Сибирский математический журнал
Май—июнь, 2012. Том 53, № 3

УДК 512.542

О РАСПОЗНАВАЕМОСТИ ПО СПЕКТРУ ПРОСТЫХ ГРУПП $B_3(q)$, $C_3(q)$ И $D_4(q)$

А. М. Старолетов

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 $B_3(q)$, $C_3(q)$, $D_4(q)$. Доказано, что в случае четной характеристики эти группы восстанавливаются по своему спектру с точностью до изоморфизма при $q > 2$. В случае нечетной характеристики получено ограничение на композиционное строение групп из рассматриваемого класса.

Ключевые слова: конечная группа, простые ортогональные и симплектические группы, спектр группы, распознавание группы по спектру.

Пусть G — конечная группа. *Спектром* $\omega(G)$ называется множество порядков элементов группы G. Нетрудно заметить, что спектр группы полностью определяется множеством $\mu(G)$, которое состоит из всех максимальных по делимости элементов множества $\omega(G)$. Две группы называются *изоспектральными*, если их спектры совпадают. Говорят, что G является *распознаваемой* (*по спектру*), если любая группа с тем же спектром, что и G, изоморфна G.

Для произвольной группы G через $h(G)$ обозначается число попарно не изоморфных групп, изоспектральных G. Таким образом, распознаваемыми являются в точности группы G, для которых $h(G) = 1$. Говорят, что группа G *почти распознаваема* (*по спектру*), если выполнено $1 < h(G) < \infty$. Если же оказалось, что $h(G) = \infty$, то G называется *нераспознаваемой* (*по спектру*).

Поскольку любая конечная группа, обладающая нетривиальной разрешимой нормальной подгруппой, нераспознаваема (см., например, лемму 1 в [1]), вопрос нахождения числа $h(G)$ в основном интересен, когда G — это простая или почти простая группа (группа G называется *почти простой*, если $L \leq G \leq \mathrm{Aut}(L)$ для некоторой неабелевой простой группы L). Наиболее полный обзор групп, для которых этот вопрос решен, можно найти в [1]. В частности, в этом обзоре указано, что $\omega(D_4(2)) = \omega(B_3(2))$ и $h(D_4(2)) = h(B_3(2)) = 2$ (см. [2]), кроме того, группа $C_3(3)$ распознаваема (см. [3]), а группы $D_4(3)$, $B_3(3)$ изоспектральны, при этом $h(D_4(3)) = 2$ (см. [2]). Из основного результата работы [4] следует, что группы $C_3(4)$ и $D_4(4)$ распознаваемы.

Настоящая работа посвящена изучению вопроса распознавания для групп $B_3(q)$, $C_3(q)$ и $D_4(q)$, а именно доказаны

Работа выполнена при финансовой поддержке Совета по грантам Президента РФ (МК–2136.2010.1), Совета по грантам Президента РФ и государственной поддержке молодых российских ученых и ведущих научных школ (проект НШ–3669.2010.1), АВЦП Рособразования «Развитие научного потенциала высшей школы» (проект 2.1.1.10726) и Лаврентьевского гранта для коллективов молодых ученых СО РАН (постановление Президиума СО РАН № 43 от 04.02.2010).

Теорема 1. *Пусть L — одна из простых групп $B_3(q)$, $C_3(q)$ или $D_4(q)$, где q — степень простого числа p, $q \geq 5$. Если S — композиционный фактор конечной группы, изоспектральной L, изоморфный группе лиева типа над полем характеристики p, то $S \in \{B_3(q), C_3(q), D_4(q)\}$.*

Напомним, что при четном q группы $B_3(q)$ и $C_3(q)$ изоморфны.

Теорема 2. *Группы $C_3(q)$ и $D_4(q)$ распознаваемы по спектру при четном $q > 2$. При $q = 2$ группы $C_3(2)$ и $D_4(2)$ изоспектральны и $h(C_3(2)) = 2$.*

§ 1. Обозначения и предварительные сведения

В обозначениях простых конечных групп следуем [5]. При этом если группа лиева типа L обозначается через ${}^tX_n(q)$ [4, с. xiv, xv], будем говорить, что L — *группа ранга n над полем порядка q*. В частности, ранг скрученной группы считается равным рангу ее нескрученного аналога.

Для натурального числа n и нечетного простого числа m, взаимно простого с n, через $e(m, n)$ обозначается мультипликативный порядок числа n по модулю m. Для нечетного n положим $e(2, n) = 1$, если $n \equiv 1 (\mathrm{mod}\, 4)$, и $e(2, n) = 2$, если $n \equiv 3 (\mathrm{mod}\, 4)$; через n_r, где r — простое число, обозначается r-часть числа n, т. е. наибольшая степень числа r, делящая n, и через $n_{r'}$ — r'-часть числа n, т. е. отношение n/n_r.

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

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

Множество всех примитивных делителей числа $n^i - 1$ обозначается через $R_i(n)$. Под $r_i(n)$ понимается произвольный представитель этого множества, при этом если известно, о каком n идет речь, то обозначение сокращается до r_i. При $i \neq 2$ произведение всех примитивных делителей с учетом кратности называется *наибольшим примитивным делителем* и обозначается через $k_i(n)$. Число $k_2(n)$ — произведение всех примитивных делителей числа $n + 1$ с учетом кратности.

Несложно проверить из определения, что $k_i(n)$ взаимно просты для разных i и фиксированном n и что $k_1(q) = (n - 1)/2$, если $n \equiv 3 (\mathrm{mod}\, 4)$, и $k_1(n) = n - 1$ в остальных случаях, а также что $k_2(n) = (n + 1)/2$, если $n \equiv 1 (\mathrm{mod}\, 4)$, и $k_2(n) = n + 1$ в остальных случаях. Кроме того, далее будут использоваться значения $k_3(n)$, $k_4(n)$ и $k_6(n)$, которые также находятся непосредственно из определения.

Лемма 1.2. *Для любого натурального $n > 1$ верны следующие равенства:*

$$k_3(n) = \frac{n^2 + n + 1}{(n - 1, 3)}, \quad k_4(n) = \frac{n^2 + 1}{(n - 1, 2)}, \quad k_6(n) = \frac{n^2 - n + 1}{(n + 1, 3)}.$$

В общем случае из [7] следует, что для любого $i > 2$

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

где $\Phi_i(x)$ — 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 r и s смежны тогда и только тогда, когда $rs \in \omega(G)$.

Максимальное множество попарно не смежных вершин в графе Γ называется *кокликой*. Будем обозначать через $t(G)$ неплотность графа Γ, т. е. наибольшее число вершин в его кокликах. Для группы G положим $t(G) = t(GK(G))$. Аналогично для простого числа r через $t(r, G)$ обозначим наибольшее число вершин в кокликах графа $GK(G)$, содержащих вершину r.

Лемма 1.3 (см. [8, теорема 2; 9, предложение 2]). *Пусть L — конечная неабелева простая группа, для которой $t(L) \geq 3$ и $t(2, L) \geq 2$, а G — конечная группа, удовлетворяющая условию $\omega(G) = \omega(L)$. Тогда выполняются следующие утверждения.*

1. *Существует конечная неабелева простая группа S такая, что $S \leq \overline{G} = G/K \leq \mathrm{Aut}(S)$ для максимальной нормальной разрешимой подгруппы K группы G.*

2. *Для каждого независимого подмножества ρ множества $\pi(G)$ такого, что $|\rho| \geq 3$, 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, $t(2, S) \geq t(2, G)$.*

Лемма 1.4 [10, лемма 1]. *Путь G — конечная группа, $N \lhd G$, G/N — группа Фробениуса с ядром F и циклическим дополнением C. Если $(|F|, |N|) = 1$ и F не содержится в $NC_G(N)/N$, то $p|C|\omega(G)$ для некоторого простого делителя p числа $|N|$.*

Лемма 1.5 [11, леммы 2.1, 2.2]. *Группа $G_2(q)$ содержит подгруппы Фробениуса с ядрами порядка q^2 и $q^2 - \varepsilon q + 1$, где $\varepsilon = \pm$, в зависимости от остатка q при делении на 3 и циклическими дополнениями порядка $q^2 - 1$ и 6 соответственно.*

§ 2. Свойства простых ортогональных и симплектических групп

В [12] получено полное описание спектров для всех конечных простых ортогональных и симплектических групп. Для групп $B_3(q)$, $C_3(q)$, $D_4(q)$ в зависимости от четности q из этого описания выводятся следующие леммы.

Лемма 2.1. *Пусть $L \in \{B_3(q), C_3(q)\}$, где q нечетно. Положим $d = 2$, если $L \simeq B_3(q)$, $d = 1$ в остальных случаях. Тогда $\omega(L)$ состоит из делителей следующих чисел:*

1) $(q^3 \pm 1)/2$, $(q^2 + 1)(q + 1)/2$, $(q^2 + 1)(q - 1)/2$, $q^2 - 1$, $p(q^2 \pm 1)/d$;
2) $9(q \pm 1)/d$, *если* $p = 3$;
3) 25, *если* $p = 5$.

Лемма 2.2. *Спектр группы $D_4(q)$, где q — нечетное простое число, состоит из делителей следующих чисел:*

1) $(q^4 - 1)/4$, $(q^3 \pm 1)/2$, $q^2 - 1$, $p(q^2 \pm 1)/2$;
2) $9(q \pm 1)/2$, *если* $p = 3$;
3) 25, *если* $p = 5$.

Лемма 2.3. *Пусть q — степень числа 2. В этом случае $B_3(q) \simeq C_3(q)$ и спектр $B_3(q)$ состоит из делителей следующих чисел: $q^3 \pm 1$, $(q^2 + 1)(q + 1)$, $(q^2 + 1)(q - 1)$, $2(q^2 \pm 1)$, $4(q \pm 1)$, 8.*

Лемма 2.4. *Пусть q — степень числа 2. Спектр $D_4(q)$ состоит из делителей следующих чисел: q^4-1, $q^3\pm 1$, $2(q^2\pm 1)$, $4(q\pm 1)$, 8.*

Работа [13] посвящена изучению композиционного строения групп, изоспектральных простой симплектической или ортогональной группе. Из основной теоремы для рассматриваемых в настоящей работе групп получается следующая

Лемма 2.5. *Пусть q — степень простого числа p, L — одна из простых групп $B_3(q)$, $C_3(q)$ и $D_4(q)$. Тогда*

1) *среди неабелевых композиционных факторов конечных групп, изоспектральных L, нет знакопеременных групп, спорадических групп и группы Титса ${}^2F_4(2)'$;*

2) *если S — композиционный фактор конечной группы, изоспектральной L, изоморфный группе лиева типа над полем характеристики p, то $S\in\{A_1(q^3), B_3(q), C_3(q), D_4(q), G_2(q)\}$.*

§ 3. Доказательства теорем 1 и 2

Пусть L изоморфна одной из групп $B_3(q)$, $C_3(q)$ или $D_4(q)$ для некоторого $q = p^k$, где p — простое число. Предположим, что для некоторой конечной группы G оказалось, что $\omega(G)=\omega(L)$. Как отмечалось ранее, предполагаем, что $q\geq 5$. Заметим, что $t(2,L)\geq 2$ (см. [14, табл. 4, 6]), $t(L)=3$ (см. [14, табл. 8]), поэтому по п. 1 леммы 1.3 получаем, что существует неабелева простая группа S со свойством $S\leq \overline{G}=G/K\leq \operatorname{Aut}(S)$ для максимальной разрешимой нормальной подгруппы K в G. По лемме 2.5 группа S изоморфна либо одной из групп $A_1(q^3)$, $G_2(q)$, $B_3(q)$, $C_3(q)$, $D_4(q)$, либо простой группе лиева типа над полем характеристики, отличной от p. Следующие две леммы доказывают теорему 1.

Лемма 3.1. $S\ncong A_1(q^3)$.

Доказательство. Пусть $S\cong A_1(q^3)$. Докажем сначала, что $(|K|,k_4(q))\neq 1$. Предположим противное, тогда, учитывая, что $(|S|,k_4(q))=1$, получаем, что $|\operatorname{Out}(S)|$ делится на $k_4(q)$. Но $k_4(q)\geq (q^2+1)/2\geq (5^{2k}+1)/2=(1+(1+24)^k)/2\geq (1+1+24k)/2>6k$ при $k\geq 1$. Известно, что $|\operatorname{Out}(A_1(q^3))|=6k$, тем самым $k_4(q)>|\operatorname{Out}(A_1(q^3))|$; противоречие. Заметим, что $\{r_3,r_4,r_6\}$ является кокликой в $GK(G)$, поэтому из п. 2 леммы 1.3 следует, что $(|K|,k_3(q))=1$ и $(|K|,k_6(q))=1$.

Пусть $U\in \operatorname{Syl}_p(K)$. Докажем, что U является нормальным делителем в K. Предположим, что r — простой делитель $|K|$, отличный от p, и H — $\{p,r\}$-холлова подгруппа в K. Пусть m — какое-нибудь простое число из $R_3(q)$, если $r\in R_2(q)$, иначе положим m равным любому числу из $R_6(q)$. Из аргумента Фраттини, примененного к H, получаем, что m делит порядок $N_G(H)$. Автоморфизм группы H, индуцированный сопряжением элемента порядка m из $N_G(H)$, действует на H без неподвижных точек, поэтому по теореме Томпсона H нильпотентна. Следовательно, $|C_K(U)|$ делится на $|K|_r$. В силу произвольности r получаем требуемое.

Пусть $\overline{K}=K/U$, $\overline{G}=G/U$. Заметим, что $(|K|,k_4(q))\neq 1$, поэтому $\overline{K}\neq 1$. В группе $A_1(q^3)$ есть группа Фробениуса с ядром порядка q^3 и циклическим дополнением порядка $(q^3-1)/(2,q-1)$, тем самым по лемме 1.4 в $\overline{G}$ есть элемент порядка вида $t(q^3-1)/(2,q)$, где $t>2$, если q четно, и $t\geq 2$, если q нечетно. Получаем противоречие. □

Лемма 3.2. $S \not\cong G_2(q)$.

Доказательство. Аналогично лемме 3.1 можно показать, что $(|K|, k_4(q)) \neq 1$, $(|K|, k_3(q)) = 1$ и $(|K|, k_6(q)) = 1$. Пусть $\sigma = \pi(K) \cap R_4(q)$ и H — σ-холлова подгруппа в K. Пусть $r \in \pi(K)\backslash\sigma$ и U — $\sigma \cup \{r\}$-холлова подгруппа в K. Пусть m — какой-нибудь делитель из $R_3(q)$, если $r \in R_2(q)$, иначе положим m равным любому числу из $R_6(q)$. Применяя аргумент Фраттини к U, получаем, что m делит порядок $N_G(U)$. Элемент порядка m из $N_G(U)$ действует как автоморфизм на U без неподвижных точек, поэтому по теореме Томпсона U нильпотентна. Следовательно, $K = T \times H$ для холловой σ'-подгруппы T в K. Пусть $\overline{K} = K/T$, $\overline{G} = G/T$. Если q нечетно, то по лемме 1.5 в группе $G_2(q)$ есть группа Фробениуса с ядром порядка q^2 и циклическим дополнением порядка (q^2-1), поэтому по лемме 1.4 в G есть элемент порядка $t(q^2-1)$, где $t \in r_4(q)$. В силу лемм 2.1 и 2.2 в $\mu(L)$ только числа q^2-1 и $p(q^2-1)$ кратны q^2-1; противоречие. Если же q четно, то по лемме 1.5 в группе $G_2(q)$ есть группа Фробениуса с ядром порядка $q^2 - \varepsilon q + 1$ для некоторого ε из $\{-1, 1\}$ и циклическим дополнением порядка 6, поэтому по лемме 1.4 в G есть элемент порядка $6t$, где $t \in R_4(q)$. Числа q^4-1 и $2(q^2+1)$ не делятся на 6; получаем противоречие с леммами 2.3 и 2.4.

Теорема 1 доказана.

Чтобы доказать теорему 2, нужно сначала показать, что S не может быть изоморфна группе лиева типа над полем нечетной характеристики.

Лемма 3.3. *Если $p = 2$ и S — группа лиева типа над полем нечетной характеристики, то $S \in \{A_1(u), C_2(u), A_2(3), A_3(3), {}^2A_2(3), {}^2A_2(5), {}^2A_3(3), B_3(3), D_4(3), G_2(3), {}^2G_2(3^{2s+1})\}$, где u — степень нечетного простого числа v.*

Доказательство. При доказательстве этой леммы будем пользоваться строением спектров простых линейных и унитарных групп из [15], симплектических и ортогональных — из [12].

Пусть $S \simeq A_2(u)$. Тогда группа S содержит элемент порядка $\frac{u^2-1}{(3,u-1)}$, это число делится на 8, поэтому в силу лемм 2.3 и 2.4 равняется ему. Пусть $u \equiv 1 (\bmod 3)$, тогда $u^2 - 1 = 24$, поэтому $u = 5$; противоречие, так как $u-1$ должно делиться на 3. Пусть $u \equiv 2 (\bmod 3)$ или $u \equiv 0 (\bmod 3)$, тогда $u^2 - 1 = 8$, Следовательно, $u = 3$. Если S — исключительная группа лиева типа над полем порядка u, где u — степень простого числа v, то либо $S \simeq {}^2G_2(3^{2s+1})$, либо S в силу [16, табл. OA28] содержится в следующем ряду: $A_2(u) \prec G_2(u) \prec {}^3D_4(u) \prec F_4(u) \prec E_6^*(u) \prec E_7(u) \prec E_8(u))$, где $A \prec B$ означает, что A изоморфна фактор-группе подгруппы из B, а $E_6^*(u)$ — эта любая из групп ${}^2E_6(u)$, $E_6(u)$. По ранее доказанному $u = 3$. Группа ${}^3D_4(u)$ содержит элемент порядка 28, поэтому в этом случае получаем, что $S \simeq G_2(3)$ или $S \simeq {}^2G_2(3^{2s+1})$, $s \geq 1$.

Пусть $S \simeq A_{n-1}(u)$, докажем, что $n = 2$ или $S = A_2(3)$, $A_3(3)$. В предыдущем рассуждении показывается, что если $n = 3$, то $u = 3$. Пусть $n \geq 4$. Тогда в S есть элемент порядка $u^2 - 1$, который делится на 8 и больше 8 при $u > 3$. Поэтому $u = 3$. При $n \geq 5$ в группе $A_{n-1}(u)$ есть элемент порядка $v(u^2-1)$. Получаем требуемое.

Пусть $S \simeq {}^2A_{n-1}(u)$. При $n = 3$ в S есть элемент порядка $\frac{u^2-1}{(3,u+1)}$, который делится на 8, значит, равен 8. Если $u \equiv 0 (\bmod 3)$, то $u^2 - 1 = 8$, стало быть, $u = 3$. Для $u \equiv 1 (\bmod 3)$ должно быть выполнено $u^2 - 1 = 8$, что несовместимо. Наконец, если $u \equiv 2 (\bmod 3)$, то $\frac{u^2-1}{3} = 8$, следовательно, $u = 5$. Если $n = 4$, то $u^2 - 1 \in \omega(S)$, это число делится на 8, поэтому $u^2 - 1 = 8$, значит, $u = 3$. При

$n \geq 5$ выполнено $v(u^2-1) \in \omega(S)$. В итоге среди унитарных групп возможны ${}^2A_2(3)$, ${}^2A_2(5)$ и ${}^2A_3(3)$.

Пусть $S \simeq B_n(u)$ или $C_n(u)$. Группа $B_n(u)$ при $n \geq 4$ и группа $C_n(u)$ при $n \geq 3$ содержат элемент порядка $v(u^2-1)$. Если же $S \simeq B_3(u)$, то $u^2-1 \in \omega(S)$, поэтому $u^2-1=8$, следовательно, $u=3$. Группы $B_2(u)$ и $C_2(u)$ изоморфны, тем самым в этом случае получаем, что $S \simeq B_2(u)$ либо $B_3(3)$.

Наконец, пусть $S \simeq D_n(u)$ или ${}^2D_n(u)$. Можно считать, что $n \geq 4$. При $n \geq 5$ в S есть элемент порядка $v(u^2-1)$, поэтому $n=4$. Группа ${}^2D_4(u)$ содержит элемент порядка $(u^4-1)/2$, значит, она не подходит. В группе $D_4(u)$ есть элемент порядка u^2-1, тем самым в этом случае $u=3$. $\square$

Лемма 3.4. *Существует два таких различных нечетных элемента d_1 и d_2 в $\mu(S)$, что $k_3(q)$ делит d_1, $k_6(q)$ делит d_2 и для каждой такой пары (d_1, d_2) число d_1 делит q^3-1, а d_2 делит q^3+1.*

Доказательство. По лемме 1.3 для любого простого числа r, не смежного с 2 в $GK(G) = GK(L)$, число r взаимно просто с $|K||\overline{G} : S|$, где $\overline{G} = G/K$. Пусть R — прообраз S относительно K в G. Обозначим через C циклическую подгруппу порядка $\frac{q^3-1}{(q-1,3)}$ в G. Тогда порядок $C_1 = C \cap R$ делится на $k_3(q)$, как и порядок $C_2 = C_1K/K$. Поскольку C_2 — циклическая подгруппа в S, число $k_3(q)$ делит некоторый элемент d_1 в $\mu(S)$. Нетрудно проверить, что четные элементы в $\mu(L)$ не делятся на $k_3(q)$, поэтому d_1 нечетно. Аналогично показывается, что существует такое число $d_2 \in \mu(S)$, что $k_6(q)$ делит d_2. Число d_1 не может делиться на $k_6(q)$, поэтому $d_1 \neq d_2$. Если d_1 делит некоторый элемент m из $\mu(G) = \mu(L)$, то по леммам 2.3 и 2.4 выполняется $m = q^3-1$, аналогично d_2 делит q^3+1. Лемма доказана. $\square$

Лемма 3.5. *Пусть S — группа лиева типа над полем нечетной характеристики, причем $8k \notin \omega(S)$ при $k > 1$. Тогда S и $\mu(S)$ содержатся в табл. 1.*

Таблица 1

S	$\mu(S)$
$A_1(u)$	$\{(u+1)/2, (u-1)/2, v\}$
$C_2(u)$, если $v \neq 3$	$\{u^2 \pm 1/2, v(u \pm 1)\}$
$C_2(u)$, если $v = 3$	$\{u^2 \pm 1/2, v(u \pm 1), 9\}$
$A_2(3)$	$\{13, 8, 6\}$
$A_3(3)$	$\{20, 18, 13, 12, 8\}$
${}^2A_2(3)$	$\{12, 8, 7\}$
${}^2A_2(5)$	$\{10, 8, 7, 6\}$
${}^2A_3(3)$	$\{12, 9, 8, 7, 5\}$
$B_3(3)$	$\{20, 18, 15, 14, 13, 12, 9, 8\}$
$D_4(3)$	$\{20, 18, 15, 14, 13, 12, 9, 8\}$
$G_2(3)$	$\{13, 12, 9, 8, 7\}$
${}^2G_2(3^{2s+1})$	$\{3^{2s+1}+3^{s+1}+1, 3^{2s+1}-3^{s+1}+1, 3^{2s+1}-1, (3^{2s+1}+1)/2, 6\}$

Доказательство. Возможные варианты для S получены в лемме 3.3. Для каждой такой группы S множество $\mu(S)$ получается из строения спектров групп лиева типа. $\square$

Лемма 3.6. *S неизоморфна группе лиева типа над полем нечетной характеристики.*

Доказательство. Заметим, что по лемме 3.4 в $\mu(S)$ должно быть хотя бы два нечетных числа, каждое из которых не меньше, чем $\min(k_3(q), k_6(q)) \geq (q^2-q+1)/3 \geq (8^2-8+1)/3 = 19$, поэтому $S \simeq A_1(u)$ или ${}^2G_2(3^{2s+1})$.

Если $S \simeq {}^2G_2(3^{2s+1})$, то в $\mu(S)$ есть четное число $3^{2s}-1$, которое должно делить одно из четных чисел в $\mu(L)$, следовательно, $3^{2s+1}-1 \leq 2(q^2+1)$. Поэтому $\sqrt{3}\cdot 3^s \leq \sqrt{2q^2+3} \leq \sqrt{3}\cdot q$, откуда $3^s \leq q$. Пусть $\varepsilon \in \{+,-\}$ такое, что $q^2+\varepsilon q+1$ не делится на 3. Из лемм 3.4, 3.5 следует, что для некоторого $\tau \in \{+,-\}$ число $q^2+\varepsilon q+1$ делит $3^{2s+1}+\tau 3^{s+1}+1$. Докажем, что эти числа не равны между собой. Если это не так, то $q(q+\varepsilon 1) = 3^{s+1}(3^s+\tau 1)$. Число q не делится на 3, поэтому $q+\varepsilon 1$ делится на 3^{s+1}, следовательно, $q+\varepsilon 1 \geq 3^{s+1}$, откуда $q \geq 3^{s+1}-\varepsilon 1 > 3^s+\tau 1$. Получаем, что $q(q+\varepsilon 1) > 3^{s+1}(3^s+\tau 1)$; противоречие. Значит, $3^{2s+1}+\tau 3^{s+1}+1 = k(q^2+\varepsilon q+1)$ для натурального числа $k>1$. Очевидно, что k нечетно и не равно 3, следовательно, $k \geq 5$. Учитывая полученные ранее оценки для 3^{2s+1} и 3^s, выводим следующую цепочку неравенств: $5(q^2+\varepsilon q+1) \leq 3^{2s+1}+\tau 3^{s+1}+1 \leq 2q^2+3+3q+1$, откуда $3q^2+1 \leq (3-\varepsilon 5)q$. Но $q \geq 8$, поэтому $3q^2+1 \geq 24q+1 > (3-\varepsilon 5)q$; противоречие.

Значит, $S \simeq A_1(u)$. Докажем, что $u = v$. Предположим, что $u \geq v^2$. В $\mu(A_1(u))$ ровно два нечетных числа: v и $(u-\varepsilon 1)/2$ для некоторого $\varepsilon \in \{+,-\}$. Поэтому по лемме 3.4 $v \geq (q^2-q+1)/3$. Число $(u+\varepsilon 1)/2$ четно, тем самым оно делит одно из четных чисел из $\mu(L)$, следовательно, $(u+\varepsilon 1)/2 \leq 2(q^2+1)$, поэтому $(q^2-q+1)/3 \leq v \leq \sqrt{u} \leq \sqrt{4q^2+5}$, что невозможно при $q \geq 8$.

Получаем, что $u = v$. По леммам 3.4 и 3.5 число v большее из нечетных чисел в $\mu(S)$. Учитывая, что оно простое, получаем, что $v = q^2+\varepsilon q+1$ для некоторого $\varepsilon \in \{+,-\}$. Тогда нечетным будет $(v+1)/2 = (q^2+\varepsilon q)/2+1$. Это число должно делиться на $(q^2-\varepsilon q+1)/3$, поэтому $(q^2+\varepsilon q)/2+1 = k((q^2-\varepsilon q+1)/3)$, где k — нечетное натуральное число. При $k=1$ это равенство эквивалентно $q^2+\varepsilon 5q+4 = 0$, чего не может быть, так как $q^2 \geq 8q$. Следовательно, $k \geq 3$, но тогда $k((q^2-\varepsilon q+1)/3) \geq q^2-\varepsilon q+1 = (q^2+\varepsilon q+2)/2+(q^2-\varepsilon 2q)/2 > (q^2+\varepsilon q+2)/2$; противоречие. Лемма доказана. □

В силу теоремы 1 имеем $S \in \{C_3(q), D_4(q)\}$.

Лемма 3.7. $K = 1$.

Доказательство. Если K нетривиальна, то в силу разрешимости K для некоторого простого r подгруппа $O^r(K)$ нетривиальна. Пусть $\overline{K} = K/O^r(K)$, $\overline{G} = G/O^r(K)$. В $\overline{G}$ существует группа Фробениуса с ядром порядка q^3 и дополнением порядка q^3-1 (для $C_3(q)$ см. лемму 2.8 в [17], кроме того, известно, что при четном q группа $C_3(q)$ вкладывается в $D_4(q)$). Поэтому при $r \neq 2$ по лемме 1.4 в группе $\overline{G}$ есть элемент порядка $r(q^3-1)$, что невозможно, так как q^3-1 является элементом множества $\mu(L)$. Значит, $r=2$. Заметим, что без ограничения общности можно считать, что $\overline{K}$ — элементарная абелева 2-группа, а действие $\overline{G}$ на $\overline{K}$ точное. Пусть U — естественный 2-модуль группы S, $x \in S$, $|x| = 3$ и $\dim C_U(x) = 4$. Тогда в S найдется подгруппа $A \simeq SL_3(q)$ такая, что $x \in A$ и $x \notin Z(A)$. По [18, лемма 1] имеем $V = C_{\overline{K}} \neq 1$. В группе $C_S(x)$ содержится подгруппа, изоморфная $\langle x\rangle \times M$, где $M \simeq C_2(q)$. Группа M содержит подгруппу Фробениуса с циклическим ядром J порядка q^2+1 и дополнением порядка 4. Если $C_V(J) \neq 1$, то $2\cdot 3\cdot (q^2+1) \in \omega(\overline{G})$. Если $C_V(J) = 1$, то по лемме 1.4 имеем $8\cdot 3 \in \omega(\overline{G})$; противоречие. Значит, K тривиальна. Лемма доказана. □

Лемма 3.8. $G = L$.

Доказательство. Из предыдущей леммы следует, что $S \leq G \leq \mathrm{Aut}(S)$, где $S \in \{C_3(q), D_4(q)\}$. Пусть $L = C_3(q)$ и $G \not\simeq L$, тогда $S \simeq C_3(q)$, так как $q^4 - 1 \in \omega(D_4(q))\backslash\omega(C_3(q))$. В этом случае $\mathrm{Out}(L)$ состоит только из полевых автоморфизмов. Пусть $x \in G\backslash S$ и $|x| = r$ для некоторого простого числа r. Тогда $D = C_S(x) \simeq C_3(2^{k/r})$ (см. [19, предложение 4.9.2]). Если $r \neq 2$, то x централизует элемент порядка 8 из D, поэтому $8r \in \omega(G)$; противоречие. Значит, $r = 2$. В этом случае по лемме 2.3 имеем $r(q\sqrt{q} - 1) \in \omega(G)$. Это число должно делить какое-то четное число из $\omega(L)$, очевидно, что это либо $2(q^2+1)$, либо $2(q^2-1)$. Но число q^2+1 делит $(\sqrt{q})^8-1$, q^2-1 делит $(\sqrt{q})^4-1$, поэтому они не могут делиться на числа из $r_3(\sqrt{q})$, каждое из которых является делителем $(\sqrt{q})^3 - 1$; противоречие. Значит, $G \simeq L$.

Пусть теперь $L \simeq D_4(q)$. Если $S \simeq C_3(q)$, то, как и в предыдущих рассуждениях, приходим к противоречию, показывая существование в $\omega(G)$ элемента порядка $8r$, где r — нечетное простое число, либо элемента порядка $2(q\sqrt{q} - 1)$. Значит, $S \simeq D_4(q)$. Предположим, что $G \not\simeq S$. Заметим, что каждый элемент из $\mathrm{Aut}(S)$ можно представить как произведение внутреннего, диагонального, полевого и графового автоморфизмов (см. [20, теорема 12.5.1]). В нашем случае в $\mathrm{Out}(S)$ группа диагональных автоморфизмов единична, группа полевых автоморфизмов циклическая порядка k, а группа графовых автоморфизмов изоморфна Sym_6. Можно считать, что в $G\backslash S$ есть автоморфизм δ простого порядка r.

Допустим, что δ — это полевой автоморфизм. Тогда $C_S(\delta) \simeq D_4(2^{k/r})$ (см. [19, предложение 4.9.2]). Рассуждая, как в случае группы $C_3(q)$, получаем противоречие.

Допустим, что δ — это графовый автоморфизм и $r = 3$. В этом случае $C_S(\delta) \simeq G_2(q)$ (см. [19, теорема 4.7.3]). Поскольку в группе $G_2(q)$ есть элемент порядка 8, то $24 \in \omega(G)$; противоречие. Пусть δ — это графово-полевой автоморфизм и $r = 3$. Тогда $C_S(\delta) \simeq^3 D_4(\sqrt{q})$ (см. [19, предложение 4.9.1]). В группе ${}^3D_4(\sqrt{q})$ есть элемент порядка 8, поэтому $24 \in \omega(G)$; противоречие. Допустим, что δ — графовый автоморфизм и $r = 2$. В этом случае $C_S(\delta) \simeq C_3(q)$ (см. [19, предложение 4.9.2]). Как и в случае полевого автоморфизма порядка 2 для группы $C_3(q)$, получаем противоречие с тем, что $2(q\sqrt{q} - 1) \in \omega(G)$. Пусть δ — графово-полевой автоморфизм и $r = 2$, тогда $C_S(\delta) \simeq^2 D_4(\sqrt{q})$ (см. [19, предложение 4.9.2]). В группе ${}^2D_4(\sqrt{q})$ есть элемент порядка $q(\sqrt{q} - 1)$ (см. [12]), поэтому $2(q\sqrt{q} - 1) \in \omega(G)$. Этого не может быть, как доказывалось ранее.

Теорема 2 доказана. □

ЛИТЕРАТУРА

1. *Мазуров В. Д.* Группы с заданным спектром // Изв. Урал. гос. ун-та. Математика, механика. 2005. Вып. 7, № 36. С. 119–138.
2. *Мазуров В. Д.* Характеризации конечных групп множествами порядков их элементов // Алгебра и логика. 1997. Т. 36, № 1. С. 37–53.
3. *Мазуров В. Д.* Распознавание конечных простых групп $S_4(q)$ по порядкам их элементов // Алгебра и логика. 2002. Т. 41, № 2. С. 166–198.
4. *Горшков И. Б.* Распознавание по спектру конечных простых групп, простые делители порядков которых не превосходят 17 // Сиб. электрон. мат. изв. 2010. Т. 7. С. 14–20.
5. *Conway J. H, Curtis R. T., Norton S. P., Parker R. A., Wilson R. A.* Atlas of finite groups. Oxford: Clarendon Press, 1985.
6. *Zsigmondy K.* Zür Theorie der Potenzreste // Monatsh. Math. Phys. 1892. Bd 3. S. 265-284.
7. *Roitman M.* On Zsigmondy primes // Proc. Amer. Math. Soc. 1997. V. 125, N 7. P. 1913–1919.

8. *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.
9. *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.
10. *Мазуров В. Д.* Характеризация конечных групп множествами порядков их элементов // Алгебра и логика. 1997. Т. 36, № 1. С. 37–53.
11. *Васильев А. В.* Распознаваемость групп $G_2(3^n)$ по порядкам их элементов // Алгебра и логика. 2002. Т. 41, № 2. С. 130–142.
12. *Бутурлакин А. А.* Спектры конечных симплектических и ортогональных групп // Мат. тр. 2010. Т. 13, № 2. С. 33–83.
13. *Васильев А. В., Гречкосеева М. А., Мазуров В. Д.* О конечных группах, изоспектральных простым симплектическим и ортогональным группам // Сиб. мат. журн. 2009. Т. 50, № 6. С. 1225–1247.
14. *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.
15. *Бутурлакин А. А.* Спектры конечных линейных и унитарных групп // Алгебра и логика. 2008. Т. 47, № 2. С. 157–173.
16. *Stensholt E.* Certain embeddings among finite groups of Lie type // J. Algebra. 1978. V. 53, N 1. P. 136–187.
17. *Deng H. W., Shi W. J.* Recognition of some finite simple groups of type $D_n(q)$ by spectrum // Int. J. Algebra Comput. 2009. V. 19, N 5. P. 681–698.
18. *Заварницин А. В., Мазуров В. Д.* О порядках элементов в накрытиях простых групп $L_n(q)$ и $U_n(q)$ // Тр. Ин-та математики и механики УрО РАН. 2007. Т. 13. С. 89–98.
19. *Gorenstein D., Lyons R., Solomon R.* The classification of the finite simple groups. Providence, RI: Amer. Math. Soc., 1998. N 3. (Math. Surv. Monogr.; V. 40).
20. *Carter R.* Simple groups of Lie type. London: John Wiley&Sons, 1972.

Статья поступила 15 июня 2011 г.

Старолетов Алексей Михайлович
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
astaroletov@gmail.com