Сибирский математический журнал
Январь—февраль, 2007. Том 48, № 1

УДК 512.542

О РАЗЛИЧИИ СПЕКТРОВ ПРОСТЫХ ГРУПП $B_n(q)$ И $C_n(q)$

М. А. Гречкосеева

Аннотация: Доказывается, что любые две неизоморфные простые группы $B_n(q)$ и $C_n(q)$ имеют разные множества порядков элементов.

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

Спектром $\omega(G)$ конечной группы G называется множество порядков ее элементов. Спектр возникает в таких задачах характеризации групп, как задачи распознавания групп по спектру или по спектру и порядку. Будем называть конечную группу G *распознаваемой по спектру и порядку в классе* $\mathscr{C}$, если любая группа H из $\mathscr{C}$, удовлетворяющая условиям $\omega(H) = \omega(G)$ и $|H| = |G|$, изоморфна G. В Коуровской тетради [1] записан вопрос 12.39, поставленный Ши: верно ли, что любая конечная простая группа распознаваема по спектру и порядку в классе всех конечных групп? Из результатов, полученных Ши и его соавторами (см. обзор в [2]), следует, что для ответа на вопрос осталось проверить свойство распознаваемости для простых групп лиева типа B_n, C_n и D_{2n}.

Очевидно, что необходимым условием распознаваемости группы в классе всех конечных групп является ее распознаваемость в классе конечных простых групп. Для любых n и q простые группы $B_n(q)$ и $C_n(q)$ имеют одинаковые порядки. Эти группы изоморфны, когда $n = 2$ или q четно, и не являются изоморфными в остальных случаях. Естественным образом возникает вопрос о том, различаются ли в этих случаях их спектры. Цель данной работы — показать, что неизоморфные простые группы $B_n(q)$ и $C_n(q)$ имеют разные спектры.

Приведем некоторые известные факты о множествах $\omega(B_n(q))$ и $\omega(C_n(q))$. Пусть G — группа лиева типа, определенная над конечным полем порядка q и характеристики p. Естественно выделить в $\omega(G)$ два подмножества: $\omega_p(G)$ — множество порядков p-элементов группы G и $\omega_{p'}(G)$ — множество порядков p'-элементов группы G. Кроме того, на множестве простых делителей порядка группы G определим граф простых чисел $GK(G)$ по следующему правилу: две различные вершины r_1 и r_2 смежны тогда и только тогда, когда $r_1 \cdot r_2 \in \omega(G)$. Из предложения 0.5 работы [3] вытекает, что для любых n и q множества $\omega_p(B_n(q))$ и $\omega_p(C_n(q))$ совпадают. Из рассмотрения максимальных торов в соответствующих группах следует, что для любых n и q множества $\omega_{p'}(B_n(q))$ и $\omega_{p'}(C_n(q))$ также совпадают. Наконец, в [4], в качестве следствия из критерия

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 05–01–00797), Совета по грантам Президента РФ и государственной поддержке ведущих научных школ (проект НШ–2069.2003.1), Президиума СО РАН (интеграционный проект 2006.1.2).

смежности в графах простых чисел конечных простых групп, установлено, что $GK(B_n(q)) = GK(C_n(q))$ для любых n и q.

Таким образом, симметрическая разность множеств $\omega(B_n(q))$ и $\omega(C_n(q))$ состоит из элементов вида prr_1, где r — простое число, отличное от p, и $r_1 \neq 1$. В настоящей работе показано, что эта разность непуста. Отметим, что для найденного элемента $r = 2$ и r_1 взаимно просто с p.

Теорема. *Пусть q — степень нечетного простого числа p, n — натуральное число, большее 2. Тогда $p(q^{n-1}+1) \in \omega(C_n(q)) \setminus \omega(B_n(q))$.*

Доказательство. Для конечной группы G и простого числа p обозначим через $\omega_{p'}(G)$ множество p'-частей элементов из $\omega(G)$. Для доказательства включения $p(q^{n-1}+1) \in \omega(C_n(q))$ мы воспользуемся матричным представлением группы $C_n(q)$. Группа $C_n(q)$ изоморфна простой симплектической группе $PSp_{2n}(q)$.

Лемма 1. *Пусть $q = p^k$, $n \geq 2$. Тогда $p \cdot \omega_{p'}(Sp_{2n-2}(q)) \subseteq \omega(PSp_{2n}(q))$.*

Доказательство. Рассмотрим элемент X группы $Sp_{2n}(q)$, являющийся трансвекцией с нетривиальным $(1, n+1)$-м элементом. Порядок этого элемента равен p. Подгруппа P группы $Sp_{2n}(q)$, состоящая из всех симплектических матриц вида $\begin{pmatrix} A & B \\ C & D \end{pmatrix}$, где $A, B, C, D \in M_n(q)$ и

$$A = \begin{pmatrix} 1 & 0 \\ 0 & A' \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 0 & B' \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 \\ 0 & C' \end{pmatrix}, \quad D = \begin{pmatrix} 1 & 0 \\ 0 & D' \end{pmatrix},$$

централизует матрицу X. Группа P изоморфна группе $Sp_{2n-2}(q)$ и не содержит центр группы $Sp_{2n}(q)$, состоящий из матриц $\pm E$. Таким образом, спектр образа группы $\langle X \rangle \times P$ в $PSp_{2n}(q)$ содержит множество $p \cdot \omega_p(Sp_{2n-2}(q))$. Лемма доказана.

Хорошо известно, что в группе $Sp_{2n-2}(q)$ есть циклическая группа порядка $q^{n-1}+1$, так называемый цикл Зингера (см. [5, теорема 5.6]). Следовательно, по лемме 1 в группе $C_n(q)$ есть элемент порядка $p(q^{n-1}+1)$.

Для доказательства второй части утверждения теоремы нам потребуется представление конечных групп лиева типа как множеств неподвижных точек некоторых эндоморфизмов простых алгебраических групп. Пусть G — простая односвязная алгебраическая группа типа B_n над алгебраически замкнутым полем характеристики p. Пусть σ — сюръективный эндоморфизм группы G, полученный из морфизма, возводящего матричные коэффициенты в q-ю степень. Для σ-инвариантной подгруппы H группы G обозначим централизатор σ в H через H_σ. Группа G_σ конечна и изоморфна универсальной группе Шевалле типа B_n над полем порядка q. Простая группа $B_n(q)$ изоморфна фактор-группе $G_\sigma/Z(G_\sigma)$.

Предположим, что в группе $G_\sigma/Z(G_\sigma)$ есть элемент x порядка $p(q^{n-1}+1)$. Обозначим через s полупростую часть прообраза элемента x в G_σ. Централизатор $C_{G_\sigma}(s)$ равен $(C_G(s))_\sigma$. Поскольку группа G односвязна, по теореме 3.6.5 из [6] группа $C_G(s)$ связна и, следовательно, по теореме 3.5.4 из [6] является редуктивной подгруппой максимального ранга группы G. Такие подгруппы для простых алгебраических групп нормального лиева типа описаны в статье [7]. Нам потребуются некоторые обозначения и утверждения из этой статьи.

Пусть G_1 — σ-инвариантная редуктивная подгруппа группы G максимального ранга, T — σ-инвариантный максимальный тор группы G, содержащийся в G_1. Пусть Φ — корневая система группы G относительно тора T, X_α — корневая подгруппа, соответствующая корню α. Тогда $G_1 = \langle T, X_\alpha, \alpha \in \Phi_1 \rangle$, где Φ_1 — некоторая подсистема системы Φ.

Корневую систему типа B_n можно представить в виде

$$\Phi = \{\pm e_i \pm e_j, \pm e_i : 1 \leqslant i < j \leqslant n\},$$

где $e_1, e_2, \ldots, e_n$ — это ортонормированный базис n-мерного евклидова пространства. Подсистемы системы Φ получаются следующим образом. Пусть λ и μ — разбиения с условием $|\lambda| + |\mu| \leq n$, причем никакая часть разбиения μ не равна 1. Положим $\nu = n - |\lambda| - |\mu|$. Пусть $I_1, I_2, \ldots, J_1, J_2, \ldots$ — попарно не пересекающиеся подмножества множества $\{1, 2, \ldots, n\}$ такие, что $|I_l| = \lambda_l$ и $|J_l| = \mu_l$, и пусть K — дополнение объединения множеств $I_1, I_2, \ldots, J_1, J_2, \ldots$ в множестве $\{1, 2, \ldots, n\}$. Тогда

$$\Phi_1 = \bigcup_l \{e_i - e_j : i \neq j, i, j \in I_l\} \bigcup_l \{\pm e_i \pm e_j : i \neq j, i, j \in J_l\} \\ \cup \{\pm e_i \pm e_j, \pm e_i : i \neq j, i, j \in K\}$$

является подсистемой системы Φ и любая подсистема системы Φ эквивалентна некоторой системе Φ_1 относительно группы Вейля W системы Φ.

Сопряженная в G с G_1 подгруппа G_1^g будет σ-инвариантной тогда и только тогда, когда элемент $g^\sigma g^{-1}$ принадлежит $N_G(T)$ и его образ w при естественном гомоморфизме π из $N_G(T)$ в W лежит в $N_W(W_1)$, где W_1 — группа Вейля системы Φ_1. Группы $G_1^{g_1}$ и $G_2^{g_2}$ сопряжены элементом из G_σ тогда и только тогда, когда смежные классы $W_1 w_1$ и $W_1 w_2$ соответствующих элементов w_1 и w_2 сопряжены в $N_W(W_1)/W_1$.

Таким образом, с точностью до сопряжения элементом из G_σ любая σ-инвариантная редуктивная подгруппа группы G максимального ранга однозначно определяется тройкой (λ, μ, ν) и классом сопряженности группы $N_W(W_1)/W_1$.

Пусть $M = \langle X_\alpha, \alpha \in \Phi_1 \rangle$, и пусть S — компонента связности центра группы G_1. Тогда M — полупростая группа, S — тор и $G_1 = MS$. Если G_1^g является σ-инвариантной, то таковыми являются и группы M^g и S^g. Порядок группы $\big(G_1^g\big)_\sigma$ равен произведению порядков групп $(M^g)_\sigma$ и $(S^g)_\sigma$.

Лемма 2 [7, предложение 11]. *Пусть G — группа типа B_n, $n \geq 3$, над алгебраически замкнутым полем нечетной характеристики. Пусть G_1 — редуктивная подгруппа максимального ранга группы G с системой корней Φ_1, определенной тройкой (λ, μ, ν). Пусть m_i — число частей разбиения λ, равных i, и n_i — число частей разбиения μ, равных i. Пусть G_1^g — σ-инвариантная редуктивная подгруппа группы G с $\pi(g^\sigma g^{-1}) = w \in W$. Предположим, что при естественном гомоморфизме из $N_W(W_1)$ в группу автоморфизмов диаграммы Дынкина системы Φ_1 элемент w переходит в τ и τ дает пару разбиений $\xi^{(i)}$, $\eta^{(i)}$ с условием $|\xi^{(i)}| + |\eta^{(i)}| = m_i$ и пару разбиений $\zeta^{(i)}$, $\theta^{(i)}$ с условием $|\zeta^{(i)}| + |\theta^{(i)}| = n_i$. Тогда простые компоненты группы $(M^g)_\sigma$ имеют тип $A_{i-1}(q^{\xi_j^{(i)}})$, ${}^2A_{i-1}(q^{2\eta_j^{(i)}})$, $D_i(q^{\zeta_j^{(i)}})$, ${}^2D_i(q^{2\theta_j^{(i)}})$ по одной компоненте на каждую часть разбиений $\xi^{(i)}$, $\eta^{(i)}$, $\zeta^{(i)}$, $\theta^{(i)}$. Порядок тора $(S^g)_\sigma$ дается формулой $\Pi_{i,j}(q^{\xi_j^{(i)}} - 1)\Pi_{i,j}(q^{\eta_j^{(i)}} + 1)$.*

Пусть $C_G(s) = G_1^g$, где G_1 определяется тройкой (λ, μ, ν) и $\pi(g^\sigma g^{-1}) = w$. Поскольку $s \in Z\big(G_1^g\big)$ и $\big|Z\big(G_1^g\big) : S^g\big| \leq 2$, то $s^2 \in (S^g)_\sigma$. Пусть r_n — примитивный простой делитель числа $q^{2n-2} - 1$, т. е. простое число, делящее $q^{2n-2} - 1$ и не делящее $q^l - 1$ для всех $l < 2n - 2$. Такое число существует по теореме Жигмонди [8]. Тогда r_n делит порядок элемента s^2 и, следовательно, r_n делит порядок тора $(S^g)_\sigma$. Поскольку все части разбиений $\xi^{(i)}$ не превосходят n, число r_n не может делить множители вида $q^{\xi_j^{(i)}}-1$. Если для любого i все части разбиения $\eta^{(i)}$ меньше $n-1$, то число r_n не может делить порядок тора $(S^g)_\sigma$. Таким образом, для некоторых i и j выполнено $\left|\eta_j^{(i)}\right| \geq n-1$. Значит, $m_i \geq n-1$. Поскольку только частей размера 1 может быть больше, чем $n/2$, это i равно 1. Если $|\lambda| = n$, то по лемме 2 полупростая часть группы $\left(G_1^g\right)_\sigma$ тривиальна, но по нашему предположению в группе $\left(G_1^g\right)_\sigma = C_{G_\sigma}(s)$ есть элемент порядка p. Значит, $|\lambda| = m_1 = n-1$, и, следовательно, μ пусто, $\nu = 1$. Таким образом, можно считать, что $\Phi_1 = \{\pm e_n\}$.

Пусть X — группа рациональных характеров тора T. Для замкнутой подгруппы T_1 тора T положим $T_1^\perp = \{\chi \in X : \chi(t) = 1$ для всех $t \in T_1\}$. Предложение 7 из [9] утверждает, что группа T_1 связна тогда и только тогда, когда $X/T_1^\perp$ не содержит периодических подгрупп. Поскольку группа G односвязна, группа X, рассматриваемая как аддитивная группа, совпадает с решеткой весов системы Φ и равна $\mathbb{Z}\left\{\frac{1}{2}(\pm e_i \pm e_j), \pm e_i : 1 \leqslant i < j \leqslant n\right\}$. Группа $Z(G_1)$ равна $\{t \in T : e_n(t) = 1\}$, следовательно, $Z(G_1)^\perp = \mathbb{Z}\{\pm e_n\}$. Фактор-группа $X/Z(G_1)^\perp$ — свободная абелева группа ранга $n-1$, значит, $Z(G_1)$ связна, т. е. $S = Z(G_1)$. Таким образом, $s \in S^g$ и $Z(G) \leq S^g$.

Поскольку $s \in (S^g)_\sigma$ и $|(S^g)_\sigma| = q^{n-1}+1$, порядок s равен $q^{n-1}+1$ и $(S^g)_\sigma = \langle s \rangle$. Получаем, что группа $\langle s \rangle$ содержит группу $(Z(G))_\sigma$, которая по предложению 3.6.8 из [5] совпадает с группой $Z(G_\sigma)$. Следовательно, образ элемента s в $G_\sigma/Z(G_\sigma)$ имеет порядок $\frac{1}{2}(q^{n-1}+1)$, что противоречит выбору элемента s. Теорема доказана.

ЛИТЕРАТУРА

1. *Коуровская тетрадь.* Нерешенные вопросы теории групп. 15-е изд. (ред. Мазуров В. Д., Хухро Е. И.). Новосибирск: Изд-во Ин-та математики СО РАН, 2002.
2. *Shi W. J., Xu M.* Pure quantitative characterization of finite simple groups ${}^2D_n(q)$ and $D_l(q)$ (l odd) // Algebra Colloq. 2003. V. 10, N 3. P. 427–443.
3. *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.
4. *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.
5. *Hestenes M. D.* Singer groups // Canad. J. Math. 1970. V. 22, N 3. P. 492–513.
6. *Carter R. W.* Finite groups of Lie type: Conjugacy classes and complex characters. New York: John Wiley & Sons, 1985.
7. *Carter R. W.* Centralizers of semisimple elements in the finite classical group // Proc. London Math. Soc. (3). 1981. V. 42, N 1. P. 1–41.
8. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. Bd 3. S. 265–284.
9. *Carter R. W.* Centralizers of semisimple elements in finite groups of Lie type // Proc. London Math. Soc. (3). 1978. V. 37, N 3. P. 491–507.

Статья поступила 27 марта 2006 г.

Гречкосеева Мария Александровна
Новосибирский гос. университет, ул. Пирогова, 2, Новосибирск 630090
grechkoseeva@gorodok.net