметим, что согласно сведениям о таблицах характеров групп $O^{\pm}_8(3)$ в [11] если $S = O^{\varepsilon}_8(3)$, $S < H \leq \operatorname{Aut} S$ и $\omega(H) = \omega(S)$, то $\varepsilon = -$ и H является расширением группы S посредством графового автоморфизма порядка 2 (группа $O^{-}_8(3).2_1$ в обозначениях из [11]).

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 14–01–90013).

2. Предварительные сведения

Через $[m_1, m_2, \dots, m_k]$ и $(m_1, m_2, \dots, m_k)$ обозначаются наименьшее общее кратное и наибольший общий делитель целых чисел $m_1, m_2, \dots, m_k$ соответственно. Через $\pi(m)$ обозначается множество простых делителей натурального числа m. Если r — простое число, то через $(m)_r$ обозначается *r-часть* числа m, т. е. наибольшая степень числа r, делящая m. Через $(m)_{r'}$ обозначается *r'-часть числа* m, т. е. отношение $m/(m)_r$. Если $\varepsilon \in \{+,-\}$, то в арифметических выражениях пишем ε вместо $\varepsilon 1$.

Если G — конечная группа и $p \in \pi(G)$, то $\omega_{p'}(G)$ — это подмножество чисел, взаимно простых с p, в $\omega(G)$.

Мы обозначаем конечные простые группы и конечные классические группы согласно [12].

Лемма 2.1 [13, следствия 2, 5, 6]. *Пусть $n \geq 2$, q — степень нечетного простого числа p и L — одна из групп $S_{2n}(q)$, $O_{2n+1}(q)$ и $SO_{2n+1}(q)$. Пусть $d = 2$, если $L = O_{2n+1}(q)$ и $n \geq 3$, и $d = 1$ в остальных случаях, а $c = 1$, если $L = SO_{2n+1}(q)$, и $c = 2$ в остальных случаях. Тогда $\omega(L)$ состоит из всех делителей следующих чисел:*

(1) $(q^n \pm 1)/c$;

(2) $[q^{n_1} \pm 1, \dots, q^{n_s} \pm 1]$, *где $s \geq 2$, $n_i > 0$ для всех $1 \leq i \leq s$ и $n_1 + \dots + n_s = n$;*

(3) $p^l(q^{n_1} \pm 1)/d$, *где $l, n_1 > 0$ и $p^{l-1} + 1 + 2n_1 = 2n$;*

(4) $p^l[q^{n_1} \pm 1, \dots, q^{n_s} \pm 1]$, *где $l > 0$, $s \geq 2$, $n_i > 0$ для всех $1 \leq i \leq s$ и $p^{l-1} + 1 + 2(n_1 + \dots + n_s) = 2n$;*

(5) p^l, *если $2n = p^{l-1} + 1$ для $l > 0$.*

Лемма 2.2. *Пусть $n \geq 2$, q — степень нечетного простого числа и $L = \mathrm{Spin}_{2n+1}(q)$. Тогда $\omega(L)$ содержит следующие числа:*

(1) $q^n + 1$;

(2) $q^n - 1$, *если n нечетно;*

(3) $(q^{n_1} - 1)(q^{n_2} + 1)$, *где n_1 и n_2 нечетны, $n = n_1 + n_2$.*

Доказательство. Утверждение следует из описания строения максимальных торов спинорных групп в [14]. $\square$

Лемма 2.3. *Пусть $n \geq 4$, q — степень нечетного простого числа p, $\varepsilon \in \{+,-\}$ и $L = O^{\varepsilon}_{2n}(q)$. Положим $d = (4, q^n - \varepsilon)$ и $c = d/2$. Тогда $\omega(L)$ состоит из всех делителей следующих чисел:*

(1) $(q^n - \varepsilon)/d$;

(2) $[q^{n_1} - \delta, q^{n_2} - \varepsilon\delta]/e$, *где $\delta \in \{+,-\}$, $n_1, n_2 > 0$, $n_1 + n_2 = n$; $e = 2$, если $(q^{n_1} - \delta)_2 = (q^{n_2} - \varepsilon\delta)_2$, и $e = 1$ в остальных случаях;*

(3) $[q^{n_1} - \delta_1, q^{n_2} - \delta_2, \dots, q^{n_s} - \delta_s]$, *где $s \geq 3$, $\delta_i \in \{+,-\}$, $n_i > 0$ для всех $1 \leq i \leq s$, $n_1 + \dots + n_s = n$ и $\delta_1\delta_2 \dots \delta_s = \varepsilon$;*

(4) $p[q \pm 1, (q^{n-2} - \varepsilon)/2]$;

(5) $p[q \pm 1, q^{n_1} - \delta_1, q^{n_2} - \delta_2, \dots, q^{n_s} - \delta_s]$, *где $s \geq 2$, $\delta_i \in \{+,-\}$, $n_i > 0$ для всех $1 \leq i \leq s$, $n_1 + \dots + n_s = n - 2$ и $\delta_1\delta_2 \dots \delta_s = \varepsilon$;*

(6) $p^l(q^{n_1} \pm 1)/c$, *где $l > 0$ и $p^{l-1} + 3 + 2n_1 = 2n$;*

(7) $p^l[q^{n_1} \pm 1, \dots, q^{n_s} \pm 1]$, *где $l > 0$, $s \geq 2$, $n_i > 0$ для всех $1 \leq i \leq s$ и $p^{l-1} + 3 + 2(n_1 + \dots + n_s) = 2n$;*

(8) p^l, *если $2n = p^{l-1} + 3$ для $l > 0$.*

Доказательство. См. [13, следствия 8, 9]. Следует отметить, что в п. (3) следствия 8 из [13] есть опечатка: вместо «$p^k[d_k, (q^{n(k)} \pm 1)/d_k]$, где

$d_k = (4, q^{n-n(k)} - \varepsilon)/2$», должно быть «$p^k[d_k, (q^{n(k)} - \delta)/d_k]$, где $d_k = (4, q^{n-n(k)} - \delta\varepsilon)/2$». $\square$

Примитивным простым делителем числа $q^m - 1$, где $q > 1$ и $m \geq 3$, называется простое число r такое, что r делит $q^m - 1$ и не делит $q^l - 1$ для всех $l < m$. Множество примитивных простых делителей числа $q^m - 1$ обозначается через $R_m(q)$, и через $r_m(q)$ обозначается некоторый, вообще говоря, произвольный элемент множества $R_m(q)$. Из определения следует, что для любого k, взаимно простого с m, выполнено включение $R_m(q) \subseteq R_m(q^k)$.

Лемма 2.4 (Жигмонди [15]). *Пусть q — целое число, $q > 1$, и $m \geq 3$. Тогда множество $R_m(q)$ непусто, исключая случай, когда $q = 2$ и $m = 6$.*

Лемма 2.5. *Пусть q — целое число, $q > 1$, k и m — натуральные числа.*

(1) $(q^k - 1, q^m - 1) = q^{(k,m)} - 1$;

(2) $(q^k + 1, q^m + 1) = q^{(k,m)} + 1$, *если* $(k)_2 = (m)_2$, *и* $(q^k + 1, q^m + 1) = (2, q + 1)$ *в противном случае;*

(3) $(q^k - 1, q^m + 1) = q^{(k,m)} + 1$, *если* $(k)_2 > (m)_2$, *и* $(q^k - 1, q^m + 1) = (2, q + 1)$ *в противном случае.*

Доказательство. См., например, [5, лемма 6]. $\square$

Лемма 2.6. *Пусть q — нечетное число, $q > 1$, $\varepsilon \in \{+, -\}$ и m — натуральное число.*

(1) *Если m нечетно, то* $(q^m - \varepsilon)_2 = (q - \varepsilon)_2$.

(2) *Если* $q \equiv 1 \pmod 4$, *то* $(q^m - 1)_2 = (m)_2(q - 1)_2$.

(3) *Если m четно, то* $(q^m - 1)_2 \geq (m)_2(q - \varepsilon)_2$.

Доказательство. (1) Если m нечетно, то отношение $(q^m - \varepsilon)/(q - \varepsilon)$ также нечетно. (2) Следует по индукции по m из (1) и того, что $(q^2 - 1)_2 = (q - 1)_2(q + 1)_2 = 2(q - 1)_2$. (3) Используя (2), получаем, что $(q^m - 1)_2 = (m/2)_2(q^2 - 1)_2 \geq (m/2)_2 \cdot 2(q - \varepsilon)_2$. $\square$

Пусть G — линейная алгебраическая группа над алгебраически замкнутым полем F характеристики p. Тогда G изоморфна замкнутой подгруппе группы $GL_n(F)$ для некоторого n. Эндоморфизм τ группы G называется *отображением Фробениуса*, если найдутся положительные целые числа k и m такие, что при идентификации группы G с ее образом в $GL_n(F)$ эндоморфизм τ^k индуцируется возведением матричных коэффициентов в степень p^m (см. [16, 1.17] или [17, определение 2.1.9]).

Лемма 2.7. *Пусть G — связная линейная алгебраическая группа над алгебраически замкнутым полем характеристики $p > 0$ и τ — сюръективный эндоморфизм группы G. Для натурального числа n положим $G_n = C_G(\tau^n)$. Предположим, что для некоторого числа k группа G_k конечна. Тогда τ индуцирует изоморфизм группы G_k порядка k и для смежного класса $G_k\tau^i$ группы $G_k \rtimes \langle\tau\rangle$ выполнено*

$$\omega(G_k\tau^i) = \frac{k}{j} \cdot \omega(G_j), \tag{2.1}$$

где $j = (i, k)$.

Если к тому же G — редуктивная группа и τ — отображение Фробениуса, то $Z(G_n) = Z(G) \cap G_n$ и

$$\omega(\overline{G}_k\tau^i) = \frac{k}{j} \cdot \omega(\overline{G}_j), \tag{2.2}$$

где $\overline{G}_n = G_n/Z(G_n)$ и $j = (i,k)$.

Доказательство. Первая часть утверждения доказана в [6, предложение 13]. Идея доказательства второй части также содержится в доказательстве предложения 13 из [6]: во-первых, там было показано, что равенство (2.2) достаточно проверить при $i = 1$; во-вторых, было установлено, что любой $g \in G_1$ сопряжен в G с элементом вида $(h\tau)^k$, где $h \in G_k$. Если G — редуктивная группа и τ — отображение Фробениуса, то $Z(G_n) = Z(G) \cap G_n$ по [16, предложение 3.6.8] и, значит, для упомянутых g и h выполнено

$$|\langle g\rangle \cap Z(G_1)| = |\langle g\rangle \cap Z(G)| = |\langle (h\tau)^k\rangle \cap Z(G)| = |\langle (h\tau)^k\rangle \cap Z(G_k)|,$$

откуда следует требуемое. $\square$

Если Σ — неразложимая система корней, диаграмма Дынкина которой имеет симметрию порядка d, $d \in \{1,2,3\}$, и q — степень простого числа, то через ${}^d\Sigma(q)$ обозначаем соответствующую группу лиева типа (см. [17, определение 2.2.4]).

Лемма 2.8. *Пусть $S = {}^d\Sigma(q)$ — простая группа лиева типа, отличная от групп Ри и Сузуки. Предположим, что ψ — полевой автоморфизм группы S порядка k и $(k,d) = 1$. Тогда*

$$\omega(S\psi^i) = \frac{k}{j} \cdot \omega({}^d\Sigma(q^{j/k})), \tag{2.3}$$

$$\omega(\operatorname{Inndiag} S\psi^i) = \frac{k}{j} \cdot (\operatorname{Inndiag} {}^d\Sigma(q^{j/k})), \tag{2.4}$$

где $j = (i,k)$.

Доказательство. Пусть $q = p^m$, где p — простое число. Выберем представление группы S как множества неподвижных точек отображения Фробениуса простой алгебраической группы стандартным способом (см. [17, теорема 2.2.3, определение 2.2.4]): G — простая алгебраическая группа типа Σ над алгебраическим замыканием поля порядка p, φ_p — эндоморфизм группы G, действующий на корневых элементах по правилу $x_\alpha(t) \mapsto x_\alpha(t^p)$, γ_ρ — графовый автоморфизм группы G порядка d, индуцированный симметрией ρ диаграммы Дынкина системы Σ, $\sigma = (\varphi_p)^m\gamma_\rho$, $K = O^{p'}(C_G(\sigma))$ и $S = K/Z(K)$.

Отметим, что в силу простоты группы G любой сюръективный эндоморфизм группы G с конечным множеством неподвижных точек будет отображением Фробениуса [17, теорема 2.1.11].

Поскольку $(k,d) = 1$, найдется $\gamma_1 \in \langle\gamma_\rho\rangle$ такой, что $\gamma_1^k = \gamma_\rho$. Обозначим m/k через l и положим $\tau = (\varphi_p)^l\gamma_1$. Тогда $\tau^k = \sigma$ и τ индуцирует полевой автоморфизм группы S порядка k (при $d > 1$ в $\operatorname{Out} S$ единственная подгруппа порядка k). Если G — односвязная группа, то $K = C_G(\sigma)$ и из (2.2) леммы 2.7 следует (2.3). Если G — присоединенная группа, то $Z(K) = 1$ и $C_G(\sigma)$ действует на $K = S$ как $\operatorname{Inndiag} S$ [17, лемма 2.5.8]. Применяя лемму 2.7, получаем (2.4). $\square$

Отметим, что для линейных и унитарных групп лемма 2.8 была доказана в [6, следствие 14].

3. Доказательство теоремы 1

Пусть p — нечетное простое число, $q = p^m$ и S — одна из групп $S_{2n}(q)$ или $O_{2n+1}(q)$, где $n \geq 2$. Группа $\operatorname{Aut} S$ является полупрямым произведением группы $\operatorname{Inndiag} S$ и группы полевых автоморфизмов группы S, и $|\operatorname{Inndiag} S : S| = 2$. Обозначим через δ диагональный автоморфизм группы S, который порождает $\operatorname{Inndiag} S$ по модулю S.

Группа $\operatorname{Inndiag} S$ является присоединенной группой того же типа, что и S, над полем порядка q. Следовательно,

$$\operatorname{Inndiag} O_{2n+1}(q) \simeq SO_{2n+1}(q),$$

и $\operatorname{Inndiag} S_{2n}(q) = (C_n)_{ad}(q)$ двойственна группе $\operatorname{Spin}_{2n+1}(q) = (B_n)_{sc}(q)$ в смысле [16, с. 120]. В силу [16, предложения 4.4.1, 4.3.4] двойственные группы имеют изоморфные максимальные торы, поэтому $\omega_{p'}(\operatorname{Inndiag} S_{2n}(q)) = \omega_{p'}(\operatorname{Spin}_{2n+1}(q))$.

Приступим к доказательству теоремы. Пусть $S < H \leq \operatorname{Aut} S$ и $\omega(H) = \omega(S)$.

1. Предположим, что $|H/S|$ делится на нечетное простое число r. Тогда H содержит полевой автоморфизм порядка r. По лемме 2.8 множество $\omega(H)$ содержит $r \cdot \omega(S(q^{1/r}))$, где $S(q^{1/r})$ — простая группа того же типа, что и S, над полем порядка $q^{1/r}$. Обозначим $q^{1/r}$ через q_0. По лемме 2.1 у групп S и $S(q_0)$ одинаковые периоды силовских p-подгрупп, поэтому можно считать, что $r \neq p$.

Пусть $n = 2$. Тогда $\omega(H)$ содержит элементы порядков $rr_4(q_0)$ и $2r$. Поскольку $r_4(q_0) \in R_4(q)$, из определения примитивного делителя и леммы 2.1 следует, что если $rr_4(q_0) \in \omega(S)$, то r делит $(q^2+1)/2$ и тогда $2r \notin \omega(S)$. Значит, $\omega(H) \neq \omega(S)$.

Пусть $n \geq 4$ четно. Предположим, что $(r, n-1) = 1$, и рассмотрим числа $a = rpr_{n-1}(q_0)$ и $b = rpr_{n-1}(-q_0)$, лежащие в $\omega(H)$. В силу того, что r не делит $n-1$, число $r_{n-1}(\varepsilon q_0)$ лежит в $R_{n-1}(\varepsilon q)$. Значит, если $rpr_{n-1}(\varepsilon q_0) \in \omega(S)$, то r делит $q^{n-1} - \varepsilon$. Поскольку $(q^{n-1}-1, q^{n-1}+1) = 2$, хотя бы одно из чисел a и b не лежит в $\omega(S)$. Предположим, что r делит $n-1$. Тогда $(r, n) = (r, n-2) = 1$. В $\omega(H)$ есть числа $rr_{2n}(q_0)$ и $rpr_{2(n-2)}(q_0)$. Если первое из них лежит в $\omega(S)$, то r делит $q^n + 1$, а если второе — то r делит $[q^{n-2}+1, q \pm 1]$. Поскольку $(q^n+1, q^{n-2}+1) = (q^n+1, q^2-1) = 1$, снова получаем, что $\omega(H) \neq \omega(S)$.

Пусть n нечетно. Если $(r, n) = 1$, то $r_n(\varepsilon q_0) \in R_n(\varepsilon q)$, поэтому оба числа $rr_n(q_0)$ и $rr_{2n}(q_0)$ не могут лежать в $\omega(S)$. Значит, r делит n. Тогда $(r, n-1) = (r, n-2) = 1$. В $\omega(H)$ есть число $rpr_{2(n-1)}(q_0)$. Из того, что $rpr_{2(n-1)}(q_0) \in \omega(S)$, следует, что r делит $q^{n-1}+1$. В частности, $n \geq 5$ (иначе $r = 3$ делит q^2+1, а это невозможно). Следовательно, существует примитивный делитель $r_{2(n-2)}(q_0)$, и $rpr_{2(n-2)}(q_0) \in \omega(H)$. Если $rpr_{2(n-2)}(q_0) \in \omega(S)$, то r делит $[q^{n-2}+1, q \pm 1]$, однако $(q^{n-1}+1, q^{n-2}+1) = (q^{n-1}+1, q \pm 1) = 2$. Стало быть, $\omega(H) \neq \omega(S)$.

2. Таким образом, H/S является 2-группой. Покажем, что H является расширением группы S с помощью полевого автоморфизма. В противном случае H содержит $\delta\psi$ для некоторого полевого автоморфизма ψ порядка 2^t.

Если $\psi = 1$, то H содержит $\operatorname{Inndiag} S$. Напомним, что $\omega_{p'}(\operatorname{Inndiag} S)$ совпадает с $\omega_{p'}(\operatorname{Spin}_{2n+1}(q))$ или $\omega_{p'}(SO_{2n+1}(q))$. Значит, по леммам 2.1 и 2.2 в H есть элемент порядка $q^n + 1$ и $\omega(H) \neq \omega(S)$.

Предположим, что $t > 0$, и положим $q_0 = q^{1/2^t}$. В силу леммы 2.8 имеем

$$\omega(S\psi) \cup \omega(S\delta\psi) = \omega(\operatorname{Inndiag} S\psi) = 2^t \cdot \omega(\operatorname{Inndiag} S(q_0)),$$

$$\omega(S\psi) = 2^t \cdot \omega(S(q_0)).$$

Таким образом, если $a \in \omega(\operatorname{Inndiag} S(q_0))$ и $a \notin \omega(S(q_0))$, то $2^t a \in \omega(S\delta\psi)$. Если при этом $2^t a \notin \omega(S)$, то $2^t a \in \omega(H) \setminus \omega(S)$. Ниже найдем такое число a для каждой из рассматриваемых групп.

Предположим сначала, что S — симплектическая группа. Пусть n четно и $a = \bigl(q_0^{n-1} - 1\bigr)(q_0 + 1)$. Тогда $a \in \omega_{p'}(\mathrm{Spin}_{2n+1}(q_0))$ по лемме 2.2 и, значит, $a \in \omega(\operatorname{Inndiag} S(q_0))$. Если $n = 2$, то $a = q_0^2 - 1$ и по лемме 2.6(2) выполнено $2^t(a)_2 = 2^t\bigl(q_0^2 - 1\bigr)_2 = (q^2 - 1)_2$, поэтому $a \notin \omega(S(q_0))$ и $2^t a \notin \omega(S)$. Пусть $n \geq 4$. Тогда a делится на $r_{n-1}(q_0) \in R_{n-1}(q)$. Значит, если $a \in \omega(S(q_0))$ или $2^t a \in \omega(S)$, то a делит $b_0 = \bigl[q_0^{n-1} - 1, q_0 + 1\bigr]$ или $2^t a$ делит $b = [q^{n-1} - 1, q + 1]$ соответственно. Однако по лемме 2.6

$$(a)_2 = \bigl(q_0^{n-1} - 1\bigr)_2 (q_0 + 1)_2 = (q_0 - 1)_2 (q_0 + 1)_2 = \bigl(q_0^2 - 1\bigr)_2 > (b_0)_2,$$

$$2^t(a)_2 = 2^t\bigl(q_0^2 - 1\bigr)_2 = (q^2 - 1)_2 = (q^{n-1} - 1)_2 (q + 1)_2 > (b).$$

Пусть n нечетно, $q_0 \equiv \varepsilon \pmod 4$ и $a = q_0^n - \varepsilon$. Тогда $a \in \omega(\operatorname{Inndiag} S(q_0)) \setminus \omega(S(q_0))$. Предположим, что $2^t a \in \omega(S)$. Тогда $2^t a$ делит $(q^n - 1)/2$. Однако в силу леммы 2.6 выполнено равенство $2^t\bigl(q_0^n - \varepsilon\bigr)_2 = 2^t\bigl(\varepsilon q_0^n - 1\bigr)_2 = (q^n - 1)_2$; противоречие.

Пусть S — ортогональная группа и $q_0 \equiv \varepsilon \pmod 4$. Если n нечетно, то, как и выше, в качестве a можно взять $q_0^n - \varepsilon$. Пусть n четно. Тогда можно считать, что $n \geq 4$. Полагая $a = p\bigl(q_0^{n-1} - \varepsilon\bigr)$ и рассуждая аналогично случаю нечетного n, получаем, что $a \in \omega(\operatorname{Inndiag} S(q_0)) \setminus \omega(S(q_0))$ и $2^t a \notin \omega(S)$.

3. Таким образом, $H = S \rtimes \langle\psi\rangle$ для некоторого полевого автоморфизма ψ. Осталось показать, что $\omega(H) \neq \omega(S)$, если $2n - 1$ является степенью числа p, и $\omega(H) = \omega(S)$ в противном случае.

Пусть $2n = p^{l-1} + 1$ для некоторого $l \geq 1$. Тогда $2p^l \in 2\omega(S(q^{1/2})) \subseteq \omega(H)$ по лемме 2.8 и $2p^l \notin \omega(S)$.

Пусть теперь $2n - 1$ не является степенью числа p. В силу леммы 2.8 для доказательства равенства $\omega(H) = \omega(S)$ достаточно показать, что для любого t такого, что $2 \leq 2^t \leq (m)_2$, выполнено включение $2^t\omega(S(q^{1/2^t})) \subseteq \omega(S)$.

Пусть $2 \leq 2^t \leq (m)_2$, $q_0 = q^{1/2^t}$ и $a \in \omega(S(q_0))$. Число a делит одно из чисел, указанных в пп. (1)–(4) леммы 2.1. Каждое из этих чисел можно записать как $f_0 = p^l\bigl[q_0^{n_1} \pm 1, \dots, q_0^{n_s} \pm 1\bigr]/e$, где $l \geq 0$, $n_1, \dots, n_s > 0$, e зависит от типа группы S и не зависит от q_0, причем $\omega(S)$ будет содержать число $f = p^l\bigl[q^{n_1} - 1, \dots, q^{n_s} - 1\bigr]/e$. Поскольку $q_0^k \pm 1$ делит $q^k - 1$ и $2^t\bigl(q_0^k \pm 1\bigr)_2 \leq (q^k - 1)_2$ по лемме 2.6(3), получаем, что $2^t f_0$ делит f. Значит, $2^t a \in \omega(S)$, как и требовалось. Теорема 1 доказана.

4. Доказательство теоремы 2

Пусть $S = O_{2n}^{\varepsilon}(q)$, где $q = p^m$, p — нечетное простое число, $n \geq 4$ и $\varepsilon \in \{+, -\}$. Предположим от противного, что $S \leq H \leq \operatorname{Aut}(S)$, $\omega(H) = \omega(S)$ и $\pi(H/S)$ содержит нечетное простое число r. Группа $\operatorname{Aut} S$ является полупрямым произведением группы $\operatorname{Inndiag} S$ и группы, порожденной полевыми и графовыми автоморфизмами. Поскольку $|\operatorname{Inndiag} S : S| = (4, q^n - \varepsilon)$ и порядок группы графовых автоморфизмов при $(n, \varepsilon) \neq (4, +)$ не превосходит 2, получаем, что либо H содержит полевой автоморфизм порядка r, либо $S = O_8^+(q)$ и $r = 3$.

Пусть H содержит полевой автоморфизм порядка r. Тогда по лемме 2.8 множество $\omega(H)$ содержит $r\cdot\omega\big(O^{\varepsilon}_{2n}(q_0)\big)$, где $q=q_0^r$. По лемме 2.4 у групп $O^{\varepsilon}_{2n}(q)$ и $O^{\varepsilon}_{2n}(q_0)$ одинаковые периоды силовских p-подгрупп, поэтому можно считать, что $r\neq p$.

Пусть n нечетно. Из условия $(r,n-1)=1$ следует, что r делит $[q^{n-1}+1,q+\varepsilon]$. Действительно, $rr_{2n-2}(q_0)\in\omega(H)=\omega(S)$, и так как $r_{2n-2}(q_0)\in R_{2n-2}(q)$, любое число из $\omega(S)$, кратное $r_{2n-2}(q_0)$, делит $[q^{n-1}+1,q+\varepsilon]$. Аналогичным образом если $(r,n-2)=1$, то, рассматривая число $rp\big(q_0^{n-2}+\varepsilon\big)$, заключаем, что r делит $q^{n-2}+\varepsilon$.

Предположим, что $(r,n)=1$. Поскольку $rr_n(\varepsilon q_0)\in\omega(H)=\omega(S)$ и $r_n(\varepsilon q_0)\in R_n(\varepsilon q)$, из леммы 2.4 следует, что r делит $q^n-\varepsilon$. Число r не делит хотя бы одно из чисел $n-1$ и $n-2$, поэтому по результату предыдущего абзаца r делит хотя бы одно из чисел $[q^{n-1}+1,q+\varepsilon]$ и $q^{n-2}+\varepsilon$. Так как $(q^n-\varepsilon,q^{n-1}+1)=(q^n-\varepsilon,q+\varepsilon)=2$ и $(q^n-\varepsilon,q^{n-2}+\varepsilon)=2$, приходим к противоречию.

Таким образом, r делит n. Тогда $(r,n-1)=(r,n-2)=1$ и, значит, r делит $([q^{n-1}+1,q+\varepsilon],q^{n-2}+\varepsilon)=q+\varepsilon$. Отметим, что r также делит $q_0+\varepsilon=\big(q_0^r+\varepsilon,q^{r-1}-1\big)$. Допустим, что $n\geq 7$. В $\omega(H)$ есть элемент порядка $a=rp\big[q_0^{n-4}-\varepsilon,q_0^2+1\big]$. Так как $(r,n-4)=1$ и $n-4\geq 3$, число a должно делить число $p[q^{n-4}-\varepsilon,q^2+1]$, но это противоречит тому, что r делит $q+\varepsilon$. Значит, $n=5$. Тогда $r=5$ и 5 делит $q+\varepsilon$. В $\omega(H)$ есть элемент порядка $a=5p\big[q_0^2+1,q_0-\varepsilon\big]$. Поскольку $p[q^2+1,q-\varepsilon]$ не делится на 5, получаем, что a делит $p[q^2+1,q+\varepsilon]$ и, значит, $q_0-\varepsilon$ делит $q+\varepsilon$. Тогда $q_0-\varepsilon=2$, откуда $q_0=3$, $\varepsilon=+$ и r делит $q_0+\varepsilon=4$; противоречие.

Пусть n четно и $\varepsilon=+$. Предположим, что $(r,n-1)=1$. В силу того, что $rr_{n-1}(q_0)$ и $rr_{2n-2}(q_0)$ лежат в $\omega(H)$, заключаем, что r делит и $q^{n-1}-1$, и $q^{n-1}+1$. Однако $(q^{n-1}-1,q^{n-1}+1)=2$; противоречие.

Значит, r делит $n-1$. Тогда r не делит $n-2$ и из того, что $rpr_{2n-4}(q_0)\in\omega(H)$, вытекает, что r делит $q^{n-2}+1$. В частности, $r\neq 3$ и $r\neq n-1$, иначе r делило бы $q^{n-2}-1$. Из последнего замечания следует, что $n\geq 16$. Пусть $a=rpr_{n-5}(q_0)r_6(q_0)$. Тогда $a\in\omega(H)$. Поскольку $r_{n-5}(q_0)\in R_{n-5}(q)$, $r_6(q_0)$ лежит в $R_6(q)$ и не делит $q^{n-5}-1$, если $a\in\omega(S)$, то a делит $p[q^{n-5}-1,q^3+1]$. Значит, r делит $[q^{n-5}-1,q^3+1]$, однако $(q^{n-2}+1,q^k\pm 1)=2$ для любого нечетного числа k.

Пусть n четно и $\varepsilon=-$. Если $(r,n-1)=1$, то из условия $rr_{2n-2}(q_0)\in\omega(H)$ следует, что r делит $[q^{n-1}+1,q-1]$. Если $(r,n-2)=1$, то, рассматривая число $rp\big(q_0^{n-2}+1\big)$, заключаем, что r делит $[q^{n-2}+1,q\pm 1]$.

Предположим, что $(r,n)=1$. Тогда из того, что $rr_{2n}(q_0)\in\omega(H)$, следует, что r делит q^n+1. Число r не делит хотя бы одно из чисел $n-1$ и $n-2$, поэтому по результату предыдущего абзаца r делит хотя бы одно из чисел $[q^{n-1}+1,q-1]$ и $[q^{n-2}+1,q\pm 1]$. Поскольку $(q^n+1,q^{n-1}+1)=(q^n+1,q-1)=2$ и $(q^n+1,q^{n-2}+1)=(q^n+1,q^2-1)=2$, приходим к противоречию.

Значит, r делит n. Тогда $(r,n-1)=(r,n-2)=1$, поэтому из равенства $(q^{n-1}+1,q^{n-2}+1)=2$ следует, что r делит $q\pm 1$. Выберем $\epsilon\in\{+,-\}$ так, чтобы r делило $q-\epsilon$. Отметим, что r также делит $q_0-\epsilon$. В $\omega(H)$ есть число $a=rp\big[\big(q_0^{n-2}+1\big)/2,q_0+\epsilon\big]=rp\big[q_0^{n-2}+1,q_0+\epsilon\big]$, где второе равенство выполнено в силу нечетности числа $\big(q_0^{n-2}+1\big)/2$. Поскольку $r_{2n-4}(q_0)\in R_{2n-4}(q)$, если $a\in\omega(S)$, то a делит одно из чисел $p[q^{n-2}+1,q+\epsilon]$ и $p[q^{n-2}+1,q-\epsilon]$. Однако r не делит первое из этих чисел. Значит, $q_0+\epsilon$ делит второе из этих чисел. Однако $(q_0+\epsilon,q-\epsilon)=(q_0+\epsilon,q^{n-2}+1)=2$, следовательно, $q_0=3$, $\epsilon=-1$ и r

делит $q_0 - \epsilon = 4$; противоречие.

Осталось рассмотреть случай, когда $S = O_8^+(q)$ и $r = 3$. Как и в доказательстве леммы 2.8, рассмотрим односвязную простую алгебраическую группу G типа D_4 над алгебраически замкнутым полем характеристики p и ее эндоморфизм φ_p. Также обозначим через γ графовый автоморфизм группы G порядка 3, индуцированный соответствующей симметрией диаграммы Дынкина. Если $\sigma = \varphi_p^m$ и $K = C_G(\sigma)$, то $K/Z(K) \simeq S$, φ_p индуцирует полевой автоморфизм группы S порядка m и γ индуцирует графовый автоморфизм порядка 3. При этом силовская 3-подгруппа группы $\operatorname{Out} S$ является образом группы $\langle\psi\rangle \times \langle\gamma\rangle$, где ψ — полевой автоморфизм порядка $(m)_3$. В силу доказанного выше можно считать, что H не содержит полевых автоморфизмов порядка 3, поэтому с точностью до сопряжения H содержит γ или $\phi\gamma$, где ϕ — полевой автоморфизм порядка 3, индуцированный $\varphi_p^{(m)_3/3}$.

Выпишем для удобства спектр группы S: по лемме 2.4 он состоит из делителей чисел $q^4 - 1$, $(q^3 \pm 1)/2$, $q^2 - 1$, $p(q^2 \pm 1)/2$, а также делителей чисел $9(q \pm 1)/2$ при $p = 3$ и числа 25 при $p = 5$.

Пусть $\gamma \in \omega(H)$. Тогда $3 \cdot \omega_{3'}(C_S(\gamma)) \subseteq \omega(S)$. Группа $C_S(\gamma)$ изоморфна $G_2(q)$, поэтому ее спектр содержит числа $q^2 \pm q + 1$ (строение максимальных торов группы $G_2(q)$ указано в [18, (15.1)]). Если $p = 3$, то $3(q^2 + q + 1) \in \omega(H) \setminus \omega(S)$. Если $p \neq 3$ и $q \equiv \epsilon \pmod 3$, то $3(q^2 - \epsilon q + 1) \in \omega(H) \setminus \omega(S)$.

Пусть $\phi\gamma \in H$. Полагая $\tau = (\varphi_p)^{m/3}\gamma$ и применяя к G и τ лемму 2.7, получаем, что

$$\omega(S\phi\gamma) = 3 \cdot \omega({}^3D_4(q^{1/3})).$$

Обозначим $q^{1/3}$ через q_0. В спектре группы ${}^3D_4(q_0)$ есть числа $\big(q_0^3 \pm 1\big)(q_0 \mp 1)$ (строение максимальных торов группы ${}^3D_4(q)$ указано в [19, предложение 1.2]), а также число 9, если $p = 3$ [20, предложение 0.5]. Таким образом, если $p = 3$, то $27 \in \omega(H)\backslash\omega(G)$. Если $p \neq 3$ и $q \equiv \epsilon \pmod 3$, то $a = 3\big(q_0^3 - \epsilon\big)(q_0 + \epsilon) \in \omega(H)\backslash\omega(S)$. Действительно, поскольку $3\big(q_0^3 - \epsilon\big)_3 = 3(q - \epsilon)_3 = (q^3 - \epsilon)_3$, если $a \in \omega(S)$, то a делит $(q^3 - \epsilon)/2$, однако $q_0 + \epsilon$ не делит это число. Теорема 2 доказана.

Отметим, что при $n = 2^l$ и $\varepsilon = -$ теорема 2 была доказана в [21, лемма 12], однако формулировка п. (1) этой леммы содержит ошибку. Правильная формулировка, следующая из доказательства, звучит следующим образом: «Пусть S — одна из групп $B_n(q), C_n(q)$ и ${}^2D_n(q)$, $S \leq G \leq \operatorname{Aut} S$ и $\omega(G) \subseteq \omega(C_n(q))$. Если α нечетно и $S \neq {}^2D_n(q)$, то $G = S$; если α четно или $S = {}^2D_n(q)$, то $\pi(G/S) \subseteq \{2\}$.»

ЛИТЕРАТУРА

1. *Grechkoseeva M. A., Vasil'ev A. V.* On the structure of finite groups isospectral to finite simple groups // J. Group Theory. 2015. V. 18, N 5. P. 741–759.
2. *Коуровская тетрадь.* Нерешенные вопросы теории групп. Новосибирск: Ин-т математики СО РАН, 2010.
3. *Brandl R., Shi W. J.* The characterization of $PSL(2, q)$ by its element orders // J. Algebra. 1994. V. 163, N 1. P. 109–114.
4. *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.
5. *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.
6. *Заварницин А. В.* Распознавание простых групп $U_3(q)$ по порядкам элементов // Алгебра и логика. 2006. Т. 45, № 2. С. 185–202.

7. *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.
8. *Гречкосеева М. А.* Распознавание по спектру конечных простых линейных групп над полями характеристики 2 // Алгебра и логика. 2008. Т. 47, № 4. С. 405–427.
9. *Grechkoseeva M. A., Shi W. J.* On finite groups isospectral to finite simple unitary groups over fields of characteristic 2 // Сиб. электрон. мат. изв. 2013. V. 10. P. 31–37.
10. *Zvezdina M. A.* Spectra of automorphic extensions of finite simple symplectic and orthogonal groups over fields of characteristic 2 // Сиб. электрон. мат. изв. 2014. V. 11. P. 823–832.
11. The GAP group. GAP – Groups, Algorithms, and Programming. Version 4.7.2. 2013. (http://www.gap-system.org).
12. *Conway J. H., Curtis R. T., Norton S. P., Parker R. A., Wilson R. A.* Atlas of finite groups. Oxford: Clarendon Press, 1985.
13. *Бутурлакин А. А.* Спектры конечных симплектических и ортогональных групп // Мат. тр. 2010. Т. 13, № 2. С. 33–83.
14. *Заварницин А. В.* Строение максимальных торов в спинорных группах // Сиб. мат. журн. 2015. Т. 56, № 3. С. 537–548.
15. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. V. 3. P. 265–284.
16. *Carter R. W.* Finite groups of Lie type. Conjugacy classes and complex characters. Chichester; New York: John Wiley & Sons, 1985.
17. *Gorenstein D., Lyons R., Solomon R.* The classification of the finite simple groups. Number 3. Providence, RI: Amer. Math. Soc., 1998.
18. *Aschbacher M.* Chevalley groups of type G_2 as the group of a trilinear form // J. Algebra. 1987. V. 109, N 1. P. 193–259.
19. *Deriziotis D. I., Michler G. O.* Character table and blocks of finite simple triality groups ${}^3D_4(q)$ // Trans. Amer. Math. Soc. 1987. V. 303. P. 39–70.
20. *Testerman D. M.* 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.
21. *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, ${}^2D_n$ при $n = 2^k$ // Тр. ИММ УрО РАН. 2009. Т. 15, № 2. С. 58–73.

Статья поступила 3 ноября 2015 г.

Гречкосеева Мария Александровна
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090;
Новосибирский гос. университет,
ул. Пирогова, 2, Новосибирск 630090
gma@math.nsc.ru