Сибирский математический журнал
Май—июнь, 2004. Том 45, № 3

УДК 512.542

О РАСПОЗНАВАЕМОСТИ КОНЕЧНЫХ ПРОСТЫХ ОРТОГОНАЛЬНЫХ ГРУПП РАЗМЕРНОСТИ 2^m, 2^m+1 И 2^m+2 НАД ПОЛЕМ ХАРАКТЕРИСТИКИ 2

А. В. Васильев, М. А. Гречкосеева

Аннотация: *Спектром* $\omega(G)$ *конечной группы* G называется множество порядков ее элементов. Конечная группа G называется *распознаваемой по ее спектру* (кратко, *распознаваемой*), если для каждой конечной группы H такой, что $\omega(H)=\omega(G)$, имеет место изоморфизм $H\simeq G$. Основная цель статьи — указать две бесконечные по размерности серии конечных простых классических групп, распознаваемых по своим спектрам.

Ключевые слова: распознавание по спектру, конечная ортогональная группа.

Введение

Спектром $\omega(G)$ конечной группы G называется множество порядков ее элементов. Иными словами, натуральное число n принадлежит $\omega(G)$ тогда и только тогда, когда в G есть элемент порядка n. Конечная группа G называется *распознаваемой по ее спектру* (кратко, *распознаваемой*), если для каждой конечной группы H такой, что $\omega(H)=\omega(G)$, имеет место изоморфизм $H\simeq G$. Поскольку любая конечная группа, обладающая нетривиальной разрешимой нормальной подгруппой, нераспознаваема (см. [1, лемма 1]), то каждая распознаваемая группа является расширением прямого произведения M неабелевых простых групп с помощью некоторой подгруппы из $\mathrm{Out}(M)$. Особый интерес представляет вопрос о распознаваемости простых и почти простых групп (группа G называется почти простой, если $S\le G\le \mathrm{Aut}(S)$ для некоторой неабелевой простой группы S). Первые примеры распознаваемых конечных простых групп были указаны Ши в середине 80-х гг. прошлого века (см. [2, 3]). В 1994 г. Ши и Брандл доказали распознаваемость бесконечной серии простых линейных групп $L_2(q)$, $q\neq 9$ (см. [4, 5]). К настоящему времени решен вопрос о распознаваемости (или нераспознаваемости) для всех групп, простые делители которых не превосходят 13 (см. [6]), доказана распознаваемость нескольких бесконечных серий конечных простых и почти простых групп. Список групп, для которых к настоящему времени решен вопрос о распознаваемости, можно найти в [6].

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (коды проектов 02–01–00495, 02–01–39005), Совета по грантам президента РФ и программы «Ведущие научные школы» (грант НШ–2069.2003.1), СО РАН (грант для коллективов молодых ученых, постановление Президиума СО РАН № 404 от 06.12.2002), а также программы «Университеты России» (проект УР.04.01.031).

Однако все имеющиеся примеры распознаваемых групп, исключая знакопеременные и симметрические группы подстановок, в некотором смысле ограничены по размерности. Уточним. В силу классификационной теоремы все конечные простые неабелевы группы, кроме знакопеременных групп подстановок и 26 спорадических групп, являются группами лиева типа. Лиев ранг любой конечной группы, для которой решен вопрос о ее распознаваемости, не превосходит 6 для скрученных групп и 5 для нескрученных. В частности, размерность известных распознаваемых классических групп, т. е. групп, имеющих естественное матричное представление, не превосходит 10. Основная цель настоящей работы — указать две бесконечные по размерности серии конечных простых групп, распознаваемых по своим спектрам, а именно серии ортогональных групп $O_{2^m+1}(2)$ и $O^-_{2^m+2}(2)$. Так как доказательство результата в основном опирается на лиев подход к описанию соответствующих групп, в дальнейшем мы будем придерживаться лиевой нотации.

Теорема 1. *Для каждого натурального числа $m > 2$ группы $C_{2^m}(2)$ и ${}^2D_{2^m+1}(2)$ распознаваемы по своему спектру.*

Замечание 1. Имеют место изоморфизмы

$$C_{2^m}(2^k) \simeq S_{2^{m+1}}(2^k) \simeq O_{2\cdot 2^m+1}(2^k), \quad {}^2D_{2^m+1}(q) \simeq O^-_{2(2^m+1)}(q).$$

Замечание 2. Распознаваемость группы ${}^2D_5(2)$ доказана в [7]. Нераспознаваемость групп $C_2(2) \simeq S_4(2)$ и ${}^2D_3(2) \simeq U_4(2)$ установлена соответственно в [8, 9]. Группа же $C_4(2)$ не является распознаваемой, так как ее спектр совпадает со спектром естественного расширения группы ${}^2D_4(2)$ с помощью внешнего автоморфизма порядка 2. Последний факт несложно проверить, используя [10]. Таким образом, по модулю теоремы 1 вопрос о распознаваемости групп $C_{2^m}(2)$ и ${}^2D_{2^m+1}(2)$ полностью закрыт для любого натурального числа m.

Доказательство распознаваемости группы, как правило, включает в себя два основных этапа. На первом этапе доказывается, что группа H, спектр которой равен спектру исследуемой группы G, содержит композиционный фактор, изоморфный группе G. На втором — устанавливается, что H совпадает с этим фактором, т. е. изоморфна самой G. Поскольку результат первого этапа сам по себе представляет значительную ценность, а к тому же, зачастую, соответствующее утверждение удается получить для более широкого класса групп, имеет смысл выделить его в отдельную теорему. Для ее формулировки мы воспользуемся удобным термином, предложенным недавно в [11]. Конечная простая неабелева группа G называется *квазираспознаваемой*, если каждая конечная группа H такая, что $\omega(H) = \omega(G)$, имеет композиционный фактор, изоморфный G.

Теорема 2. *Пусть m и k — произвольные натуральные числа. Группа G квазираспознаваема в каждом из следующих случаев:*

а) *$G = {}^2D_{2^m}(2^k)$;*

б) *$G = {}^2D_{2^m+1}(2)$ и $m \neq 1$;*

в) *$G = C_{2^m}(2^k)$ и $m > 2$.*

Замечание 1. Тот факт, что группа ${}^2D_3(2) \simeq U_4(2)$ не является квазираспознаваемой, следует из доказательства предложения 6 в [9]. То, что группы $C_2(2^k)$ не квазираспознаваемы, вытекает из предложения 1 в [6]. Группа $C_4(2)$ не является квазираспознаваемой в силу аргумента, приведенного в замечании 2 к теореме 1. Вопрос о квазираспознаваемости групп $C_4(2^k)$ при $k > 1$ остается открытым. Наконец, поскольку распознаваемость групп $G = {}^2D_2(2^k) \simeq A_1(2^{2k})$ была установлена еще Брандлом и Ши, при доказательстве теоремы мы можем считать, что $m > 1$.

Замечание 2. Отметим, что, как и в случае с распознаваемостью, все известные до сих пор квазираспознаваемые группы лиева типа имели ограниченный лиев ранг.

§ 1. Предварительные результаты

Множество $\omega(H)$ конечной группы H замкнуто относительно делимости и однозначно определено множеством $\mu(H)$ тех элементов из $\omega(H)$, которые являются максимальными относительно делимости. Кроме того, множество $\omega(H)$ определяет граф Грюнберга — Кегеля $GK(H)$, вершинами которого служат все простые делители порядка группы H, и два простых числа p и q смежны, если H содержит элемент порядка $p \cdot q$. Обозначим через $s(H)$ число компонент связности графа $GK(H)$, а через $\pi_i(H)$, $i = 1, \dots, s(H)$, — его i-ю компоненту связности. Если группа H имеет четный порядок, то положим $2 \in \pi_1(H)$. Обозначим через $\mu_i(H)$ (соответственно через $\omega_i(H)$) множество чисел $n \in \mu(H)$ ($n \in \omega(H)$) таких, что каждый простой делитель числа n принадлежит π_i.

Лемма 1.1 (Грюнберг — Кегель). *Если H — конечная группа с несвязным графом $GK(H)$, то выполняется одно из следующих условий:*

(а) *$s(H) = 2$, H — группа Фробениуса;*

(б) *$s(H) = 2$, $H = ABC$, где A, AB — нормальные подгруппы в H; AB, BC — группы Фробениуса с ядрами A, B и дополнениями B, C соответственно;*

(в) *существует такая неабелева простая группа S, что $S \leq \overline{H} = H/K \leq \mathrm{Aut}(S)$ для некоторой нильпотентной нормальной $\pi_1(H)$-подгруппы K из H и группа $\overline{H}/S$ является $\pi_1(H)$-подгруппой; более того, граф $GK(S)$ несвязен, $s(S) \geq s(H)$ и для любого числа i, $2 \leq i \leq s(H)$, существует j, $2 \leq j \leq s(S)$, такое, что $\omega_i(H) = \omega_j(S)$.*

Доказательство см. в [12].

Лемма 1.2. *Пусть S — конечная простая группа с несвязным графом $GK(S)$. Тогда $|\mu_i(S)| = 1$ для $2 \leq i \leq s(S)$. Обозначим через $n_i = n_i(S)$ единственный элемент в $\mu_i(S)$, $i \geq 2$. Тогда S, $\pi_1(S)$ и $n_i(S)$, $2 \leq i \leq s(S)$, будут такими, как в табл.* 1a–1c.

Доказательство см. в [13, лемма 2].

Лемма 1.3. *Пусть H — конечная группа, K — нормальная нильпотентная подгруппа группы H, $H/K \simeq S$ и $R \leq S$. Пусть для некоторого простого числа p силовская p-подгруппа V группы K является элементарной абелевой p-группой и M — естественное полупрямое произведение $V \leftthreetimes R$. Тогда $\omega(M) \subseteq \omega(H)$.*

Доказательство. В силу того, что $V \subseteq Z(K)$, действие группы R на группе V определено корректно. Если $v \in V$, $r \in R \leq S$ и $\bar{r}$ — соответствующий r смежный класс группы H по подгруппе K, то $v^r = v^h$ для любого $h \in \bar{r}$.

Предположим, что $g \in M$ и $|g| \notin \omega(H)$. Имеем $g = r \cdot v$, где $r \in R$, $v \in V$. Если $|r| = m$, то $g^m = r^m v^{r^{m-1}} \dots v^r v \in V$. Следовательно, порядок g равен mp, и $mp \notin \omega(H)$. Рассмотрим теперь смежный класс $\bar{r}$. Любой элемент $h \in \bar{r}$ имеет порядок mt для некоторого t. Если $(t, p) = p$, то $mp \in \omega(H)$, значит, $(t, p) = 1$. Обозначим через N наименьшее общее кратное чисел из множества $\{|h|, h \in \bar{r}\}$.

Тогда N делится на m и не делится на mp. Для любых $h \in \bar{r}$, $k \in K$ будет $hk \in \bar{r}$, следовательно,

$$1 = (hk)^N = h^N k^{h^{N-1}} \dots k^h k = k^{h^{N-1}} \dots k^h k.$$

Так как $V \subseteq K$, для каждого $v \in V$ выполнено равенство $v^{h^{N-1}} \dots v^h v = 1$, если $h \in \overline{r}$. С другой стороны, $v^h = v^r$. Поэтому

$$g^N = (r \cdot v)^N = r^N v^{r^{N-1}} \dots v^r v = v^{h^{N-1}} \dots v^h v = 1.$$

Но число N не делит порядок элемента g; противоречие. Лемма доказана.

Лемма 1.4. *Пусть H — конечная группа, $K \lhd H$, H/K — группа Фробениуса с ядром F и циклическим дополнением C. Если $(|F|, |K|) = 1$ и F не содержится в $KC_H(K)/K$, то $p|C| \in \omega(H)$ для некоторого простого делителя p числа $|K|$.*

Доказательство см. в [14, лемма 1].

Лемма 1.5 (Жигмонди). *Пусть q — простое число, s — натуральное число, $s \geq 2$. Тогда верно одно из следующих утверждений:*

(а) *существует простое число p такое, что p делит $q^s - 1$ и p не делит $q^t - 1$ при любом натуральном $t < s$;*

(б) *$s = 6$ и $q = 2$;*

(в) *$s = 2$ и $q = 2^t - 1$ для некоторого натурального числа t.*

Доказательство см. в [15].

Простое число p, удовлетворяющее п. (а) леммы 1.5, называется *примитивным* простым делителем числа $q^s - 1$.

Лемма 1.6. *Пусть $r = q^l$ — степень простого числа q, s — натуральное число, $s \geq 2$. Тогда верны следующие утверждения:*

(а) *если s — нечетное число, то примитивный простой делитель числа $r^s - 1$ не делит $r^t + 1$ при любом натуральном $t < s$;*

(б) *если $(r, s) \neq (2, 3)$, то существует простое число p такое, что p делит $r^s + 1$ и p не делит $r^t - 1$ и $r^t + 1$ при любом натуральном $t < s$ (по аналогии с предыдущим определением будем называть это простое число p примитивным простым делителем числа $r^s + 1$);*

(в) *если p — примитивный простой делитель числа $r^s - \varepsilon$, $\varepsilon = \pm 1$, то p не делит l.*

Доказательство. (а) Пусть p — примитивный простой делитель числа $r^s - 1$. Предположим, что p делит $r^t + 1$ для некоторого $t < s$. Тогда p делит наибольший общий делитель чисел $r^s - 1$ и $r^{2t} - 1$, равный $r^{(s,2t)} - 1$. Так как s нечетно, то $(s, 2t) = (s, t) < s$; противоречие с выбором p.

(б) Пусть p — примитивный простой делитель числа $r^{2s} - 1$. Тогда p не делит $r^s - 1$, следовательно, p делит $r^s + 1$. Кроме того, p не делит $r^{2t} - 1$ для любого $t < s$.

(в) Предположим, что p делит l, и пусть $l = tp$. По условию p делит $r^s - \varepsilon = q^{ls} - \varepsilon = q^{tps} - \varepsilon$. С другой стороны, по теореме Ферма p делит $q^{tps} - q^{ts}$. Следовательно, p делит $q^{ts} - \varepsilon$, что противоречит примитивности p.

Таблица 1а. Конечные простые группы S с $s(S)=2$

S	Ограничения на S	$\pi_1(S)$	n_2
A_n	$6<n=p,p+1,p+2$; одно из чисел n, $n-2$ не просто	$\pi((n-3)!)$	p
$A_{p-1}(q)$	$(p,q)\neq(3,2),(3,4)$	$\pi(q\prod_{i=1}^{p-1}(q^i-1))$	$\frac{q^p-1}{(q-1)(p,q-1)}$
$A_p(q)$	$(q-1)\|(p+1)$	$\pi(q(q^{p+1}-1)\prod_{i=1}^{p-1}(q^i-1))$	$\frac{q^p-1}{q-1}$
${}^2A_{p-1}(q)$		$\pi(q\prod_{i=1}^{p-1}(q^i-(-1)^i))$	$\frac{q^p+1}{(q+1)(p,q+1)}$
${}^2A_p(q)$	$(q+1)\|(p+1)$, $(p,q)\neq(3,3),(5,2)$	$\pi(q(q^{p+1}-1)\times$ $\times\prod_{i=1}^{p-1}(q^i-(-1)^i))$	$\frac{q^p+1}{q+1}$
${}^2A_3(2)$		$\{2,3\}$	5
$B_n(q)$	$n=2^m\geq4$, q нечетно	$\pi(q\prod_{i=1}^{n-1}(q^{2i}-1))$	$(q^n+1)/2$
$B_p(3)$		$\pi(3(3^p+1)\prod_{i=1}^{p-1}(3^{2i}-1))$	$(3^p-1)/2$
$C_n(q)$	$n=2^m\geq2$	$\pi(q\prod_{i=1}^{n-1}(q^{2i}-1))$	$\frac{q^n+1}{(2,q-1)}$
$C_p(q)$	$q=2,3$	$\pi(q(q^p+1)\prod_{i=1}^{p-1}(q^{2i}-1))$	$\frac{q^p-1}{(2,q-1)}$
$D_p(q)$	$p\geq5$, $q=2,3,5$	$\pi(q\prod_{i=1}^{p-1}(q^{2i}-1))$	$\frac{q^p-1}{(q-1)}$
$D_{p+1}(q)$	$q=2,3$	$\pi(q(q^p+1)\prod_{i=1}^{p-1}(q^{2i}-1))$	$\frac{q^p-1}{(2,q-1)}$
${}^2D_n(q)$	$n=2^m\geq4$	$\pi(q\prod_{i=1}^{n-1}(q^{2i}-1))$	$\frac{q^n+1}{(2,q+1)}$
${}^2D_n(2)$	$n=2^m+1\geq5$	$\pi(2(2^n+1)\prod_{i=1}^{n-2}(2^{2i}-1))$	$2^{n-1}+1$
${}^2D_p(3)$	$5\leq p\neq2^m+1$	$\pi(3\prod_{i=1}^{p-1}(3^{2i}-1))$	$(3^p+1)/4$
${}^2D_n(3)$	$9\leq n=2^m+1\neq p$	$\pi(3(3^n+1)\prod_{i=1}^{n-2}(3^{2i}-1))$	$(3^{n-1}+1)/2$
$G_2(q)$	$2<q\equiv\varepsilon(3)$, $\varepsilon=\pm1$	$\pi(q(q^2-1)(q^3-\varepsilon))$	$q^2-\varepsilon q+1$
${}^3D_4(q)$		$\pi(q(q^6-1))$	q^4-q^2+1
$F_4(q)$	q нечетно	$\pi(q(q^6-1)(q^8-1))$	q^4-q^2+1
${}^2F_4(2)'$		$\{2,3,5\}$	13
$E_6(q)$		$\pi(q(q^5-1)(q^8-1)(q^{12}-1))$	$\frac{q^6+q^3+1}{(3,q-1)}$
${}^2E_6(q)$	$q>2$	$\pi(q(q^5+1)(q^8-1)(q^{12}-1))$	$\frac{q^6-q^3+1}{(3,q+1)}$
M_{12}		$\{2,3,5\}$	11
J_2		$\{2,3,5\}$	7
Ru		$\{2,3,5,7,13\}$	29
He		$\{2,3,5,7\}$	17
McL		$\{2,3,5,7\}$	11
Co_1		$\{2,3,5,7,11,13\}$	23
Co_3		$\{2,3,5,7,11\}$	23
Fi_{22}		$\{2,3,5,7,11\}$	13
HN		$\{2,3,5,7,11\}$	19

Таблица 1b. Конечные простые группы S с $s(S) = 3$

S	Ограничения на S	$\pi_1(S)$	n_2	n_3
A_n	$n > 6$, $n = p$	$\pi((n-3)!)$	p	$p-2$
	$p-2$ — простое число			
$A_1(q)$	$3 < q \equiv \varepsilon(4)$, $\varepsilon = \pm 1$	$\pi(q-\varepsilon)$	$\pi(q)$	$(q+\varepsilon)/2$
$A_1(q)$	$q > 2$, q четно	$\{2\}$	$q-1$	$q+1$
${}^2A_5(2)$		$\{2,3,5\}$	7	11
${}^2D_p(3)$	$p = 2^m + 1$	$\pi(3(3^{p-1}-1)\times$	$\frac{3^{p-1}+1}{2}$	$(3^p+1)/4$
		$\times \prod_{i=1}^{p-2}(3^{2i}-1))$		
$G_2(q)$	$q \equiv 0(3)$	$\pi(q(q^2-1))$	q^2-q+1	q^2+q+1
${}^2G_2(q)$	$q = 3^{2m+1} > 3$	$\pi(q(q^2-1))$	$q-\sqrt{3q}+1$	$q+\sqrt{3q}+1$
$F_4(q)$	q четно	$\pi(q(q^4-1)(q^6-1))$	q^4+1	q^4-q^2+1
${}^2F_4(q)$	$q = 2^{2m+1} > 2$	$\pi(q(q^3+1)(q^4-1))$	$q^2-\sqrt{2q^3}+$	$q^2+\sqrt{2q^3}+$
			$+q-\sqrt{2q}+1$	$+q+\sqrt{2q}+1$
$E_7(2)$		$\{2,3,5,7,11,13,17,$	73	127
		$19,31,43\}$		
$E_7(3)$		$\{2,3,5,7,11,13,19,$	757	1093
		$37,41,61,73,547\}$		
M_{11}		$\{2,3\}$	5	11
M_{23}		$\{2,3,5,7\}$	11	23
M_{24}		$\{2,3,5,7\}$	11	23
J_3		$\{2,3,5\}$	17	19
HiS		$\{2,3,5\}$	7	11
Suz		$\{2,3,5,7\}$	11	13
Co_2		$\{2,3,5,7\}$	11	23
Fi_{23}		$\{2,3,5,7,11,13\}$	17	23
F_3		$\{2,3,5,7,13\}$	19	31
F_2		$\{2,3,5,7,11,13,$	31	47
		$17,19,23\}$		

Лемма 1.7. *Пусть l и s — натуральные числа. Тогда выполнены следующие утверждения:*

(a) *число $2^{3^{l-1}} + 1$ делится на 3^l и не делится на 3^{l+1};*

(б) *если $2^s + 1$ или $2^s - 1$ делится на 3^l, то $s \geq 3^{l-1}$.*

Доказательство. (a) Проведем доказательство по индукции. При $l = 1$ утверждение верно. Предположим, что оно верно для всех натуральных чисел, меньших $l + 1$, и рассмотрим число $2^{3^l} + 1 = (2^{3^{l-1}} + 1)(2^{2\cdot 3^{l-1}} - 2^{3^{l-1}} + 1)$.

Таблица 1с. Конечные простые группы S с $s(S) > 3$

$s(S)$	S	Ограничения на S	$\pi_1(S)$	n_2	n_3	n_4	n_5	n_6
4	$A_2(4)$		$\{2\}$	3	5	7		
	$^2B_2(q)$	$q = 2^{2m+1}$ $q > 2$	$\{2\}$	$q-1$	$q-\sqrt{2q}++1$	$q+\sqrt{2q}++1$		
	$^2E_6(2)$		$\{2,3,5,7,11\}$	13	17	19		
	$E_8(q)$	$q \equiv 2,3(5)$	$\pi(q(q^8-1)(q^{12}-1)(q^{14}-1)(q^{18}-1)(q^{20}-1))$	$\frac{q^{10}-q^5+1}{q^2-q+1}$	$\frac{q^{10}+q^5+1}{q^2+q+1}$	q^8-q^4+1		
	M_{22}		$\{2,3\}$	5	7	11		
	J_1		$\{2,3,5\}$	7	11	19		
	$O'N$		$\{2,3,5,7\}$	11	19	31		
	LyS		$\{2,3,5,7,11\}$	31	37	67		
	Fi'_{24}		$\{2,3,5,7,11,13\}$	17	23	29		
	F_1		$\{2,3,5,7,11,13,17,19,23,29,31,47\}$	41	59	71		
5	$E_8(q)$	$q \not\equiv 2,3(5)$	$\pi(q(q^8-1)(q^{10}-1)(q^{12}-1)(q^{14}-1)(q^{18}-1))$	$\frac{q^{10}-q^5+1}{q^2-q+1}$	$\frac{q^{10}+q^5+1}{q^2+q+1}$	q^8-q^4+1	$\frac{q^{10}+1}{q^2+1}$	
6	J_4		$\{2,3,5,7,11\}$	23	29	31	37	43

Выражение в первых скобках делится на 3^l и не делится на 3^{l+1}, выражение во вторых скобках делится на 3 и не делится на 9. Следовательно, все выражение делится на 3^{l+1} и не делится на 3^{l+2}.

(б) Пусть $s < 3^{l-1}$. Из условия следует, что $2^{2s} - 1$ делится на 3^l. Таким образом, наибольший общий делитель чисел $2^{2\cdot 3^{l-1}} - 1$ и $2^{2s} - 1$, равный $2^{2(s,3^{l-1})} - 1 = 2^{2\cdot 3^t} - 1$, где $t < l-1$, также делится на 3^l. Следовательно, число $2^{3^t} + 1$ делится на 3^l, что противоречит п. (а) настоящей леммы.

§ 2. Свойства групп $C_n(q)$ и $^2D_n(q)$

Лемма 2.1. *Пусть T — максимальный тор в группе $C_n(q)$ или $^2D_n(q)$. Тогда порядок T равен*

$$|T| = \prod_{j=1}^{t}(q^{t_j} - 1)\prod_{i=1}^{s}(q^{s_i} + 1),$$

где натуральные числа s_i, t_j удовлетворяют соотношению

$$\sum_{j=1}^{t} t_j + \sum_{i=1}^{s} s_i = n, \tag{1}$$

и в случае $^2D_n(q)$ число s нечетно.

И обратно, если натуральные числа t_j, s_i, $1 \leq j \leq t$, $1 \leq i \leq s$, удовлетворяют соотношению (1), то в группе $C_n(q)$, а если дополнительно s нечетно, то и в группе $^2D_n(q)$, есть тор соответствующего порядка.

Доказательство см. в [16, ч. E, гл. II, § 1, теорема 1.7, п. b) и ч. G, пп. 15 и 16].

Лемма 2.2. *Пусть $n \geq 4$, $q = 2^k \geq 2$ и p — простое нечетное число. Тогда справедливы следующие утверждения:*

(а) *если $n = 2^m$ и $G = C_n(q)$, $^2D_n(q)$, $^2D_{n+1}(q)$, то $4n \notin \omega(G)$;*

(б) *если n четно и $p(q^{n-1} - 1) \in \omega(C_n(q))$, то p делит $q + 1$ или $q - 1$;*

(в) *если $3^l < n < 3^{l+1}$, то $3^{l+2} \notin \omega(C_n(2))$.*

Доказательство. (а) В силу вложений $^2D_n(2^k) < C_n(2^k) < {}^2D_{n+1}(2^k) < D_{n+1}(2^{2k})$ достаточно доказать, что $4n \notin \omega(D_{n+1}(2^{2k}))$. Силовская 2-подгруппа U группы $D_{n+1}(2^{2k})$ порождается элементами порядка 2. Следовательно, если $U^{(l)}$ — l-й коммутант группы U и u — произвольный элемент группы U, то $u^{2^l} \in U^{(l)}$. По [17, теорема 5.3.3] ступень нильпотентности группы U равна $2n - 1 = 2^{m+1} - 1$, следовательно, $U^{(m+1)} = 1$, и в группе U нет элемента порядка $2^{m+2} = 4n$.

(б) Пусть T — максимальный тор группы $C_n(q)$, содержащий элемент порядка $p(q^{n-1} - 1)$. По лемме 2.1 порядок тора T равен $\prod\limits_{j=1}^{t}(q^{t_j} - 1)\prod\limits_{i=1}^{s}(q^{s_i} + 1)$, где сумма $\sum\limits_{j=1}^{t} t_j + \sum\limits_{i=1}^{s} s_i$ равна n. Пусть p' — примитивный простой делитель числа $q^{n-1} - 1$. Число $n - 1$ нечетно, поэтому если $s_i < n - 1$ и $t_i < n - 1$, то по п. (а) леммы 1.6 число p' не делит порядок T. Кроме того, если $s_i = n, n - 1$, то $(q^{n-1} - 1, q^{s_i} + 1) = 1$, если $t_j = n$, то $(q^{n-1} - 1, q^{t_j} - 1) = q - 1$. Таким образом, $t_1 = n - 1$, $t_2 = 1$ или $t_1 = n - 1$, $s_1 = 1$. Поэтому порядок T равен $(q^{n-1} - 1)(q - 1)$ или $(q^{n-1} - 1)(q + 1)$. Отсюда немедленно следует заключение п. (б).

(в) Предположим, что в группе $C_n(2)$ есть элемент порядка 3^{l+2} и T — максимальный тор, содержащий этот элемент . Из результатов частей E и G книги [16] следует, что $T \simeq T_1 \times T_2 \times \cdots \times T_s$, где $|T_i| = 2^{s_i} + \varepsilon_i$, $s_i \leq n$, $\varepsilon_i = \pm 1$, $1 \leq i \leq s$. Следовательно, найдется i, $1 \leq i \leq s$, такое, что $3^{l+2} \in \omega(T_i)$, и, значит, $2^{s_i} + \varepsilon_i$ делится на 3^{l+2}. По п. (б) леммы 1.7 $s_i \geq 3^{l+1} > n$; противоречие.

Лемма 2.3. *Группа $A_n(q)$, $n \geq 4$, $q \geq 2$, содержит подгруппу Фробениуса с ядром порядка q^n и циклическим дополнением порядка $q^n - 1$.*

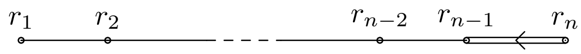
Доказательство см. в [18, лемма 3].

Группа $C_n(2)$ содержит подгруппу, изоморфную группе $A_{n-1}(2)$. Из леммы 2.3 вытекает

Следствие. *Группа $C_n(2)$, $n \geq 5$, содержит подгруппу Фробениуса с ядром порядка 2^{n-1} и циклическим дополнением порядка $2^{n-1} - 1$.*

Далее нам потребуются некоторые определения и обозначения, касающиеся групп лиева типа, в первую очередь группы $C_n(2)$. Подробности можно найти в [17].

Пусть Φ — система корней, Φ^+ — положительная, а $\Pi = \{r_1, r_2, \dots, r_n\}$ — фундаментальная системы корней алгебры C_n, причем диаграмма Дынкина выглядит так:



Обозначим через Π_i подсистему простых корней $\Pi \setminus \{r_i\}$, через Φ_i — множество корней, которые являются линейными комбинациями с целыми коэффициентами корней из Π_i, и через Φ_i^+ — множество корней $\Phi_i \cap \Phi^+$.

Пусть W — группа Вейля системы Φ и w_r — отражение относительно гиперплоскости, ортогональной корню r. Отражение w_{r_i}, соответствующее простому корню r_i, будем для простоты обозначать через w_i.

Группа $G = C_n(2)$ порождается своими корневыми подгруппами X_r, $r \in \Phi$. Каждая корневая подгруппа X_r имеет порядок два. Обозначим ее единственный нетривиальный элемент через x_r.

Пусть $n_r = x_r x_{-r} x_r$, где $r \in \Phi$. Подгруппа $N = \langle n_r \mid r \in \Phi \rangle$ — мономиальная подгруппа группы G — изоморфна группе Вейля, причем при подходящем изоморфизме элемент n_r переходит в элемент w_r. Будем отождествлять группы N и W.

Лемма 2.4. *Пусть $n = 2^m \geq 2$. Тогда группа $G = C_n(2)$ содержит подгруппу Фробениуса с ядром порядка $2^n + 1$ и циклическим дополнением порядка $2n$.*

Доказательство. В группе G есть максимальный тор T порядка $2^n + 1$. Множество $\pi(T)$ образует компоненту связности $\pi_2(G)$ графа $GK(G)$, следовательно, нормализатор $N_G(T)$ подгруппы T в группе G является группой Фробениуса с ядром T. Фактор-группа $N_G(T)/T$ изоморфна централизатору в группе Вейля элемента Кокстера $w_0 = w_1 w_2 \dots w_n$ (см. [16, ч. E и G]) и, значит, содержит элемент того же порядка, что и элемент w_0. Элемент w_0 имеет порядок $2n$ (см., например, [17, теорема 10.5.3]), и лемма доказана.

Группа ${}^2D_{n+1}(2)$ содержит подгруппу, изоморфную группе $C_n(2)$. Из леммы 2.4 вытекает

Следствие. *Пусть $n = 2^m \geq 4$. Тогда группа ${}^2D_{n+1}(2)$ содержит подгруппу Фробениуса с ядром порядка $2^n + 1$ и циклическим дополнением порядка $2n$.*

Лемма 2.5. *Пусть $n = 3^l + 1$. Тогда группа $G = C_n(2)$ содержит подгруппу Фробениуса с ядром порядка $2^{2 \cdot 3^l}$ и циклическим дополнением порядка 3^{l+1}.*

Доказательство. Рассмотрим в группе G параболическую подгруппу P_1, соответствующую подсистеме простых корней Π_1. По теореме о разложении

Леви [17, теорема 8.5.2] группа P_1 равна $U_1 : L_1$, где $U_1 = \langle X_r \mid r \in \Phi^+ \setminus \Phi_1\rangle$ и $L_1 = \langle X_r \mid r \in \Phi_1\rangle$.

Группа U_1 имеет порядок 2^{2n-1}. В [19] доказано, что U_1 является элементарной абелевой 2-группой. Элемент $x = w_2 w_3 \dots w_{n-1} x_{r_n} x_{-r_n} \in L_1$ действует на группе U_1 сопряжением. Это действие определяется действием элементов w_2, $w_3, \dots, w_{n-1}$, x_{r_n}, x_{-r_n} на порождающих группы U_1. Пусть $a = r_1 + r_2 + \dots + r_{n-1}$, $b = r_1 + r_2 + \dots + r_n$ и $c = 2(r_1 + r_2 + \dots + r_{n-1}) + r_n$. Тогда

$$x_r^{w_i} = x_{w_i(r)}, \quad r \in \Phi,$$

$$x_{r_n} x_r x_{r_n} = x_r, \quad r \in \Phi^+ \setminus (\Phi_1 \cup \{a\}),$$
$$x_{-r_n} x_r x_{-r_n} = x_r, \quad r \in \Phi^+ \setminus (\Phi_1 \cup \{b\}),$$
$$x_{r_n} x_a x_{r_n} = x_{-r_n} x_b x_{-r_n} = x_a x_b x_c.$$

Эти формулы позволяют составить следующую схему действия элемента x:

$$x_a \xrightarrow{x} x_{a-r_{n-1}} \xrightarrow{x} x_{a-r_{n-1}-r_{n-2}} \xrightarrow{x} \dots \xrightarrow{x} x_{r_1} \xrightarrow{x} x_b,$$

$$x_b \xrightarrow{x} x_{b+r_{n-1}} \xrightarrow{x} x_{b+r_{n-1}+r_{n-2}} \xrightarrow{x} \dots \xrightarrow{x} x_{c-r_1} \xrightarrow{x} x_a x_b x_c,$$

$$x_c \xrightarrow{x} x_c.$$

Пусть

$$v_1 = x_a x_c, \quad v_2 = x_{a-r_{n-1}} x_c, \dots, v_{n-1} = x_{r_1} x_c,$$
$$v_n = x_b x_c, \quad v_{n+1} = x_{b+r_{n-1}} x_c, \dots, v_{2n-2} = x_{c-r_1} x_c.$$

Элемент x нормализует группу $U_1' = \langle v_1, v_2, \dots, v_{2n-2}\rangle$. Отождествим группу U_1' с векторным пространством V над полем порядка два. Элементы $v_1, v_2, \dots, v_{2n-2}$ образуют базис в V. Отождествление дает естественный гомоморфизм группы $\langle x\rangle$ в группу $GL_{2n-2}(2)$ всех невырожденных матриц размерности $2n-2$ над полем порядка 2. При этом гомоморфизме элемент x переходит в матрицу

$$X = \begin{bmatrix} 0_{2n-3,1} & E_{2n-3} \\ E_1 & v \end{bmatrix},$$

где E_k — единичная матрица размерности k, $0_{k_1,\,k_2}$ — нулевая матрица размера $k_1 \times k_2$, v — строка длины $2n-3$, в которой на $(n-1)$-м месте стоит 1, на остальных — нули.

Нетрудно посчитать, что

$$X^k = \begin{bmatrix} 0_{2n-2-k,\,k} & E_{2n-2-k} \\ E_k & Y \end{bmatrix}, \quad \text{где} \quad Y = \begin{bmatrix} 0_{k,\,n-k-1} & E_k & 0_{k,\,n-k-1} \end{bmatrix}.$$

Поэтому

$$X^{n-1} = \begin{bmatrix} 0_{n-1,\,n-1} & E_{n-1} \\ E_{n-1} & E_{n-1} \end{bmatrix} \quad \text{и} \quad X^{3(n-1)} = E_{2n-2}.$$

Так как $n - 1 = 3^l$, то X действует на V регулярно, если X^{n-1} действует на V регулярно, а это верно, потому что $\det(X^{n-1} + E_{2n-2}) = 1$.

Порядок элемента x делится на $|X| = 3^{l+1}$ и по п. (в) леммы 2.2 не делится на 3^{l+2}, поэтому $|x| = 3^{l+1}t$, где $(t, 3) = 1$. Элемент x^t имеет порядок 3^{l+1} и, кроме того, действует регулярно на U_1', потому что его образ X^t действует регулярно на V. Следовательно, произведение $U_1' \cdot \langle x^t\rangle$ является искомой группой Фробениуса.

Лемма 2.6. *Пусть $n = 2^m \geq 4$. Тогда группа $G = {}^2D_{n+1}(2)$ содержит подгруппу Фробениуса с ядром порядка 2^{2n} и циклическим дополнением порядка $2^n + 1$.*

Доказательство. В [19] описана параболическая подгруппа P_1^1 группы G. А именно, $P_1^1 = U_1^1 : L_1^1$, где группа U_1^1 — элементарная абелева 2-группа порядка 2^{2n} и группа L_1^1 изоморфна группе ${}^2D_n(2)$. Группа L_1^1 действует сопряжениями на U_1^1 и содержит элемент y порядка $2^n + 1$. Этот элемент действует регулярно, так как простые делители $2^n + 1$ образуют компоненту связности $\pi_2(G)$. Следовательно, группа $U_1 \cdot \langle y \rangle$ является искомой группой Фробениуса.

§ 3. Доказательство теоремы 2

Пусть k и m — натуральные числа, $m \geq 2$, и $n = 2^m$, $r = 2^k$. В этом параграфе, если не оговорено особо, будем обозначать через G одну из групп ${}^2D_n(r)$, $C_n(r)$ или ${}^2D_{n+1}(2)$. В последнем случае будем считать, что $r = 2$, $k = 1$.

Пусть H — конечная группа такая, что $\omega(H) = \omega(G)$. Тогда из табл. 1a имеем $s(H) = s(G) = 2$ и $n_2(H) = n_2(G) = r^n + 1$.

Так как $s(H) > 1$, для группы H имеется три возможности, соответствующие пп. (а)–(в) леммы 1.1. Из результатов [20] следует, что для группы H выполнен пункт (в). Таким образом, $H = K \cdot S_1$, где $S \leq S_1 \leq \mathrm{Aut}(S)$ для некоторой простой неабелевой группы S, причем $\omega(S) \subseteq \omega(H)$, $s(S) \geq 2$ и существует i, $2 \leq i \leq s(S)$, такое, что $n_i(S) = n_2(H) = r^n + 1$.

Докажем, что $S \simeq G$. Рассмотрим каждую из групп в табл. $1a - 1c$. В этих таблицах p обозначает нечетное простое число, q — порядок соответствующего группе поля. Порядки и группы автоморфизмов рассматриваемых групп можно найти в [10]. Будем сначала предполагать, что число n достаточно велико. Оставшиеся при этом без доказательства случаи малых размерностей разберем отдельно в конце параграфа.

Легко проверить, что группа S не совпадает ни с одной из групп, перечисленных в таблицах отдельно. Покажем, что группа S также не является знакопеременной группой A_l, где $l > 6$.

Если $S = A_l$, где $l = p, p+1, p+2$ и одно из чисел l и $l-2$ не просто, то $s(S) = 2$ и $n_2(S) = p$. Так как $n_2(S) = n_2(H)$, то $p = r^n + 1$. Группы A_{r^n+1}, A_{r^n+2} и A_{r^n+3} содержат произведение двух независимых циклов длины $r^n/2$, т. е. элемент порядка $r^n/2 = 2^{kn-1}$. По п. (а) леммы 2.2 множество $\omega(G)$ не содержит числа $4n$, следовательно, $2n \geq r^n/2 \geq 2^{n-1}$. Это противоречит тому, что $2n < 2^{n-1}$ при $n > 4$.

Если $S = A_p$, причем $p - 2$ — простое число, то $s(S) = 3$ и $n_2(S) = p$, $n_3(S) = p - 2$. Если $n_2(H) = n_2(S)$, то $r^n + 1 = p$ и $p - 2$ не является простым числом. Если $n_2(H) = n_3(S)$, то $r^n + 1 = p - 2$ и $S = A_{r^n+3}$, а этот случай уже рассмотрен.

Теперь можно считать, что S является группой лиева типа над полем порядка q. Предположим, что S и i, $1 < i \leq s(S)$, таковы, что число $n_i(S)$ можно представить в виде $q^l f(q) + 1$, где $f(x)$ — некоторый многочлен с целыми коэффициентами и $(q, f(q)) = 1$. Если $f(q) \neq 1$, то $q^l f(q) \neq r^n$ и, следовательно, $n_i(S) \neq n_2(H)$. Таким образом, достаточно рассмотреть группы S, для которых это рассуждение не подходит.

Предположим, $S = A_{p-1}(q)$, где $(p, q) \neq (3, 2), (3, 4)$ и p делит $q - 1$, или $S = {}^2A_{p-1}(q)$, где p делит $q + 1$. Тогда $s(S) = 2$ и $n_2(S) = (q^p - \varepsilon)/p(q - \varepsilon)$, где $\varepsilon = 1$ в первом случае и $\varepsilon = -1$ во втором. Так как $n_2(H) = n_2(S)$, то $r^n + 1 = (q^p - \varepsilon)/p(q - \varepsilon)$ и $p(q - \varepsilon)(r^n + 1) = q^p - \varepsilon$. Пусть $q - \varepsilon = pt$. Тогда $p^2t(r^n + 1) = (pt + \varepsilon)^p - \varepsilon = p^3ts + p^2t$, где s — некоторое натуральное число. Сокращая на p^2t, получаем, что $r^n + 1 = ps + 1$ и $2^{kn} = r^n = ps$, что невозможно.

Пусть S равна $B_{n'}(q)$, ${}^2D_{n'}(q)$ или $C_{n'}(q)$, где q нечетно, $n' = 2^{m'}$, $n' \geq 4$ в первых двух случаях и $n' \geq 2$ в последнем случае. Тогда $s(S) = 2$ и $n_2(S) = (q^{n'} + 1)/2$. Так как $n_2(S) = n_2(H)$, то $q^{n'} = 2r^n + 1 \equiv 0\,(3)$, следовательно, $q = 3^l$ и $3^{ln'} = 2^{kn+1} + 1$. Последнее уравнение имеет два решения: $nk + 1 = 1$ и $nk + 1 = 3$, что неверно при $n > 2$.

Если $S = B_p(3), C_p(3)$ или $D_{p+1}(3)$, то $n_2(S) = (3^p - 1)/2$, и из равенства $n_2(H) = n_2(S)$ следует, что $3^p = 2r^n + 3$, а это неверно.

Если $S = C_p(2)$ или $D_{p+1}(2)$, то $n_2(S) = 2^p - 1$, но равенство $2^p - 1 = 2^{kn} + 1$ невозможно. По тем же соображениям невозможен случай $S = {}^2B_2(q)$, $q = 2^{2l+1} > 2$, $n_2(S) = n_2(H)$.

Если $S = {}^2D_{n'}(3)$, где $9 \leq n' = 2^{m'} + 1 \neq p$, то $s(S) = 2$ и $n_2(S) = (3^{n'-1} + 1)/2$. Так как $(3^{n'-1} + 1)/2 = r^n + 1$, то $3^{n'-1} = 2r^n + 1$. Последнее уравнение, как было отмечено, не имеет решений при $n > 2$. Аналогичным образом доказывается, что невозможен случай $S = {}^2D_p(3)$.

Пусть $S = E_6(q)$ или ${}^2E_6(q)$, $q > 2$, причем 3 делит $q - \varepsilon$, где $\varepsilon = 1$ в первом случае и $\varepsilon = -1$ во втором. Тогда $n_2(S) = (q^6 + \varepsilon q^3 + 1)/3$. Так как $n_2(S) = n_2(H)$, то $q^6 + \varepsilon q^3 - 2 = 3 \cdot r^n$. Заметим, что если $q - \varepsilon$ делится на 3, то $q^3 - \varepsilon$ делится на 9. Таким образом, $q^6 + \varepsilon q^3 - 2 = q^6 - 1 + \varepsilon(q^3 - \varepsilon)$ делится на 9, следовательно, r^n делится на 3; противоречие.

Предположим, что $S = A_1(q)$, где $q = p^l$, $3 < q \equiv \varepsilon(4)$, $\varepsilon = \pm 1$. Тогда $s(S) = 3$, $n_2(S) = p$ и $n_3(S) = (q + \varepsilon)/2$. Если $p = r^n + 1$, то подгруппа Картана группы S содержит циклическую подгруппу порядка $(p - 1)/2 = r^n/2 = 2^{kn-1}$. По п. (a) леммы 2.2 множество $\omega(G)$ не содержит числа $4n$, следовательно, $2^{kn-1} \leq 2n$, что неверно для $n > 4$. Пусть теперь $n_3(S) = n_2(H)$. Если $\varepsilon = 1$, то $q = 2r^n + 1 \equiv 0(3)$, значит, $p = 3$ и $3^l = 2^{kn+1} + 1$, что невозможно при $n > 2$. Если $\varepsilon = -1$, то $q = 2r^n + 3 \equiv 0(5)$, следовательно, $q \equiv 1(4)$; противоречие.

Предположим, что $S = F_4(q)$, где q четно, и $n_2(S) = n_2(H)$. Тогда $q^4 + 1 = r^n + 1$ и $q = r^{n/4}$. Пусть p' — примитивный простой делитель числа $q^6 + 1 = r^{3n/2} + 1$. Тогда p' делит порядок группы S и в силу примитивности не делит порядок группы G, так как

$$\pi(G) \subseteq \pi(2(r^{n+1} + 1)(r^n + 1)(r^n - 1)(r^{n-1} + 1)(r^{n-1} - 1) \ldots (r + 1)(r - 1)).$$

Следовательно, $\omega(S) \not\subseteq \omega(G)$, и этот случай невозможен.

Предположим, что $S = {}^2D_{n'+1}(2)$, $n' = 2^{m'} \geq 4$ и $G \neq S$. Тогда $n_2(S) = 2^{n'} + 1$ и $2^{n'} + 1 = r^n + 1$, так что $n' = kn$. Пусть p' — примитивный простой делитель числа $2^{n'+1} + 1 = 2^{nk+1} + 1$. Тогда p' делит $|S|$ и в силу примитивности не делит $|G|$, ибо

$$\pi(G) = \pi(2(2^{nk} + 1)(2^{nk} - 1)(2^{nk-k} + 1)(2^{nk-k} - 1) \ldots (2^k + 1)(2^k - 1)).$$

Итак, $\omega(S) \not\subseteq \omega(G)$, и этот случай также невозможен.

Предположим, что $S = C_{n'}(2^{k'})$, $n' = 2^{m'} \geq 2$, ${}^2D_{n'}(2^{k'})$, $n' = 2^{m'} \geq 4$, и $n_2(H) = n_2(S) = 2^{k'n'} + 1$ или $S = A_1(2^{k'})$ и $n_2(H) = n_3(S) = 2^{k'} + 1$. Будем считать, что в последнем случае $n' = 1$. Тогда $r^n + 1 = 2^{n'k'} + 1$, тем самым $r^{n/n'} = 2^{k'}$ и $k' = kn/n'$. Заметим, что $|\operatorname{Out}(S)| = dk' = dk2^{m-m'}$, где $d = 1$ или $d = 2$.

Если пара (r, n) не равна $(2, 4)$, то существуют и различны числа p^+ и p^- — примитивные простые делители чисел $r^{n-1}+1$ и $r^{n-1}-1$ соответственно. Докажем, что если $n \neq n'$, то p^+ и p^- не делят порядок группы S, а значит, в силу п. (в) леммы 1.6 и порядок группы S_1.

Если $S = A_1(r^n)$, то $|S| = r^n(r^n+1)(r^n-1)^2$, и утверждение справедливо, так как если $\varepsilon_1, \varepsilon_2 = \pm 1$, то $(r^n+\varepsilon_1, r^{n-1}+\varepsilon_2)$ делит $r-\varepsilon_1\varepsilon_2$.

Если $S = C_{n'}(r^{n/n'})$, то

$$|S| = r^{nn'}(r^n+1)(r^n-1)(r^{n-n/n'}+1)(r^{n-n/n'}-1)\dots(r^{n/n'}+1)(r^{n/n'}-1),$$

если $S = {}^2D_{n'}(r^{n/n'})$, то

$$|S| = r^{n(n'-1)}(r^n+1)(r^{n-n/n'}+1)(r^{n-n/n'}-1)\dots(r^{n/n'}+1)(r^{n/n'}-1).$$

Так как $n \neq n'$, числа p^+ и p^- не делят порядок группы S в силу своей примитивности и сделанного выше замечания.

Порядок группы G в отличие от порядка группы S_1 делится на числа $r^{n-1}+1$ и $r^{n-1}-1$, поэтому $p^+, p^- \in \omega(G)$. Предположим, что $p^+ \cdot p^- \in \omega(G)$. Тогда элемент порядка $p^+ \cdot p^-$ лежит в некотором максимальном торе T группы G. По лемме 2.1 порядок этого тора равен $\prod\limits_i (r^{s_i}+1)\prod\limits_j (r^{t_j}-1)$, где $\sum\limits_i s_i + \sum\limits_j t_j = n$. В силу примитивности чисел p^+ и p^- порядок $|T|$ делится на $(r^{n-1}+1)(r^{n-1}-1)$, но $n-1+n-1 > n$ при $n > 2$ и такого тора в группе G быть не может. Следовательно, $p^+ \cdot p^- \notin \omega(G)$.

Так как $p^+ \in \omega(H) \setminus \omega(S_1)$, то $p^+ \in \omega(K)$. То же самое верно и для p^-. Группа K нильпотентна, значит, $p^+ \cdot p^- \in \omega(K) \subseteq \omega(H) = \omega(G)$; противоречие.

Для завершения доказательства осталось рассмотреть случай $S = C_n(r)$ или $S = {}^2D_n(r)$.

Пусть $G = {}^2D_n(r)$ и $S = C_n(r)$. Пусть p_1^+ и p_1^- — примитивные простые делители чисел $r^{n/2+1}-1$ и $r^{n/2-1}-1$ соответственно. При $n > 4$ числа p_1^+ и p_1^- различны, так как в этом случае

$$(r^{n/2+1}-1, r^{n/2-1}-1) = (r^2-1, r^{n/2-1}-1) = 1.$$

По лемме 2.1 группа S содержит тор порядка $(r^{n/2+1}+1)(r^{n/2-1}+1)$, следовательно, $p_1^+ \cdot p_1^- \in \omega(S)$.

По этой же лемме порядки максимальных торов в группе G совпадают с числами $\prod\limits_{i=1}^{s}(r^{s_i}+1)\prod\limits_j (r^{t_j}-1)$, где s нечетно, $\sum\limits_{i=1}^{s} s_i + \sum\limits_j t_j = n$. Следовательно, $p_1^+,\ p_1^- \in \omega(G)$. Предположим, что $p_1^+ \cdot p_1^- \in \omega(G)$. Тогда в G есть тор T, порядок которого делится на $r^{n/2+1}-1$ и $r^{n/2-1}-1$. Так как число сомножителей в $|T|$ вида $2^{s'}+1$ должно быть нечетно, то $|T|$ имеет по крайней мере еще один множитель, равный $2^{s'}+1$. С другой стороны, $s'+(n/2+1)+(n/2-1) = s'+n > n$; противоречие. Следовательно, $p_1^+ p_1^- \notin \omega(G)$. Таким образом, $\omega(S) \nsubseteq \omega(G)$, и этот случай невозможен.

Пусть теперь, наоборот, $G = C_n(r)$ и $S = {}^2D_n(r)$. Рассмотрим числа p_1^+, p_1^-, p_2^+, p_2^-, p_3^+ и p_3^- — примитивные простые делители чисел $r^{n/2+1}-1$, $r^{n/2-1}-1$, $r^{n/2+1}+1$, $r^{n/2-1}+1$, $r^{n/2+3}+1$ и $r^{n/2-3}+1$ соответственно. Если $n > 8$, то числа p_1^+, p_1^-, p_2^+, p_2^-, p_3^+ и p_3^- попарно различны. Так же, как и в предыдущем случае, доказывается, что для каждого $i = 1, 2, 3$ число $p_i^+ \cdot p_i^-$ лежит в $\omega(G)$, но не лежит в $\omega(S)$. Более того, по п (в) леммы 1.6 число $p_i^+ \cdot p_i^-$ не лежит в $\omega(S_1)$.

Предположим, что $p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot p_3^{\varepsilon_3} \in \omega(G)$ для некоторых ε_1, ε_2, $\varepsilon_3 \in \{+,-\}$. Тогда в группе G есть тор T, порядок которого делится на

$$(r^{n/2+\varepsilon_1}-1)(r^{n/2+\varepsilon_2}+1)(r^{n/2+3\varepsilon_3}-1),$$

но

$$n/2+\varepsilon_1+n/2+\varepsilon_2+n/2+3\varepsilon_3 \geq 3n/2-5>n$$

при $n>10$; противоречие.

Для каждого $i=1,2,3$ имеем $p_i^+ \cdot p_i^- \in \omega(H) \backslash \omega(S_1)$, следовательно, найдется $\varepsilon_i \in \{+,-\}$ такое, что $p_i^{\varepsilon_i} \in \omega(K)$. Группа K нильпотентна, поэтому

$$p_1^{\varepsilon_1} \cdot p_2^{\varepsilon_2} \cdot p_3^{\varepsilon_3} \in \omega(K) \subseteq \omega(H)=\omega(G),$$

что неверно.

Осталось рассмотреть случай $G={}^2D_{n+1}(2)$ и $S=C_n(2)$ или ${}^2D_n(2)$. Заметим, что в этом случае $S_1=S$ или $S_1=S\cdot 2$. Как отмечено ранее, если p' — примитивный простой делитель $2^{n+1}-1$, то $p' \in \omega(G) \setminus \omega(S)$. Пусть p_1 и p_2 — примитивные простые делители $2^{n/2}+1$ и $2^{n/2+1}-1$ соответственно. Числа p', p_1 и p_2 попарно различны при $n>2$.

Число $p_1 \cdot p_2$ принадлежит $\omega(G) \setminus \omega(S)$, так как по лемме 2.1 в группе G есть тор порядка $(2^{n/2}+1)(2^{n/2+1}-1)$, а в группе S такого тора нет. По той же лемме в G нет торов порядков $(2^{n+1}-1)(2^{n/2}+1)$ и $(2^{n+1}-1)(2^{n/2+1}-1)$, следовательно, $p' \cdot p_1$, $p' \cdot p_2 \notin \omega(G)$.

Так как $p', p_1 \cdot p_2 \in \omega(H) \setminus \omega(S)$, то $p', p_i \in \omega(K)$ для некоторого $i \in \{1,2\}$, тем самым $p' \cdot p_i \in \omega(K) \subseteq \omega(H)=\omega(G)$, что неверно.

Таким образом, теорема доказана для всех групп ${}^2D_{n+1}(2)$ и групп ${}^2D_n(2^k)$ при $n>4$ и для групп $C_n(2^k)$ при $n>8$. Кроме того, в [7] доказано, что группы ${}^2D_4(2)$ и ${}^2D_5(2)$ распознаваемы по своему спектру. Поэтому для завершения доказательства нам осталось рассмотреть группы ${}^2D_4(r), r>2$, и $C_8(r)$.

Пусть $G={}^2D_4(r)$, $r=2^k>2$. Достаточно рассмотреть те группы S, для отбрасывания которых использовалось неравенство $n>4$.

Предположим, $S=A_{p+1}, A_{p+2}, A_{p+3}$, где $p=r^4+1$. Пусть p' — примитивный простой делитель числа r^6+1. Тогда p' делит число $(r^6+1)/(r^2+1)=r^4-r^2+1<p$, следовательно, в S есть элемент порядка p'. С другой стороны, в силу примитивности p' не делит порядок группы G. Таким образом, $p' \in \omega(S) \setminus \omega(G)$, и мы пришли к противоречию.

Предположим, что $S=A_1(p^l)$, где $p=r^4+1$. Порядок группы S равен $p^l(p^l+1)(p^l-1)^2$. Нетрудно показать, что это число делится на

$$p+1=r^4+2=2^{4k}+2=2(2^{4k-1}+1).$$

Так как $k>1$, примитивный простой делитель числа $2^{4k-1}+1$ не делит порядок группы G, поэтому $\omega(S) \nsubseteq \omega(G)$, и мы опять пришли к противоречию.

Предположим, что $S=C_4(r)$. Достаточно доказать, что $\omega(S) \nsubseteq \omega(G)$.

Мы докажем более общее утверждение о том, что для некоторого простого нечетного p число $2\cdot p$ принадлежит $\omega(C_n(r)) \setminus \omega({}^2D_n(r))$, где $r=2^k \geq 2$, $n \geq 4$. Свойства централизаторов инволюций в группах $C_n(r)$ и ${}^2D_n(r)$ описаны в [21]. Если C — централизатор инволюции в группе ${}^2D_n(r)$, то фактор-группа $C/O_2(C)$ изоморфна группе $C_l(r) \times {}^2D_{n-2l}(r)$ или группе $C_{l-1}(r) \times C_{n-2l}(r)$, где $l \leq n/2$. Таким образом, $\pi(C) \subseteq \pi(C_{n-2}(r))$. В группе $C_n(r)$ есть централизатор инволюции C такой, что $C/O_2(C) \simeq C_{n-1}(r)$. Если $(n,r) \neq (4,2)$ и p — примитивный простой делитель числа $r^{n-1}+1$, то p не делит порядок группы $C_{n-2}(r)$

и делит порядок группы $C_{n-1}(r)$. Если $(n,r)=(4,2)$, то таким же свойством обладает число $p=7$. Таким образом, в любом случае p связано с 2 в $\omega(C_n(r))$ и не связано в $\omega(^2D_n(r))$.

Случай $G={}^2D_4(r)$ разобран полностью.

Пусть $G=C_8(r)$. Единственная простая группа S, при отбрасывании которой использовалось условие $n>8$, — это группа $S={}^2D_8(r)$. Ранее было доказано, что если p_1^+ и p_1^- — примитивные простые делители чисел $r^{n/2+1}-1$ и $r^{n/2-1}-1$ соответственно, то $p_1^+p_1^-\in\omega(G)\setminus\omega(S)$. Следовательно, $p=p_1^\varepsilon\in\omega(K)$ для некоторого $\varepsilon\in\{+,-\}$.

Пусть P — силовская p-подгруппа группы K. Подгруппа $\Phi(P)$ нормальна в H. Рассмотрим вместо групп H, K и P фактор-группы $\overline{H}=H/\Phi(P)$, $\overline{K}=K/\Phi(P)$ и $V=P/\Phi(P)$. Нетрудно заметить, что так как $p\in\pi_1(H)$, то граф $GK(\overline{H})$ несвязен, как и граф $GK(H)$. По следствию из леммы 2.3 в группе G есть подгруппа Фробениуса R с ядром порядка r^7 и циклическим дополнением порядка r^7-1. Группы $\overline{H}$, $\overline{K}$, $R\le G\simeq\overline{H}/\overline{K}$, V и $M=V\rtimes R$ удовлетворяют условиям леммы 1.3. Следовательно, $\omega(M)\subseteq\omega(\overline{H})\subseteq\omega(H)=\omega(G)$.

Поскольку $\overline{K}\le C_{\overline{H}}(V)\trianglelefteq(\overline{H})$ и группа $\overline{H}/\overline{K}\simeq G$ проста, то $C_{\overline{H}}(V)=\overline{K}$ или $C_{\overline{H}}(V)=\overline{H}$. Так как граф $GK(\overline{H})$ несвязен, последний случай невозможен и $C_{\overline{H}}(V)=\overline{K}$. По лемме 1.4 в группе M, а значит, и в группе G, есть элемент порядка $p\cdot(r^7-1)$. По п. (б) леммы 2.2 число p делит $r+1$ или $r-1$, что противоречит примитивности числа p.

Случай $G=C_8(r)$ также разобран, и теорема доказана.

§ 4. Доказательство теоремы 1

Пусть $G=C_n(2)$, $n=2^m>4$ и H — конечная группа такая, что $\omega(H)=\omega(G)$. По результатам предыдущего параграфа в группе H есть нормальная нильпотентная подгруппа K такая, что $G\le H/K\le \mathrm{Aut}(G)$. Группа $\mathrm{Aut}(G)=G$, поэтому $H/K=G$. Докажем, что $K=1$.

Предположим, что $K\neq1$. Без ограничения общности можно считать, что K — элементарная абелева p-группа. Поскольку граф $GK(H)$ несвязен, то $C_H(K)\neq H$. Так как группа G проста, то $C_H(K)=K$. Следовательно, H индуцирует при сопряжении группу автоморфизмов группы K, изоморфную G. В своих дальнейших рассуждениях мы будем использовать лемму 1.4 и подгруппы Фробениуса группы G.

По лемме 2.4 группа G содержит подгруппу Фробениуса с ядром порядка 2^n+1 и циклическим дополнением порядка $2n$. Если $p=2$, то по лемме 1.4 группа H, а значит, и группа G, содержат элемент порядка $2\cdot2n$, что противоречит п. (а) леммы 2.2.

По лемме 2.5 группа G содержит подгруппу Фробениуса с ядром порядка $2^{2\cdot3^l}$ и циклическим дополнением порядка 3^{l+1}, где $3^l<n<3^{l+1}$. Если $p=3$, то по лемме 1.4 группа H содержит элемент порядка $3\cdot3^{l+1}$, что противоречит п. (в) леммы 2.2.

Пусть теперь $p\neq2,3$. По следствию из леммы 2.3 группа G содержит подгруппу Фробениуса с ядром порядка 2^{n-1} и циклическим дополнением порядка $2^{n-1}-1$. Так как $p\neq2$, то по лемме 1.4 группа H содержит элемент порядка $p\cdot(2^{n-1}-1)$. По п. (б) леммы 2.2 число p равно 3; противоречие.

Таким образом, $K=1$. Следовательно, $H=G$, и для группы $C_n(2)$ теорема доказана.

Пусть $G = {}^2D_{n+1}(2)$, $n = 2^m > 4$ и H — конечная группа такая, что $\omega(H) = \omega(G)$. По результатам предыдущего параграфа в группе H есть нормальная нильпотентная подгруппа K такая, что $G \leq H/K \leq \mathrm{Aut}(G)$. Известно, что $\mathrm{Aut}(G) = G \cdot 2$ и $\mathrm{Aut}(G) \setminus G$ содержит инволютивный полевой автоморфизм g. Централизатор элемента g в группе G содержит подгруппу, изоморфную группе $C_n(2)$, следовательно, содержит элемент порядка $2^n + 1$. Таким образом, число $2 \cdot (2^n + 1)$ лежит в $\omega(\mathrm{Aut}(G))$ и не лежит в $\omega(G)$. Поэтому $\omega(\mathrm{Aut}(G)) \neq \omega(G) = \omega(H)$ и $H/K = G$.

Как и в предыдущем случае, можно считать, что K — элементарная абелева p-группа и $C_H(K) = K$.

Если $p = 2$, то проводится то же самое рассуждение, что и для группы $C_n(2)$. По следствию из леммы 2.4 группа G содержит подгруппу Фробениуса с ядром порядка 2^n+1 и циклическим дополнением порядка $2n$. Следовательно, по лемме 1.4 группа H содержит элемент порядка $2 \cdot 2n$, что противоречит п. (a) леммы 2.2.

Пусть $p \neq 2$. По лемме 2.6 группа G содержит подгруппу Фробениуса с ядром четного порядка и циклическим дополнением порядка $2^n + 1$. По лемме 1.4 группа H содержит элемент порядка $p(2^n+1)$, но по лемме 1.2 число 2^n+1 принадлежит $\mu(G) = \mu(H)$. Полученное противоречие завершает доказательство теоремы.

ЛИТЕРАТУРА

1. *Мазуров В. Д.* О множестве порядков элементов конечной группы // Алгебра и логика. 1994. Т. 33, № 1. С. 81–89.

2. *Shi W.* A characteristic property of $PSL_2(7)$ // J. Austral. Math. Soc. Ser. A. 1984. V. 36, N 3. P. 354–356.

3. *Shi W.* A characteristic property of A_5 // J. Southwest-China Teach. Univ. 1986. V. 3. P. 11–14.

4. *Shi W.* A characteristic property of J_1 and $PSL_2(2^n)$ // Adv. Math. 1987. V. 16. P. 397–401.

5. *Brandl R., Shi W.* The characterization of $PSL(2, q)$ by its element orders // J. Algebra. 1994. V. 163, N 1. P. 109–114.

6. *Мазуров В. Д.* Распознавание конечных простых групп $S_4(q)$ по порядкам их элементов // Алгебра и логика. 2002. Т. 41, № 2. С. 166–198.

7. *Shi W., Tang C. J.* A characterization of some orthogonal groups // Prog. Nat. Sci. 1997. V. 7, N 2. P. 155–162.

8. *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.

9. *Мазуров В. Д.* Распознавание конечных групп по множеству порядков их элементов // Алгебра и логика. 1998. Т. 37, № 6. С. 651–666.

10. *Conway J. H., Curtis R. T., Norton S. P., Parker R. A., Wilson R. A.* Atlas of finite groups. Oxford: Clarendon Press, 1985.

11. *Алексеева О. А., Кондратьев А. С.* О распознаваемости группы $E_8(q)$ по множеству порядков элементов // Укр. мат. журн. 2002. Т. 54, № 7. С. 998–1003.

12. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.

13. *Кондратьев А. С., Мазуров В. Д.* Распознавание знакопеременных групп простой степени по порядкам их элементов // Сиб. мат. журн. 2000. Т. 41, № 2. С. 359–371.

14. *Мазуров В. Д.* Характеризация конечных групп множествами порядков их элементов // Алгебра и логика. 1997. Т. 36, № 1. С. 37–53.

15. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. V. 3. P. 265–284.

16. *Семинар* по алгебраическим группам. М.: Мир, 1973.

17. *Carter R. W.* Simple groups of Lie type. London: John Wiley & Sons, 1972.

18. *Заварницин А. В.* Порядки элементов в накрытиях групп $L_n(q)$ и распознаваемость знакопеременной группы A_{16}. Новосибирск, 2000. (Препринт/НИИДМИ; № 48).

19. *Гречкосеева М. А.* О минимальных подстановочных представлениях классических простых групп // Сиб. мат. журн. 2003. Т. 44, № 3. С. 560–586.

20. *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.

21. *Aschbacher M., Seitz G. M.* Involutions in Chevalley groups over fields of even order // Nagoya Math. J. 1976. V. 63. P. 1–91.

Статья поступила 29 декабря 2003 г.

Васильев Андрей Викторович
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
vdr@gorodok.net

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