Сибирский математический журнал
Сентябрь—октябрь, 2002. Том 43, № 5

УДК 512.542

РАСПОЗНАВАНИЕ ПО МНОЖЕСТВУ ПОРЯДКОВ ЭЛЕМЕНТОВ СИММЕТРИЧЕСКИХ ГРУПП СТЕПЕНИ r И $r+1$ ДЛЯ ПРОСТОГО r

А. В. Заварницин

Аннотация: Доказывается, что симметрическая группа S_r простой степени $r \geq 17$ распознаваема по множеству порядков элементов. Получен критерий распознаваемости симметрической группы S_{r+1}, где $r \geq 17$ простое.

Ключевые слова: конечная группа, порядок элемента, распознаваемость

Для произвольной конечной группы G обозначим через $\omega(G)$ множество порядков ее элементов. Говорят, что *группа G распознается* по своему множеству порядков элементов $\omega(G)$, если равенство $\omega(G) = \omega(H)$ влечет изоморфизм G и H для любой конечной группы H. В работах [1, 2] установлено, что знакопеременные группы степени r, $r+1$, $r+2$ для простого $r \geq 7$ распознаваемы по множеству порядков элементов. В доказательстве этих утверждений используется несвязность графа Грюнберга — Кегеля таких групп (определение см. в [1]). Симметрические группы степени r и $r+1$, где $r > 3$ простое, также имеют несвязный граф Грюнберга — Кегеля. Это позволило распространить те же идеи для доказательства следующей теоремы.

Теорема. 1. *Симметрическая группа простой степени $r \geq 17$ распознаваема по множеству порядков элементов.*

2. *Распознаваемость симметрической группы степени $r+1$, где $r \geq 17$ простое, эквивалентна следующему утверждению.*

Для любого собственного накрытия $G = N.A$ произвольной группы N с помощью группы A, изоморфной S_r или A_r, выполнено $\omega(G) \neq \omega(S_{r+1})$.

Отметим, что распознаваемость групп S_n для $n = 7, 9, 11, 12, 13, 14$ и нераспознаваемость для $n = 2, 3, 4, 5, 6, 8$ были установлены в работах [3–6]. Распознаваемость пропущенной здесь симметрической группы S_{10} пока остается под вопросом.

В настоящей работе используются те же обозначения, что и в [2].

Предварительные результаты

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 99–01–00550), гранта Минобразования РФ в области фундаментального естествознания (шифр Е00–1.0–77), ФЦП «Интеграция» (проект № 274) и гранта СО РАН для коллективов молодых ученых (постановление Президиума № 83 от 10.03.2000).

Лемма 1. *В интервале* $(m/2, m-15]$ *содержится по меньшей мере два простых числа, где* $m \geq 44$ *— натуральное число.*

Доказательство. Мы используем тот факт, что интервал $[3s, 4s]$ для натурального s содержит простое число (см. [7]). Пусть $m-15 = 16t + r$, где $0 \leq r \leq 15$. Тогда между $9t$ и $12t$, а также между $12t$ и $16t$ существует простое число. Покажем, что $m/2 \leq 9t$. Пусть, напротив, $9t < m/2$. Тогда $18t < m = 16t + r + 15 \leq 16t + 30$, откуда $t \leq 14$ и $m \leq 16 \cdot 14 + 30 = 254$. Для таких m утверждение легко проверить непосредственно. Лемма доказана.

Лемма 2. *Если* $m \geq 4$, $m \neq 8, 14$ *и* p *простое, то* $\omega(Z_p \times A_m) \nsubseteq \omega(A_{m+2})$.

Доказательство будем вести индукцией по m. Если $4 \leq m \leq 43$ и $m \neq 8, 14$, то утверждение можно проверить перебором. Считаем, что $m \geq 44$. Тогда по лемме 1 существуют два простых числа из интервала $(m/2, m-15]$. Одно из них, скажем r, отлично от p. Поскольку $m - r \geq 15$ и $m/2 > r \neq p$, то по индукции существует число $a \in \omega(A_{m-r})$ такое, что $p \cdot a \notin \omega(A_{m-r+2})$. Поэтому $r \cdot p \cdot a \notin \omega(A_{m+2})$. Лемма доказана.

Лемма 3. *Для любого* $n \geq 11$ *существуют натуральное* k *и различные нечетные простые* $p_1, \dots, p_k$ *такие, что*

$$n - 1 \leq p_1 + p_2 + \dots + p_k \leq n,$$

причем все p_i *отличны от максимального простого* $p \leq n$.

Доказательство будем вести индукцией по n. Для $11 \leq n \leq 39$ утверждение легко проверить непосредственно. Пусть $n \geq 40$. Из леммы 1 следует, что существуют простые числа q_1, q_2 из интервала $(n/2, n-11]$. Одно из q_i не является максимальным, не превосходящим n. Обозначим его через p_1. Тогда $p_1 > n - p_1 \geq 11$ и по индукции $n - p_1 = p_2 + p_3 + \dots + p_k + \varepsilon$, где p_i — различные нечетные простые числа и $\varepsilon = 0$ или 1. Лемма доказана.

Лемма 4. *Пусть* $r \geq 17$ *простое и* P *— простая группа с несвязным графом* $GK(P)$, *не изоморфная знакопеременной, спорадической или лиевой группе ранга* 1. *Кроме того, пусть* $r = \max(\pi(P))$ *и* r *— компонента связности* $GK(P)$. *Если* $P \neq {}^2G_2(q)$, *то для любого* i *существует не более одного простого* $s \in \pi_i(P)$ *такого, что* $(r+1)/2 < s < r$. *Если* $P = {}^2G_2(q)$, *то существует не более трех простых* $s \in \pi(P)$ *таких, что* $(r+1)/2 < s < r$ *(здесь* $\pi_i(P)$ *— простые числа из* i*-й компоненты связности графа* $GK(P)$*) и любое простое* s, *удовлетворяющее* $(r+1)/2 < s < r$, *не делит* $|\operatorname{Out}(P)|$.

Доказательство. См. [1, лемма 6, пп. в, г].

Лемма 5. *Пусть* H *— конечная группа,* V *— собственная нормальная подгруппа в* H *и* V/H *изоморфна знакопеременной группе* A_m. *Тогда* $\omega(H) \nsubseteq \omega(A_{m+2})$, *если* $m \geq 6$ *и* $m \neq 8$, 14.

Доказательство. Без ограничения общности можно считать, что H — полупрямое произведение элементарной абелевой p-группы V на A_m. По лемме 2 можно считать, что A_m действует точно на V. Теперь утверждение следует из лемм 1.4–1.6 в [2]. Лемма доказана.

Эта лемма обобщает результат из [8] при $m \neq 5$, 8, 14 и лемму 1.7 из [2].

Отметим, что $\omega(Z_3 \times A_8) \subseteq \omega(A_{10})$ и $\omega(Z_3 \times A_{14}) \subseteq \omega(A_{16})$. А также существует полупрямое произведение S элементарной абелевой группы порядка 4^2 на группу A_5 такое, что $\omega(S) = \omega(A_6) \subseteq \omega(A_7)$. В качестве такого S можно взять естественный 2-мерный $SL_2(4)$-модуль над $GF(4)$.

Лемма 6. *Пусть H — конечная группа, V — собственная нормальная подгруппа в H и V/H изоморфна знакопеременной группе A_m. Тогда $\omega(H) \not\subseteq \omega(S_m)$, если $m \geq 6$ и $m \neq 8$.*

Доказательство. Заметим, что $\omega(S_m) \subseteq \omega(A_{m+2})$. При $m \neq 14$ утверждение — очевидное следствие леммы 5. Если $m = 14$, то утверждение следует из лемм 1.4–1.6 в [2] и того факта, что $\omega(Z_p \times A_{14}) \not\subseteq \omega(S_{14})$ для любого простого p. Лемма доказана.

Отметим, что существует полупрямое произведение $S = 2^6 : A_8$ такое, что $\omega(S) \subseteq \omega(S_8)$. В качестве S можно взять 6-мерный A_8-модуль, являющийся нетривиальным композиционным фактором регулярного A_8-модуля над полем $GF(2)$.

Доказательство теоремы

Пусть G — конечная группа, для которой $\omega(G) = \omega(S_n)$, где n равно r или $r+1$ и $r \geq 17$ простое. Поскольку граф $GK(G)$ несвязен, то по [9] верно одно из утверждений:

(а) $G = FC$ — группа Фробениуса и $\pi(F)$, $\pi(C)$ — компоненты связности графа $GK(G)$.

(б) $G = ABC$ — 2-фробениусова группа.

(в) G является расширением нильпотентной $\pi_1(G)$-группы N посредством группы A, где $P \leq A \leq \operatorname{Aut}(P)$ для простой неабелевой группы с несвязным графом $GK(P)$, а A/P — $\pi_1(G)$-группа.

Пусть выполнен случай (а). Если r делит $|F|$, то F — r-группа и $|C|$ — четное число. Поэтому в C есть центральная инволюция. Поскольку $n \geq r \geq 17$, то по лемме 3 существуют различные нечетные простые $p_1, \ldots, p_k$, отличные от r и такие, что

$$n - 1 \leq p_1 + \ldots + p_k \leq n. \tag{1}$$

Отсюда следует, что число $p_1 \cdot \ldots \cdot p_k$ лежит в $\omega(S_n) = \omega(G)$ и, значит, в $\omega(C)$. Но тогда в силу неравенства (1) имеем $\omega(S_n) \not\ni 2 \cdot p_1 \cdot \ldots \cdot p_k \in \omega(C)$; противоречие. Значит, $|C| = r$. Существует натуральное t такое, что $2^t \leq n < 2^{t+1}$. Пусть q — наибольшее простое, меньшее r. Так как $n \geq 17$, по лемме 1 из [1] $q > n/2 > 2$. Отсюда 2^t, $q \in \omega(G)$, но $\omega(G) = \omega(S_n) \not\ni 2^t \cdot q \in \omega(F) \subseteq \omega(G)$; противоречие.

Пусть выполнен случай (б). Тогда $|B| = r$ и C — циклическая группа порядка, делящего $r - 1$. Так как $r \geq 14$, то по лемме 1 из [1] существует пара простых чисел p_1 и p_2 таких, что $n/2 \leq (r+1)/2 < p_i < r \leq n$, где $i = 1, 2$, и тем самым p_1, p_2 делят $|A|$. Из нильпотентности группы A следует, что $\omega(S_n) \not\ni p_1 \cdot p_2 \in \omega(A) \subseteq \omega(G) = \omega(S_n)$; противоречие.

Значит, выполнен случай (в). Пусть N, A, P такие, как в условии.

1. Покажем, что $P \neq L_2(q)$.

1а. Если $P = L_2(q)$, $\pi(q) \neq r$ и q нечетно, то $(q + \varepsilon)/2 = r$, где $q \equiv \varepsilon(4)$, поскольку число r является максимальным простым делителем порядка $|P|$ и компонентой связности графа $GK(P)$. По лемме 1 из [1] существуют простые числа p_1, p_2 такие, что $(r+1)/2 < p_i < r$, $i = 1, 2$. Поскольку $|P| = q(q^2-1)/2$ и $|\operatorname{Out}(P)| = 2t$, где $q = p^t$ для простого p, и, как легко проверить, p_i не делят $|\operatorname{Aut}(P)|$, но $p_i \in \pi(S_n) = \pi(G)$, то p_i делят $|N|$. Ввиду нильпотентности N получаем $p_1 \cdot p_2 \in \omega(G) = \omega(S_n)$, однако $p_1 + p_2 > r + 1 \geq n$; противоречие. Случаи, когда q четно или $q = r$, рассматриваются аналогично.

1б. Если $P = L_2(q)$, $\pi(q) = r$ (т. е. $q = r^k$) и $k > 1$, то силовская r-подгруппа R в P нециклическая и, значит, $N = 1$. В силу того, что $N_G(R)$ — группа Фробениуса, имеем $|N_G(R)| \leq |R| - 1$ и $|G : P| \leq 2$. Все элементы из G нечетного порядка лежат в P. Так как $q^2 - 1$ делится на 3, то $3|q+\delta$, где $\delta = \pm 1$, и $3 \not| q - \delta$. Заметим, что $m = (q-\delta)2$ не степень простого, ибо иначе $m \in \omega(P) \subseteq \omega(G) = \omega(S_n)$ и $m \leq n \leq r+1 < (r^2-1)/2 \leq (r^k-1)/2 \leq m$; противоречие. Поэтому $m = uv$, где u и v взаимно просты, отличны от 1 и u нечетно. Но $m \in \omega(S_n)$ и, значит, существует подстановка $x \in S_n$ порядка m. Очевидно, что $|x^v| = u$ и подстановка x^v оставляет на месте по меньшей мере три точки. Поэтому $\omega(G) \ni 3u \notin \omega(P)$, так как $3u$ нечетно; противоречие.

2. P не изоморфна спорадической простой группе. Предположим противное. Заметим, что r — компонента связности графа $GK(P)$, $r = \max(\pi(G))$, $|\operatorname{Aut}(P)| \leq 2|P|$. Поэтому любое нечетное простое, меньшее r, делит $|NP|$. Ввиду нильпотентности N существует не более одного простого делителя p порядка $|N|$ такого, что $(r+1)/2 < p < r$. Из этих замечаний и таблиц простых групп с несвязным графом Грюнберга — Кегеля (см. [1 табл. 1–3]) следует, что $P = Fi_{23}$ или Fi'_{24}, порядок N делится на 19 и $r \leq 29$. Так как P содержит подгруппу Фробениуса порядка $17 \cdot 16$, то в G есть элемент порядка $19 \cdot 17$ или $19 \cdot 16$, но $\omega(S_n)$ не содержит таких чисел, так как $n \leq r+1 \leq 30$; противоречие.

3. Пусть P изоморфна простой лиевой группе ранга больше 1 над $GF(q)$. Учитывая лемму 4, лемму 1 из [1] и тот факт, что N делится самое большее на одно простое s, удовлетворяющее $(r+1)/2 < s < r$, получаем следующие утверждения.

(а) Если $s(P) = 2$, то $r < 18$ и P равно $C_2(4)$, $C_4(2)$, ${}^2D_4(2)$ или ${}^2D_5(2)$. Однако в первых трех случаях 11, 13 не принадлежат $\omega(\operatorname{Aut}(P))$ и делят $|N|$ вопреки нильпотентности N и тому, что $n \leq 18$. В случае $P =^2 D_5(2)$ имеем $13 \in \pi(N)$ и в P существует подгруппа Фробениуса порядка $17 \cdot 8$. Поэтому в $\omega(G) - \omega(S_n)$ лежит $13 \cdot 17$ или $13 \cdot 8$; противоречие.

(б) Если $s(P) = 3$ и $P \neq^2 G_2(q)$, то $r < 38$; если $s(P) = 3$ и $P =^2 G_2(q)$ или $s(P) = 4$, то $r < 42$; если $s(P) = 5$, то $r < 48$. Используя табл. 1–3 из [1], легко проверить, что при $s(P) > 2$ неравенство $r \leq 47$ выполнено только в следующих случаях: $P =^2 B_2(32)$ и $r = 41$, $P =^2 G_2(27)$ и $r = 37$, $P =^2 E_6(2)$ и $r = 19$, $P = F_4(2)$ и $r = 17$.

В первых двух случаях $23, 29 \in \pi(N)$, что невозможно, так как в этих случаях $n \leq r+1 \leq 42$. Если $P =^2 E_6(2)$, то $n = 19$ или 20. В S_n есть элементы порядков $13 \cdot 5$, $11 \cdot 7 \notin \omega(\operatorname{Aut}(P))$. Поэтому $|N|$ делится на $13 \cdot 7$, $5 \cdot 11$, или $5 \cdot 7$. Элемент порядка 19 из P не централизует в N элементов порядка 5, 7, 11, 13. Из существования в P подгруппы Фробениуса порядка $19 \cdot 9$ следует, что одно из чисел $13 \cdot 7 \cdot 9$, $5 \cdot 11 \cdot 9$, $5 \cdot 7 \cdot 9$ лежит в $\omega(G) = \omega(S_n)$, что противоречит тому, что $n \leq 20$.

Если $P = F_4(2)$ и $r = 17$, то $11 \in \pi(N)$. Элемент порядка 17 из P не централизует в N элементы порядка 11. Поэтому из существования в P группы Фробениуса порядка $17 \cdot 8$ вытекает, что $11 \cdot 8 \in \omega(G) = \omega(S_n)$, но $n \leq 18$; противоречие.

4. Итак, P — знакопеременная группа A_m, где m равно r, $r+1$ или $r+2$. По лемме 6 если $n = r$, то $N = 1$. Поскольку все множества $\omega(A_r)$, $\omega(A_{r+1})$, $\omega(A_{r+2})$, $\omega(S_{r+1})$, $\omega(S_{r+2})$ отличны от $\omega(S_r)$ (см. [1, лемма 2; 2, лемма 1.2 и следствие из нее]) отсюда следует, что $G = S_n$.

Если $n = r+1$, то аналогично $G \neq A_r$, A_{r+1}, A_{r+2}, S_r, S_{r+2} и, значит, распознаваемость симметрической группы S_{r+1} для $r \geq 17$ эквивалентна следующему утверждению.

Для любого собственного накрытия $G = N.A$ произвольной группы N с помощью группы A, изоморфной S_r или A_r, выполнено $\omega(G) \neq \omega(S_{r+1})$. Теорема доказана.

ЛИТЕРАТУРА

1. *Кондратьев А. С., Мазуров В. Д.* Распознавание знакопеременных групп простой степени по порядкам их элементов // Сиб. мат. журн. 2000. Т. 31, № 2. С. 359–369.
2. *Заварницин А. В.* Распознавание по множеству порядков элементов знакопеременных групп степени $r+1$ и $r+2$ для простого r и группы степени 16 // Алгебра и логика. 2000. Т. 39, № 6. С. 635–648.
3. *Brandl R., Shi W.* Finite groups whose element orders are consecutive integers // J. Algebra. 1991. V. 143, N 2. P. 388–400.
4. *Praeger C. E., Shi W.* A characterization of some alternating and symmetric groups // Comm. Algebra. 1994. V. 22, N 5. P. 1507–1530.
5. *Мазуров В. Д.* Характеризация конечных групп множествами порядков их элементов // Алгебра и логика. 1997. Т. 36, № 1. С. 37–53.
6. *Darafsheh M. R., Modhaddamfar A. R.* A characterization of some finite groups by their element orders // Algebra Colloq. 2000. V. 7, N 4. P. 467–476.
7. *Hanson D.* On a theorem of Sylvester and Schur // Canad. Math. Bull. 1973. V. 16, N 1. P. 195–199.
8. *Заварницин А. В., Мазуров В. Д.* О порядках элементов в накрытиях симметрических и знакопеременных групп // Алгебра и логика. 1999. Т. 38, № 3. С. 296–315.
9. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.

Статья поступила 10 июля 2001 г.

Заварницин Андрей Витальевич
Институт математики им. С. Л. Соболева СО РАН, Новосибирск 630090
zav@math.nsc.ru