Сибирский математический журнал
Март—апрель, 2008. Том 49, № 2

УДК 512.54

СВОЙСТВА ПОРЯДКОВ ЭЛЕМЕНТОВ В НАКРЫТИЯХ ГРУПП $\mathrm{L}_n(q)$ И $\mathrm{U}_n(q)$

А. В. Заварницин

Аннотация. Доказано, что если G — конечная простая группа, изоморфная $\mathrm{PSL}_n(q)$ или $\mathrm{PSU}_n(q)$, где либо $n \neq 4$, либо q простое или четное, которая действует на векторном пространстве над полем характеристики определения группы G, то соответствующее полупрямое произведение содержит элемент, порядок которого отличен от порядков всех элементов группы G. Как следствие доказано, что группа $\mathrm{PSL}_n(q)$, где либо $n \neq 4$, либо q простое или четное, распознаваема по спектру среди своих накрытий. Тем самым дан частичный положительный ответ на проблему 14.60 из Коуровской тетради.

Ключевые слова: модулярное представление, вес, порядок элемента, распознаваемость.

1. Введение

Если группа H является гомоморфным образом конечной группы G, то будем говорить, что G — *накрытие* группы H или что G *накрывает* H. Эта работа посвящена следующей проблеме из Коуровской тетради [1, проблема 14.60].

Проблема 1. *Пусть G — собственное накрытие конечной простой группы $L = \mathrm{L}_n(q)$, $n \geq 3$. Верно ли, что в G найдется элемент, порядок которого отличен от порядка любого элемента из L?*

Эта проблема связана с распознаванием конечных групп по спектру. Напомним, что *спектром* $\omega(H)$ конечной группы H называется множество порядков ее элементов. Говорят, что H *распознаваема* (*по спектру*) *среди своих накрытий*, если для любой конечной группы G, накрывающей H, равенство спектров $\omega(G) = \omega(H)$ влечет изоморфизм $G \cong H$. Таким образом, в проблеме 1 спрашивается, является ли каждая простая группа $\mathrm{L}_n(q)$, $n \geq 3$, распознаваемой среди накрытий?

Некоторые частные случаи этой проблемы уже рассматривались в других работах (см., например, [2–4]). Кроме того, простые группы $\mathrm{L}_2(q)$ распознаваемы среди накрытий в силу [5, 6].

Можно показать (см. лемму 11), что рассмотрение проблемы 1 сводится к случаю, когда накрытие G является естественным полупрямым произведением $W \leftthreetimes L$, где W — элементарная абелева p-группа (p — характеристика определения группы $L = \mathrm{L}_n(q)$) и действие L на W точное и абсолютно неприводимое. Мы доказываем, что такая группа G, как правило, содержит элемент нового порядка. А именно, если обозначить $\mathrm{L}_n^+(q) = \mathrm{PSL}_n(q)$ и $\mathrm{L}_n^-(q) = \mathrm{PSU}_n(q)$, то имеет место следующее утверждение.

Работа выполнена при финансовой поддержке фонда FAPESP (Бразилия) (грант 06/60776–3), Российского фонда фундаментальных исследований (код проекта 05–01–00797) и СО РАН (грант № 29 для молодых ученых и Интеграционный проект 2006.1.2).

Теорема 1. *Пусть $\varepsilon \in \{+,-\}$ и $L = \mathrm{L}_n^{\varepsilon}(q)$ — простая группа, где $q = p^m$. Предположим, что либо $n \geq 5$, либо $n = 4$ и q простое, либо $n = 4$ и q четное. Если L действует на векторном пространстве W над полем характеристики p, то $\omega(W \rtimes L) \neq \omega(L)$.*

Как следует из доказательства, в случае, когда либо $n \geq 5$, либо q нечетное простое, можно утверждать даже больше: группа L содержит *полупростой* элемент g, порядок которого p-максимален (т. е. такой, что $p\,|g| \notin \omega(L)$) и который централизует нетривиальный вектор из W. Более того, если $n \geq 5$ и $q > 3$, то такой элемент g может быть выбран независимо от модуля W. Доказательство использует свойства весов неприводимых модулей алгебраических групп типа A_l.

Из этого результата вытекает (частичное) положительное решение проблемы 1.

Следствие 1. *Пусть $L = \mathrm{L}_n(q)$ — простая линейная группа. Если либо $n \neq 4$, либо q простое или четное, то L распознаваема по спектру среди своих накрытий.*

Таким образом, единственный оставшийся открытый случай в проблеме 1, когда $L = \mathrm{L}_4(q)$, где q непростое и нечетное. Отметим, что действие группы $\mathrm{L}_4^{\varepsilon}(q)$ в характеристике определения требует более тонкого анализа. Вышеописанные методы не всегда применимы, поскольку существуют примеры полупрямых произведений $W \rtimes L$, не содержащих элементы порядка pt, где t — p-максимальный порядок, взаимно простой с p. Это означает, что здесь также следует учитывать действие унипотентных элементов группы $\mathrm{L}_4^{\varepsilon}(q)$. Пусть, например, характеристика $p = 2$ и модуль W — естественный модуль для группы $L = \mathrm{SU}_4(2)$. Тогда $\omega(W \rtimes L) \setminus \omega(L) = \{8\}$. Существуют также более сложные примеры подобного рода и в нечетной характеристике.

2. Предварительные результаты

Всюду далее мы обозначаем через $\mathbb{F}_q$ конечное поле из $q = p^m$ элементов. Центр группы G обозначается через $Z(G)$.

Пусть $t > 1$ и n — натуральные числа и $\varepsilon \in \{+,-\}$. Если существует простое число, делящее $t^n - (\varepsilon 1)^n$ и не делящее $t^i - (\varepsilon 1)^i$ для $1 \leq i < n$, то такое число будет обозначаться через $t_{[\varepsilon n]}$ и называться *примитивным делителем* числа $t^n - (\varepsilon 1)^n$. В общем случае примитивный делитель может не существовать или не быть единственным. Следующая лемма обобщает известную теорему Жигмонди.

Лемма 1. *Пусть $t, n > 1$ — натуральные числа и $\varepsilon \in \{+,-\}$. Тогда примитивный делитель $t_{[\varepsilon n]}$ числа $t^n - (\varepsilon 1)^n$ существует, за исключением следующих случаев:*

(i) *$\varepsilon = +$, $n = 6$ и $t = 2$;*
(ii) *$\varepsilon = +$, $n = 2$ и $t = 2^l - 1$ для некоторого $l \geq 2$;*
(iii) *$\varepsilon = -$, $n = 3$ и $t = 2$;*
(iv) *$\varepsilon = -$, $n = 2$ и $t = 2^l + 1$ для некоторого $l \geq 0$.*

Доказательство. См. [4, лемма 5]. □

Пусть q — степень простого числа и $\varepsilon \in \{+,-\}$. Для $n \in \mathbb{N}$ определим *обобщенный примитивный делитель*

$$q^*_{[\varepsilon n]} = \begin{cases} q_{[\varepsilon n]}, & \text{если } \ q_{[\varepsilon n]} \text{ существует}, \\ 9, & \text{если } \ (\varepsilon, n, q) = (+, 6, 2), \\ 2^l, & \text{если } \ (\varepsilon, n, q) = (+, 2, 2^l - 1) \text{ для } l \geq 2, \\ 2^l, & \text{если } \ (\varepsilon, n, q) = (-, 2, 2^l + 1) \text{ для } l \geq 2. \end{cases}$$

Заметим, что $q^*_{[\varepsilon n]}$ не определен тогда и только тогда, когда

$$(\varepsilon, n, q) \in \{(-, 2, 2), (-, 2, 3), (-, 3, 2)\}. \tag{1}$$

Следующее утверждение напрямую следует из данного выше определения.

Лемма 2. *Предположим, что обобщенный примитивный делитель $r = q^*_{[\varepsilon n]}$ определен. Выполнены следующие утверждения:*

(i) *$r \mid \big(q^s - (\varepsilon 1)^s\big)$ тогда и только тогда, когда $n \mid s$;*

(ii) *если $n > 1$, то $\gcd(r, q - \varepsilon 1) = 1$, за исключением случая, когда $(\varepsilon, n, q) = (+, 2, 2^l - 1)$ или $(-, 2, 2^l + 1)$;*

(iii) *если $s \mid n$ и $s > 1$, то*

$$r \mid \frac{q^n - (\varepsilon 1)^n}{q^{n/s} - (\varepsilon 1)^{n/s}}, \tag{2}$$

за исключением случая, когда $(\varepsilon, n, s, q) = (+, 6, 3, 2)$;

(iv) *если $n > 1$, то группа $\mathrm{SL}^\varepsilon_n(q)$ содержит неприводимый элемент порядка r.*

В нижеследующих леммах фактор-группа конечной группы $\mathrm{SL}^\varepsilon_n(q)$ по центральной подгруппе называется *группой типа $A^\varepsilon_{n-1}(q)$*.

Лемма 3. *Пусть q — степень простого числа p. Группа типа $A^\varepsilon_{n-1}(q)$ содержит элемент порядка p^{t+1}, $t \geq 0$, тогда и только тогда, когда $n \geq p^t + 1$.*

Доказательство. См. [7, следствие 0.5] □

Лемма 4. (i) *Пусть $L = \mathrm{L}^\varepsilon_n(q)$ — простая группа. Числа*

$$\frac{q^n - (\varepsilon 1)^n}{d(q - \varepsilon 1)}, \quad \frac{q^{n-1} - (\varepsilon 1)^{n-1}}{d} \tag{3}$$

взаимно просты и являются максимальными по делимости элементами $\omega(L)$.

(ii) *Пусть $n \in \mathbb{N}$, q — степень простого числа p и $\varepsilon \in \{+, -\}$. Предположим, что $n = s + b_1 + \dots + b_k$, где $s = 0$ или $s = p^t$ при $t \geq 0$, $k \geq 0$ и все b_i попарно взаимно просты и больше чем 1. Если $(\varepsilon, q) = (-, 2)$, то предположим дополнительно, что $b_i \neq 2, 3$ для всех i. Если $(\varepsilon, q) = (-, 3)$, то предположим, что $b_i \neq 2$ для всех i. Обозначим $r_i = q^*_{[\varepsilon b_i]}$ (существование $q^*_{[\varepsilon b_i]}$ следует из ограничений на b_i). Тогда $p^{t+1} r_1 \cdot \ldots \cdot r_k \notin \omega\big(\mathrm{SL}^\varepsilon_n(q)\big)$, где предполагается, что $t = 0$ при $s = 0$.*

Доказательство. Сначала докажем (ii). Частный случай $s = p^t$ доказан в [4, лемма 9]. Однако мы не исключаем его из рассмотрения, поскольку приводим здесь другое доказательство. Пусть, напротив, существует $a \in \mathrm{SL}^\varepsilon_n(q)$ порядка $p^{t+1} r_1 \cdot \ldots \cdot r_k$. Тогда a принадлежит централизатору C в $\mathrm{SL}^\varepsilon_n(q)$ полупростого элемента $u = a^{p^{t+1}}$. По [8, предложения 7, 8] группа C является центральным произведением групп $M_{i,j}$, $i \geq 2$, типа $A^\varepsilon_{i-1}(q^{\mu^{(i)}_j})$, расширенным с помощью абелевой группы T порядка $\prod\limits_{i,j}(q^{\mu^{(i)}_j}-(\varepsilon 1)^{\mu^{(i)}_j})/(q-\varepsilon 1)$, где $\mu^{(i)}$ — разбиение n_i и числа n_i удовлетворяют равенству $\sum i\, n_i = n$. В частности,

$$\sum_{i,j} i\,\mu^{(i)}_j = n. \tag{4}$$

Заметим, что $u \in Z(C)$ и $Z(C)$ является абелевой группой порядка, делящего $\prod\limits_{i,j}(q^{\mu^{(i)}_j}-(\varepsilon 1)^{\mu^{(i)}_j})$. Поскольку $|u| = r_1 \cdot \ldots \cdot r_k$, из леммы 2(i) следует, что для каждого $f = 1, \ldots, k$ найдутся i, j такие, что b_f делит $\mu^{(i)}_j$ (если r_f не простое, то здесь необходимо также использовать тот факт, что $Z(C)$ является подгруппой прямого произведения циклических групп порядков $q^{\mu^{(i)}_j}-(\varepsilon 1)^{\mu^{(i)}_j}$ по всем i, j). По предположению все числа b_f попарно взаимно просты и больше чем 1. Поэтому сумма тех $\mu^{(i)}_j$, которые больше 1, не менее чем $b_1 + \cdots + b_k$.

Далее, поскольку C содержит элемент порядка p^{t+1}, одна из компонент $M_{i',j'}$ нетривиальна и для нее выполнено неравенство $i' \geq p^t + 1$ по лемме 3. Если $\mu^{(i')}_{j'} = 1$, то

$$\sum_{i,j} i\,\mu^{(i)}_j \geq b_1 + \cdots + b_k + p^t + 1 > n \tag{5}$$

вопреки (4). Если $\mu^{(i')}_{j'} > 1$, то $i'\,\mu^{(i')}_{j'} \geq p^t + 1 + \mu^{(i')}_{j'}$ и, значит, по-прежнему выполнено (5). Это противоречие завершает доказательство.

Теперь докажем (i). Сначала, следуя предыдущему рассуждению, покажем, что числа (3) принадлежат $\mu(M)$. Пусть k обозначает любое из этих чисел. Хорошо известно, что L содержит элемент порядка k. Проверим максимальность k в $\omega(L)$ относительно делимости. Можно считать, что $(\varepsilon, n, q) \neq (-, 3, 3)$, $(-, 4, 2)$, поскольку для групп $\mathrm{U}_3(3)$ и $\mathrm{U}_4(2)$ утверждение проверяется непосредственно. Предположим, что существует элемент $\bar{a} \in L$, порядок которого кратен k. Тогда прообраз $a \in S = \mathrm{SL}^{\varepsilon}_n(q)$ элемента $\bar{a}$ лежит в централизаторе C в S полупростого элемента u порядка k. Заметим, что обобщенный примитивный делитель $r = q^*_{[\varepsilon n]}$ (соответственно $r = q^*_{[\varepsilon(n-1)]}$) существует, поскольку $L \neq \mathrm{U}_3(3), \mathrm{U}_4(2)$. Тогда $u \in Z(C)$ и, как и выше, получается, что n (соответственно $n-1$) делит некоторое $\mu^{(i)}_j$. Но тогда из (4) следует, что разложением для n является $n = n_1 = \mu^{(1)}_1$ (соответственно $n = n_1 = \mu^{(1)}_1 + \mu^{(1)}_2$, где $\mu^{(1)}_1 = n-1$ и $\mu^{(1)}_2 = 1$). В частности, C совпадает со своей торической частью T, изоморфной циклической группе порядка $(q^n - (\varepsilon 1)^n)/(q - \varepsilon 1)$ (соответственно $q^{n-1} - (\varepsilon 1)^{n-1}$). В силу сопряженности максимальных торов T содержит центр $Z(S)$ порядка d и, значит, порядок элемента $\bar{a} \in T/Z(S)$ не превосходит k.

Наконец, покажем, что числа из (3) взаимно простые. Обозначим

$$x = \frac{(\varepsilon q)^n - 1}{\varepsilon q - 1}, \quad y = \frac{\varepsilon q - 1}{d}, \quad z = \frac{(\varepsilon q)^{n-1} - 1}{\varepsilon q - 1}.$$

Тогда с точностью до знака числа из (3) совпадают с x/d и yz соответственно. Заметим, что $\gcd(x, z) = 1$, поскольку

$$\gcd\left((\varepsilon q)^n - 1, (\varepsilon q)^{n-1} - 1\right) = (\varepsilon q)^{\gcd(n,n-1)} - 1 = \varepsilon q - 1.$$

Положив $f(t) = t^{n-1} + \cdots + t + 1 \in \mathbb{Z}[t]$, можно найти такой многочлен $g(t) \in \mathbb{Z}[t]$, что $f(t) = (t-1)g(t) + n$. Подстановка $t = \varepsilon q$ дает $x = f(\varepsilon q) \equiv n \pmod{\varepsilon q - 1}$. Таким образом, $\gcd(x, \varepsilon q - 1) = \gcd(n, \varepsilon q - 1) = d$, и, значит, $\gcd(x/d, y) = 1$. Требуемое следует из этих замечаний. $\square$

Лемма 5. (i) *Для любого вещественного $x \geq 22$ интервал $(x/3, x/2]$ содержит по меньшей мере одно простое число.*

(ii) *Для любого вещественного $x \geq 57$ интервал $(2x/3, x-16]$ содержит по меньшей мере одно простое число.*

(iii) *Для любого вещественного $x > 45$ интервал $(3x/4, x-8)$ содержит по меньшей мере одно простое число.*

(iv) *Для любого вещественного $x > 27$ интервал $(x/2, x-8)$ содержит по меньшей мере два простых числа.*

Доказательство. (i) Для $x < 72$ утверждение можно проверить непосредственно. Предположим, что $x \geq 72$. Существует $\alpha \in [0, 3)$ такое, что $x/3 + \alpha = 3a$ для некоторого целого числа $a > 1$. Из [9] следует, что интервал $(3a, 4a)$ содержит простое число. Осталось показать, что $4a \leq x/2$. Имеем $4a = 4(x/3 + \alpha)/3 < 4x/9 + 4 = x/2 - (x/18 - 4) \leq x/2$, поскольку $x/18 - 4 \geq 0$. Отсюда следует (i).

Утверждения (i)–(iv) можно доказать аналогично. При этом в (ii) следует использовать более сильный факт: для любого натурального $n \geq 119$ интервал $[n, 1.073n]$ содержит по меньшей мере одно простое число, см. [10]. $\square$

Лемма 6. (i) *Для любого натурального $n \geq 5$ существует разложение $n = n_1 + \dots + n_k$, где $n_1, \dots, n_k$ — попарно взаимно простые натуральные числа, самое большее одно из которых равно 1, такое, что выполнено следующее свойство: для любого $1 \leq j \leq n$ существуют разложение $j = j_1 + \dots + j_{k'}$, где $k' \leq k$, и вложение $\eta : \{j_1, \dots, j_{k'}\} \to \{n_1, \dots, n_k\}$, удовлетворяющее для всех $i = 1, \dots, k'$ условиям:*

(a) *$j_i \leq \eta(j_i)$;*

(b) *если $\eta(j_i) > 1$, то $\gcd(j_i, \eta(j_i)) > 1$.*

(ii) *Для любых натуральных $n \geq 5$ и $1 \leq j \leq n$ таких, что $(n, j) \notin \{(6,3), (8,3), (8,5)\}$, существуют разложение $n = n_1 + \dots + n_k$, где $n_1, \dots, n_k$ — попарно взаимно простые натуральные числа, отличные от $2, 3$, самое большее одно из которых равно 1, и разложение $j = j_1 + \dots + j_{k'}$ с теми же свойствами, что и в (i), удовлетворяющее дополнительному условию: $\gcd(j_i, \eta(j_i)) \neq 3$ при $\eta(j_i) = 6$, где $i = 1, \dots, k'$.*

Доказательство. (i) Для натурального $m > 1$ обозначим через $\varkappa(m)$ наибольший простой делитель числа m.

Покажем, что имеет место более сильный факт: существует требуемое разложение $n = n_1 + \dots + n_k$ с дополнительным свойством

$$\varkappa(n_1 \dots n_k) \leq (n+1)/2. \tag{6}$$

Используем индукцию по n. Предположим, что $n \leq 20$.

Если $n = 5$, то $n = 1 + 4$ — требуемое разложение. В самом деле, при $j = 1, 2, 4$ можно положить $k' = 1$ и $j_1 = j$, тогда как при $j = 3$ или 5 можно положить $k' = 2$ и $j = 1 + 2$ или $j = 1 + 4$ соответственно. Если $n = 6$, то разложим $n = 1+2+3$. Для всех j соответствующее разложение $j = j_1 + \dots + j_{k'}$ очевидно. Если $n = 7$, то положим $n = 1 + 6$. При $j = 1, 2, 3, 6$ положим $k' = 1$, а при $j = 4, 5, 7$ положим $k' = 2$ и $j = 1+3$, $1+4$ или $1+6$ соответственно. Если $n = 9$, то положим $n = 1 + 8$. Для $j = 1$ или четного j положим $k' = 1$, а для нечетного $j > 1$ положим $k' = 2$, $j_1 = 1$ и $j_2 = j - 1$.

Во всех рассмотренных случаях $n = 5, 6, 7, 9$ вложение η очевидно и свойство (6) выполнено.

Далее при $n = 8, 10, 11, \dots, 20$ мы определим рекурсивно $n = [n-r] + r$ для соответственных значений $r = 3, 5, 5, 5, 7, 7, \dots, 7, 5, 3$, где $[n-r]$ обозначает уже определенное разложение для $n - r$. Непосредственно проверяется, что все n_i попарно взаимно просты, самое большее одно из них равно 1 и выполнено (6). Если $j \le n - r$, то разложение $j = j_1 + \dots + j_{k'}$ определяется так же, как для $n - r$, с тем же вложением η, а если $j > n - r$, то положим $j = [j - r] + r$ и продолжим η, положив $\eta(r) = r$. (Заметим, что при $n = 13$ и $j = 7$ разложение $[j - r]$ предполагается пустым.)

Допустим, что $n \ge 21$. По лемме 5(i) существует простое число r такое, что $(n+1)/3 < r \le (n+1)/2$. Поскольку $n - r \ge (n-1)/2 \ge 5$, по индукции существует разложение $n - r = n_1 + \dots + n_{k_0}$, удовлетворяющее условию и такое, что $\varkappa(n_1 \dots n_{k_0}) \le (n - r + 1)/2$. Покажем, что требуемым разложением является $n = n_1 + \dots + n_{k_0} + r$. Поскольку $r > (n - r + 1)/2$, каждый простой делитель любого n_i меньше чем r; в частности, числа $n_1, \dots, n_{k_0}, r$ попарно взаимно просты, самое большее одно из них равно 1, и $\varkappa(n_1 \dots n_{k_0} r) = r \le (n+1)/2$.

Далее, пусть $1 \le j \le n$. Как и выше, если $j \le n - r$, то разложение $j = j_1 + \dots + j_{k'}$ определяется по индукции с тем же вложением η. Предположим, что $j \ge n - r + 1$. Имеем $n - r + 1 \ge r$. Если $j = r$, то это равенство можно взять в качестве (тривиального) разложения j и положить $\eta(r) = r$. В противном случае $j > r$, т. е. $1 \le j - r \le n - r$, и мы положим $j = [j - r] + r$, где разложение $[j - r]$ и вложение η на компонентах разложения $[j - r]$ определены по индукции, и положим $\eta(r) = r$. Из построения ясно, что все требования для η выполнены и тем самым доказано (i).

Теперь докажем (ii). В этом случае найдем требуемые разложения для n и j такие, что $\eta(j_i) = n_i$ для всех $1 = 1, \dots, k'$ (мы можем фиксировать порядок слагаемых n_i, поскольку теперь j зафиксировано.)

(а) Сначала предположим, что либо $j = 2,\ 3,\ n-2,\ n-3$, либо $(n, j) \in \{(8,4), (16,6), (16,10)\}$. Тогда разложения для n и j показаны в табл. 1 в колонках, обозначенных через $[n]$ и $[j]$ соответственно. Заметим, что в каждом случае в силу ограничений на n и j компоненты n_i в разложении $n = n_1 + \dots + n_k$ отличны от $2, 3$ и $\gcd(n_i, j_i) \ne 3$ при $n_i = 6$. Все остальные требования проверяются непосредственно.

(б) Теперь можно считать, что $j \ne 2, 3, n-2, n-3$ и $(n, j) \notin \{(8,4), (16,6), (16,10)\}$. Покажем индукцией по n, что в этом случае имеет место даже более сильный факт: существуют требуемые разложения $n = n_1 + \dots + n_k$ и $j = j_1 + \dots + j_{k'}$, дополнительно удовлетворяющие условию $j_i = n_i$ для всех $i = 1, \dots, k'$.

Заметим, что также мы можем считать, что $j \le n/2$. (В противном случае возьмем $n - j$ вместо j и разложим $n = n_1 + \dots + n_k$ и $n - j = n_1 + \dots + n_{k'}$. Тогда разложение $j = n_{k'+1} + \dots + n_k$ будет требуемым разложением для j, а n сохраняет свое разложение с подходящей перестановкой слагаемых.) Рассмотрим три подслучая.

(б.1) Базис индукции. Если $n \le 112$, то можно непосредственно проверить, что для каждой допустимой пары (n, j) требуемые разложения для n и j имеют один из видов:

1) $n = (j) + (n - j)$, $j = (j)$,
2) $n = (1) + (j - 1) + (n - j)$, $j = (1) + (j - 1)$,
3) $n = (j) + (1) + (n - j - 1)$, $j = (j)$,
4) $n = [j] + [n - j]$, $j = [j]$,

Таблица 1. Разложение для $j = 2, 3, n-2, n-3$
или $(n, j) \in \{(8,4), (16,6), (16,10)\}$

(n, j)	ограничения на n	k	$[n]$	k'	$[j]$
$(n, 2)$	$n \equiv 1 \pmod 2$	2	$(n-1)+1$	1	2
	$n \equiv 0 \pmod 2$	1	n	1	2
$(n, n-2)$	$n \equiv 1 \pmod 2$	2	$1+(n-1)$	2	$1+(n-3)$
	$n \equiv 0 \pmod 2$	1	n	1	$n-2$
$(n, 3)$	$n \equiv 1 \pmod 2$	2	$1+(n-1)$	2	$1+2$
	$n \equiv 0 \pmod 6$	1	n	1	3
	$n \equiv 2 \pmod 6$	3	$1+4+(n-5)$	2	$1+2$
	$n \equiv 4 \pmod 6$	2	$(n-1)+1$	1	3
$(n, n-3)$	$n \equiv 1 \pmod 2$	2	$(n-1)+1$	1	$n-3$
	$n \equiv 0 \pmod 6$	1	n	1	$n-3$
	$n \equiv 2 \pmod 6$	3	$4+(n-5)+1$	2	$2+(n-5)$
	$n \equiv 4 \pmod 6$	2	$1+(n-1)$	2	$1+(n-4)$
$(8,4)$, $(16,6)$, $(16,10)$	—	1	n	1	j

где в 1–3 слагаемое в круглых скобках обозначает единственную компоненту разложения, в то время как в виде 4 слагаемое в квадратных скобках раскладывается, как показано в табл. 2. Например, если $(n, j) = (21, 7)$, то $\gcd(j, n-j-1) = \gcd(7, 13) = 1$ и, значит, разложение из вида 3 удовлетворяет требованиям.

(б.2) Предположим, что $n \geq 113$ и $j \leq 2n/5$. Тогда $n - j \geq 3n/5 > 57$ и по лемме 5(ii) существует простое число r такое, что

$$2(n-j)/3 < r \leq n - j - 16. \tag{7}$$

Ясно, что $r \neq 2, 3$. Более того,

$$j \leq 2(n-j)/3 < r, \tag{8}$$

и, значит,

$$(n-j)/2 < 2(n-j)/3 < r. \tag{9}$$

Далее, пара $(n-r, j)$ удовлетворяет предположению индукции. В самом деле, по (7) имеем $j \neq 2, 3, n-r-2, n-r-3$ и $n - r \geq j + 16 > 16$. Следовательно, пара $(n-r, j)$ является допустимой, и по индукции имеем $n - r = n_1 + \dots + n_k$ и $j = n_1 + \dots + n_{k'}$, где $k' \leq k$ и числа n_i попарно взаимно просты, отличны от $2, 3$ и самое большее одно из них равно 1. Поскольку $r > j$ по (8) и $r > n - r - j$ по (9), отсюда вытекает, что r больше чем все n_i (значит, взаимно просто с ними). Поэтому разложения $n = n_1 + \dots + n_k + r$ и $j = n_1 + \dots + n_{k'}$ искомые.

(б.3) Предположим, что $n \geq 113$ и $j > 2n/5$. Тогда $j > 45$ и по лемме 5(iii) существует простое s такое, что

$$3j/4 < s < j - 8. \tag{10}$$

Поскольку $(n-j)/2 < 3j/4$, имеем

$$(n-j)/2 < s. \tag{11}$$

Таблица 2. Исключительное разложение для допустимых пар (n, j) при $2j \le n \le 112$

(n,j)	$[n-j]$	$[j]$	(n,j)	$[n-j]$	$[j]$	(n,j)	$[n-j]$	$[j]$
$(21,6)$	$4+11$	$1+5$	$(76,36)$	40	$7+29$	$(99,22)$	77	$5+17$
$(25,10)$	$4+11$	$1+9$	$(78,22)$	56	$5+17$	$(99,36)$	63	$5+31$
$(34,12)$	22	$5+7$	$(81,6)$	$4+71$	$1+5$	$(100,12)$	88	$5+7$
$(36,15)$	21	$4+11$	$(81,15)$	$7+59$	15	$(100,22)$	78	$5+17$
$(45,12)$	33	$5+7$	$(81,36)$	45	$7+29$	$(100,45)$	55	$4+41$
$(46,6)$	$11+29$	6	$(85,10)$	$4+71$	$1+9$	$(105,14)$	91	$5+9$
$(46,10)$	$7+29$	10	$(85,15)$	$11+59$	15	$(105,39)$	$5+61$	39
$(49,21)$	$5+23$	21	$(85,34)$	51	$5+29$	$(105,40)$	65	$7+33$
$(51,6)$	$4+41$	$1+5$	$(85,35)$	$9+41$	35	$(106,6)$	$11+89$	6
$(51,15)$	$7+29$	15	$(85,40)$	45	$11+29$	$(106,10)$	$7+89$	10
$(52,18)$	34	$5+13$	$(88,30)$	58	$7+23$	$(106,28)$	78	$5+23$
$(55,10)$	$4+41$	$1+9$	$(91,21)$	$11+59$	21	$(106,36)$	70	$13+23$
$(55,15)$	$11+29$	15	$(91,26)$	65	$7+19$	$(106,40)$	66	$17+23$
$(55,22)$	33	$5+17$	$(91,28)$	63	$5+23$	$(106,50)$	56	$9+41$
$(57,21)$	$5+31$	21	$(91,35)$	$9+47$	35	$(111,6)$	$4+101$	$1+5$
$(64,28)$	36	$5+23$	$(91,39)$	$5+47$	39	$(111,12)$	99	$5+7$
$(66,26)$	40	$7+19$	$(92,14)$	$5+73$	14	$(111,15)$	$7+89$	15
$(69,18)$	51	$5+13$	$(93,24)$	69	$5+19$	$(111,33)$	$5+73$	33
$(70,24)$	46	$5+19$	$(96,20)$	76	$7+13$	$(111,36)$	75	$7+29$
$(76,6)$	$11+59$	6	$(99,21)$	$5+73$	21	$(111,45)$	$7+59$	45
$(76,10)$	$7+59$	10						

В силу ограничения $j \le n/2$ также имеем $(n-j)/2 \ge n/4 > 27$ и, значит, по лемме 5(iv) существует простое число r, отличное от s, такое, что

$$(n-j)/2 < r < n-j-8. \tag{12}$$

Рассмотрим пару $(n-s-r, j-s)$. По (12) и (10) имеем $j-s > 8 > 2,3$; $n-j-r > 8 > 2,3$ и $n-s-r = (n-j-r)+(j-s) > 8+8 = 16$. Таким образом, пара $(n-s-r, j-s)$ является допустимой, и по индукции получаем $n-s-r = n_1 + \dots + n_k$ и $j-s = n_1 + \dots + n_{k'}$. В силу (11) и (12) выполнены соотношения $s, r > (n-j)/2 \ge j/2$. Тем самым s, r отличны от всех n_i (значит, взаимно просты с ними). Следовательно, разложения $n = s + n_1 + \dots + n_k + r$ и $j = s + n_1 + \dots + n_{k'}$ искомые, и лемма доказана. $\square$

Подчеркнем, что отличие п. (ii) леммы 6 от п. (i) не только в требовании $n_i \ne 2,3$, но также и в том, что разложение для n зависит от числа j.

Пусть r — простое число, G — конечная группа и $g \in G$. Будем говорить, что g — элемент *r-максимального порядка*, если $r\,|g| \notin \omega(G)$. Примеры r-максимальных порядков для группы $\mathrm{SL}_n^{\varepsilon}(q)$ даны в лемме 4(ii).

Лемма 7. *Пусть $S = \mathrm{SL}_n^{\varepsilon}(q)$, где $q = p^m$.*

(i) *Пусть* $n \geq 5$ *и* $q > 3$. *Тогда* S *содержит полупростой элемент* g p-*максимального порядка такой, что* $\langle g\rangle \cap Z(S) = 1$ *и для любого* $0 \leq j \leq n$ *произведение некоторых* j *различных характеристических значений элемента* g (*в естественном* n-*мерном представлении*) *равно* 1.

(ii) *Пусть* $n \geq 4$, $0 \leq j \leq n$ *и* $(\varepsilon, n, q) \neq (-, 4, 2)$. *Тогда* S *содержит полупростой элемент* g p-*максимального порядка такой, что* $\langle g\rangle \cap Z(S) = 1$ *и произведение некоторых* j *различных характеристических значений* g (*в естественном* n-*мерном представлении*) *равно* 1.

Доказательство. (i) Пусть разложение $n = n_1 + \dots + n_k$ такое, как утверждается в лемме 6(i). Тогда S содержит естественно вложенную подгруппу, изоморфную $\mathrm{SL}^{\varepsilon}_{n_1}(q) \times \dots \times \mathrm{SL}^{\varepsilon}_{n_k}(q)$. По лемме 2(iv) и в силу ограничения $q > 3$ можно выбрать элемент $g_i \in \mathrm{SL}^{\varepsilon}_{n_i}(q)$ порядка

$$r_i = \begin{cases} 1, & n_i = 1, \\ q^*_{[\varepsilon n_i]}, & n_i > 1. \end{cases} \tag{13}$$

Положим $g = g_1 \dots g_k \in S$ (так, что g — прямая сумма диагональных блоков g_i). Ввиду взаимной простоты компонент $n_1, \dots, n_k$ имеем $|g| = r_1 \dots r_k$, и, значит, $|g|$ — p-максимальный порядок по лемме 4. Заметим также, что по лемме 2(ii) либо $|g|$ взаимно прост с $q - \varepsilon 1$, либо $q = 2^l \pm 1$ и существует $1 \leq i_0 \leq k$ такое, что $n_{i_0} = 2$. Однако в последнем случае $k \geq 2$, поскольку $n \geq 5$. Из этих замечаний следует, что $\langle g\rangle \cap Z(S) = 1$ в силу построения элемента g.

Ясно, что набор характеристических значений g является объединением таких наборов для g_i, которые имеют вид

$$\bigl\{\theta_i, \theta_i^{\varepsilon q}, \theta_i^{(\varepsilon q)^2}, \dots, \theta_i^{(\varepsilon q)^{n_i - 1}}\bigr\}, \tag{14}$$

для некоторых $\theta_i \in F^{\times}$ порядка r_i, $i = 1, \dots, k$, где F — алгебраическое замыкание поля $\mathbb{F}_p$.

Если $j = 0$, возьмем в качестве g произвольный полупростой элемент p-максимального порядка такой, что $\langle g\rangle \cap Z(S) = 1$. Пусть $1 \leq j \leq n$ и $j = j_1 + \dots + j_{k'}$, как утверждается в лемме 6(i). Без ограничения общности (перенумеровав, если необходимо, слагаемые в разложении $n = n_1 + \dots + n_k$) можно считать, что $\eta(j_i) = n_i$, $i = 1, \dots, k'$, где η такое, как определено в лемме 6(i). Достаточно показать, что произведение некоторых различных j_i характеристических значений из (14) равно 1. Можно считать, что $n_i > 1$ (иначе $\theta_i = 1$ и требуемое выполнено). Тогда $d_i = \gcd(j_i, n_i) > 1$ в силу свойства (b) леммы 6(i). Заметим, что по лемме 2(iii)

$$r_i \mid \frac{(\varepsilon q)^{n_i} - 1}{(\varepsilon q)^{n_i/d_i} - 1} = 1 + x + x^2 + \dots + x^{d_i - 1}, \quad x = (\varepsilon q)^{n_i/d_i}. \tag{15}$$

В частности, множество (14) является объединением $f = n_i/d_i$ попарно не пересекающихся подмножеств

$$\bigl\{\theta_i, \theta_i^{x}, \dots, \theta_i^{x^{d_i-1}}\bigr\}, \bigl\{\theta_i^{\varepsilon q}, \theta_i^{x(\varepsilon q)}, \dots, \theta_i^{x^{d_i-1}(\varepsilon q)}\bigr\}, \\ \dots, \bigl\{\theta_i^{(\varepsilon q)^{f-1}}, \theta_i^{x(\varepsilon q)^{f-1}}, \dots, \theta_i^{x^{d_i-1}(\varepsilon q)^{f-1}}\bigr\},$$

в каждом из которых произведение всех элементов равно 1 ввиду (15). Поскольку $j_i/d_i \leq f$, по свойству (a) леммы 6(i) объединение произвольных j_i/d_i

из этих подмножеств дает требуемое множество из j_i различных характеристических значений, произведение которых равно 1.

(ii) Как и выше, можно считать, что $j > 0$. Предположим сначала, что $n \geq 5$ и $(n,j) \notin \{(6,3),(8,3),(8,5)\}$. Тогда разложим $n = n_1 + \dots + n_k$ и $j = j_1 + \dots + j_{k'}$, как утверждается в лемме 6(ii). Как и выше, в силу ограничения $n_i \neq 2, 3$ существует элемент $g = g_1 \dots g_k \in S$, порядок которого $r_1 \dots r_k$ является p-максимальным, где r_i определяются, как в (13). Теперь повторим рассуждение из (i), показав, что существуют j различных характеристических значений элемента g, произведение которых равно 1.

Если $(n,j) \in \{(8,3),(8,5)\}$ и $(\varepsilon, q) \neq (-,2)$, то ввиду (1) можно допустить число 3 в качестве слагаемого в разложении n. Поэтому положим $n = 5+3$, $j = j$ (тривиальное разложение). Если $(n,j,\varepsilon,q) \neq (6,3,+,2)$, то делимость (15) выполнена в силу (2) и можно повторить вышеприведенное рассуждение.

Если $n = 4$ и $(\varepsilon, q) \neq (-,2)$, то снова 3 может быть слагаемым для n, и мы положим $n = 1+3$ при $j = 1$ или 3, разложим тривиально $n = 4$ при $j = 2$ или 4 и применим рассуждение, как выше.

Предположим, что $S = \mathrm{SL}_6(2)$ и $j = 3$. Тогда S содержит элемент g 2-максимального порядка 21, характеристические значения которого равны $\nu_i = \theta^{2^{i-1}}$, $i = 1, \dots, 6$, где $\theta \in \overline{\mathbb{F}}_2^\times$ порядка 21. Заметим, что $Z(S) = 1$ и произведение трех характеристических значений ν_1, ν_3, ν_5 элемента g равно $\theta\theta^4\theta^{16} = 1$, как и требовалось.

Наконец, пусть $S = \mathrm{SU}_8(2)$ и $j = 3$ или 5. Тогда S содержит элемент g 2-максимального порядка 45 блочно диагонального вида $g = g_1g_2g_3$ с тремя блоками размеров 4, 3, 1, причем характеристические значения $\nu_1, \dots, \nu_8$ элемента g равны

$$\underbrace{\theta^3,\ (\theta^3)^{-2},\ (\theta^3)^4,\ (\theta^3)^{-8}}_{g_1},\ \underbrace{\theta^{-5},\ (\theta^{-5})^{-2},\ (\theta^{-5})^4}_{g_2},\ \underbrace{\theta^{30}}_{g_3}, \tag{16}$$

где $\theta \in \overline{\mathbb{F}}_2^\times$ порядка 45. Тогда $\nu_1\nu_3\nu_8 = \nu_2\nu_4\nu_5\nu_6\nu_7 = 1$ и, значит, есть j характеристических значений g, произведение которых равно 1. Поскольку $Z(S) = 1$, получаем требуемое. □

Лемма 8. *Если группа Фробениуса KC с ядром K и циклическим дополнением $C = \langle c \rangle$ порядка n действует точно на векторном пространстве V над полем ненулевой характеристики p, взаимно простой с порядком группы K, то минимальный полином элемента c на V равен $x^n - 1$. В частности, полупрямое произведение $V \rtimes C$ содержит элемент порядка $p \cdot n$ и $\dim C_V(c) > 0$.*

Доказательство см. в [11, лемма 1]. □

Лемма 9. *Группа H распознаваема по спектру среди своих накрытий тогда и только тогда, когда $\omega(H) = \omega(G)$ для любого расщепляемого расширения $G = N \rtimes H$, где N — элементарная абелева r-группа для некоторого r и H действует на N абсолютно неприводимо.*

Доказательство. Пусть G — собственное накрытие H минимального порядка такое, что $\omega(H) = \omega(G)$. По [12, лемма 12] можно считать, что $G = N \rtimes H$, где H действует на элементарной абелевой r-группе N неприводимо. Предположим, что это действие не является абсолютно неприводимым. Пусть F — конечное поле разложения для H характеристики r. Рассмотрим собственный подмодуль N_0 приводимого FH-модуля $N \otimes_{\mathbb{F}_p} F$. Достаточно показать, что

$\omega(N_0 \leftthreetimes H) = \omega(H)$. Пусть, напротив, некоторый элемент $n_0 h \in N_0 \leftthreetimes H$ имеет порядок, не лежащий в $\omega(H)$. Тогда элемент $1+h+h^2+\dots+h^{|h|-1}$, рассматриваемый как линейное преобразование N_0, является ненулевым. Но тогда он также ненулевой как линейное преобразование N, и, значит, G содержит элемент nh порядка $|n_0 h|$; противоречие. $\square$

Лемма 10. *Пусть r — простое число, и пусть $L = \mathrm{L}_n^{\varepsilon}(q)$ — простая группа, где $q = p^m$ и $\varepsilon \in \{+,-\}$. Тогда $\omega(\mathbb{Z}_r \times L) \not\subseteq \omega(L)$.*

Доказательство. Обозначим через a_1 и a_2 числа в (3). По лемме 4(i) существует $i = 1,2$ такое, что $r \nmid a_i$ и $ra_i \notin \omega(L)$. Поскольку $ra_i \in \omega(\mathbb{Z}_r \times L)$, получаем требуемое. $\square$

Лемма 11. *Пусть $L = \mathrm{L}_n(q)$ — простая линейная группа, где $q = p^m$. Тогда L распознаваема по спектру среди своих накрытий тогда и только тогда, когда $\omega(L) = \omega(G)$ для любого расщепляемого расширения $G = N \leftthreetimes L$, где N — элементарная абелева p-группа и L действует на N точно и абсолютно неприводимо.*

Доказательство. По лемме 9 можно считать, что $G = N \leftthreetimes L$, где N — элементарная абелева r-группа для некоторого r и L действует на N абсолютно неприводимо. По лемме 10 группа L действует точно. Образ в L параболической подгруппы из $\mathrm{SL}_n(q)$ вида $q^{n-1} : \mathrm{GL}_{n-1}(q)$ содержит (см. [3, лемма 5]) подгруппу Фробениуса KC с элементарным абелевым ядром порядка q^{n-1} и циклическим дополнением C порядка $a = (q^{n-1}-1)/d$, где $d = \gcd(n, q-1)$. Если $r \neq p$, то по лемме 8 имеем $ra \in \omega(G)$. Однако $ra \notin \omega(L)$ по лемме 4(i). Значит, $r = p$. $\square$

3. Веса неприводимых $\mathbf{SL}_n(F)$-модулей

В этом разделе мы напомним некоторые факты из теории представлений алгебраических групп (подробности см., например, в [13]).

Пусть $G = \mathrm{SL}_n(F)$, где F — алгебраически замкнутое поле характеристики p. Тогда G — простая односвязная алгебраическая группа типа A_l, где $l = n-1$. Обозначим через ω_0 нулевой вес и через $\omega_1, \dots, \omega_l$ — фундаментальные веса группы G (по отношению к фиксированному максимальному тору из G и системе положительных корней). Пусть $\Omega = \mathbb{Z}\omega_1 \oplus \dots \oplus \mathbb{Z}\omega_l$ — решетка весов и Δ — система корней группы G с множеством $\alpha_1, \dots, \alpha_l$ простых корней. Также пусть $\Omega_0 = \mathbb{Z}\alpha_1 \oplus \dots \oplus \mathbb{Z}\alpha_l$ — множество *радикальных весов* и $\Omega^+ = \{a_1\omega_1 + \dots + a_l\omega_l \in \Omega \mid a_1 \geq 0, \dots, a_l \geq 0\}$ — множество *доминантных весов*. Веса из множества $\Omega_k^+ = \{a_1\omega_1 + \dots + a_l\omega_l \in \Omega \mid 0 \leq a_1 < k, \dots, 0 \leq a_l < k\}$ называются *k-ограниченными*, где k обычно обозначает степень числа p.

Для неприводимого (рационального конечномерного) G-модуля L обозначим через $\Omega(L)$ множество весов L и через $\lambda(L)$ — старший вес модуля L. Известно, что $\lambda(L) \in \Omega^+$ и каждый доминантный вес является старшим весом некоторого неприводимого модуля L. Неприводимый G-модуль старшего веса λ обычно обозначается через $L(\lambda)$. Очевидно, что $\Omega(L(\omega_0)) = \{\omega_0\}$. Модуль L называется *p-ограниченным*, если $\lambda(L) \in \Omega_p^+$. Модули $L(\omega_i)$, $i = 1, \dots, l$, называются *микровесовыми модулями*. Строение микровесовых модулей хорошо известно и описывается в следующей лемме (см., например, [13, II.2.15]).

Лемма 12. *Пусть $G = \mathrm{SL}_n(F)$ и $V = F^n$ — естественный G-модуль с каноническим базисом $e_1, \dots, e_n$. Выберем диагональную подгруппу H в качестве* *максимального тора группы G. Тогда e_i — собственный вектор для H с соответствующим весом ε_i. Выберем систему положительных корней $\{\varepsilon_i - \varepsilon_j \mid 1 \le i < j \le n\}$. Тогда $\omega_k = \varepsilon_1 + \dots + \varepsilon_k$ для $1 \le k < n$, микровесовой модуль $L(\omega_k)$ изоморфен k-й внешней степени $\wedge^k V$ и имеет множество весов*

$$\Omega(L(\omega_k)) = \{\varepsilon_{i_1} + \varepsilon_{i_2} + \dots + \varepsilon_{i_k} \mid 1 \le i_1 < i_2 < \dots < i_k \le n\}.$$

Следующее утверждение является уточнением [14, предложение 2.3] для групп типа A_l.

Лемма 13. *Пусть $G = \mathrm{SL}_n(F)$ и L — неприводимый p-ограниченный G-модуль. Запишем $\lambda(L) = a_1\omega_1 + \dots + a_l\omega_l$. Предположим, что $i \in \{0, 1, \dots, l\}$ — однозначно определенное число такое, что*

$$a_1 + 2a_2 + \dots + la_l \equiv i \pmod{l+1}. \tag{17}$$

Тогда $\Omega(L(\omega_i)) \subseteq \Omega(L)$.

Доказательство. По [13, предложение II.2.4] множество $\Omega(L)$ лежит в единственном смежном классе $\Omega : \Omega_0$ и по [14, предложение 2.3] $\Omega(L)$ содержит ω_0, если вес $\lambda(L)$ радикальный, и $\Omega(L(\omega_i))$ для некоторого $i = 1, \dots, l$ иначе. В последнем случае индекс i однозначно определен, поскольку веса $\omega_0, \omega_1, \dots, \omega_l$ образуют трансверсаль множества $\Omega : \Omega_0$ в силу [15, VIII, § 7.3, предложение 8].

Следовательно, достаточно заметить, что произвольный вес $\lambda = a_1\omega_1 + \dots + a_l\omega_l \in \Omega$ лежит в смежном классе $\omega_i + \Omega_0$ тогда и только тогда, когда выполнено (17). В самом деле, если $\lambda = \alpha_i$ — простой корень, то $(a_1, \dots, a_l)$ — i-я строка матрицы Картана типа A_l и (17) проверяется непосредственно. В силу сказанного выше любой вес λ лежит в $\omega_i + \Omega_0$ для некоторого i и добавление или вычитание положительных корней из λ сохраняет соотношение (17) и принадлежность смежному классу $\omega_i + \Omega_0$. Из этих замечаний следует требуемое. □

4. Доказательство основных результатов

Доказательство теоремы 1. По лемме 9 можно считать, что W — абсолютно неприводимый модуль для L. Кроме того, в силу [16, теорема 43] можно считать, что W — ограничение на $S = \mathrm{SL}_n^{\varepsilon}(q)$ неприводимого модуля $L(\lambda)$ для группы $G = \mathrm{SL}_n(F)$, где $\lambda \in \Omega_q^+$ и $F = \overline{\mathbb{F}}_p$. Положим $l = n - 1$.

(a) Сначала рассмотрим случай, когда $n \ge 5$ и $q > 3$. Достаточно показать, что найдется полупростой элемент $g \in S$ p-максимального порядка такой, что $\langle g \rangle \cap Z(S) = 1$, который централизует ненулевой вектор $w \in W$. В самом деле, если это выполнено, то элемент $w\bar{g} \in W \rtimes L$ имеет порядок $p\,|g| \notin \omega(L)$ ввиду $\omega(L) \subseteq \omega(S)$, где $\bar{g}$ — образ g в L.

Выберем в качестве максимального тора группы G диагональную подгруппу H. Запишем

$$\lambda = \lambda_0 + p\lambda_1 + \dots + p^{m-1}\lambda_{m-1}, \quad \lambda_i \in \Omega_p^+.$$

По теореме Стейнберга о скрученном тензорном произведении [16, теорема 41] имеем

$$L(\lambda) \cong L(\lambda_0) \otimes L(\lambda_1)^{\rho} \otimes \dots \otimes L(\lambda_{m-1})^{\rho^{m-1}}, \tag{18}$$

где ρ обозначает скручивание с помощью отображения Фробениуса, соответствующего автоморфизму $x \mapsto x^p$ поля F. По лемме 13 для каждого $i =$

$0, \dots, m-1$ найдется $k_i \in \{0, \dots, l\}$ такое, что $\Omega(L(\omega_{k_i})) \subseteq \Omega(L(\lambda_i))$. В частности, множество $\Omega(L(\lambda))$ содержит все возможные веса вида

$$\mu_0 + p\mu_1 + \dots + p^{m-1}\mu_{m-1}, \quad \mu_i \in \Omega(L(\omega_{k_i})). \tag{19}$$

По лемме 12 вес μ_i может быть произвольной суммой k_i различных весов из множества $\{\varepsilon_1, \dots, \varepsilon_n\}$.

Пусть $g \in S$ — полупростой элемент, существование которого утверждается в лемме 7(i). Тогда найдется $a \in G$ такой, что $h = {}^a g \in H$. По лемме 7(i) элемент g имеет k_i различных характеристических значений, произведение которых равно 1, и мы положим μ_i равным сумме соответствующих k_i весов ε_j так, что $\mu_i(h) = 1$ для всех $i = 0, \dots, m-1$. Обозначим через μ сумму (19) для только что определенных весов μ_i. Тогда $\mu \in \Omega(L(\lambda))$ и

$$\mu(h) = \mu_0(h)\mu_1(h)^p \dots \mu_{m-1}(h)^{p^{m-1}} = 1.$$

Пусть $w_0 \in W$ — весовой вектор для G веса μ так, что $w_0 h = \mu(h) w_0 = w_0$. Положим $w = w_0 a$. Тогда

$$wg = w_0 ag = w_0 ha = w_0 a = w.$$

Таким образом, g — требуемый полупростой элемент из S.

(б) Теперь предположим, что $n \geq 4$, q простое и $(\varepsilon, n, q) \neq (-, 4, 2)$. В этом случае $\lambda \in \Omega_q^+ = \Omega_p^+$. По лемме 13 существует $j \in \{0, \dots, l\}$ такое, что $\Omega(L(\omega_j)) \subseteq \Omega(L(\lambda))$. Значит, по лемме 12 $\Omega(L(\lambda))$ содержит сумму произвольных j различных весов из $\{\varepsilon_1, \dots, \varepsilon_n\}$. Теперь выберем по лемме 7(ii) полупростой элемент $g \in S$ p-максимального порядка такой, что $\langle g \rangle \cap Z(S) = 1$ и произведение некоторых j различных характеристических значений элемента g равно 1. Существует элемент $a \in G$ такой, что $h = {}^a g \in H$ и, значит, произведение некоторых j характеристических значений h также равно 1. Положим μ равным сумме соответствующих j весов $\{\varepsilon_1, \dots, \varepsilon_n\}$ так, что $\mu(h) = 1$. (Тогда $\mu \in \Omega(L(\lambda))$ в силу вышесказанного.) Теперь если $w_0 \in W$ — весовой вектор для G, то, как и в случае (а), имеем $wg = w$, где $w = w_0 a$ и, значит, g — требуемый элемент.

Подчеркнем, что принципиальное отличие этого случая от случая (а) в том, что модуль W является p-ограниченным и выбор элемента g зависит от W.

(в) Пусть, наконец, $n = 4$ и q четно. По лемме 6 в [4] группа L содержит подгруппу Фробениуса KC с ядром K порядка $q_{[\varepsilon 4]}$ и циклическим дополнением C порядка 4. Из леммы 10 следует, что KC действует точно на W, и, значит, по лемме 8 имеем $2|C| \in \omega(W \rtimes L)$. Однако $2|C| = 8 \notin \omega(L)$ по лемме 3. Тем самым теорема доказана. $\square$

Следствие 1 теперь напрямую вытекает из леммы 11 и теоремы 1.

Автор выражает благодарность Д. О. Ревину, прочитавшему рукопись статьи и сделавшему ряд полезных замечаний.

ЛИТЕРАТУРА

1. *Нерешенные вопросы* теории групп. Коуровская тетрадь. 14-е изд. Новосибирск: Ин-т математики СО РАН, 1999.
2. *Заварницин А. В.* Веса неприводимых $\mathrm{SL}_3(q)$-модулей в характеристике определения // Сиб. мат. журн. 2004. Т. 45, № 2. С. 319–328.
3. *Васильев А. В., Гречкосеева М. А.* О распознавании по спектру конечных простых линейных групп над полями характеристики 2 // Сиб. мат. журн. 2005. Т. 46, № 4. С. 749–758.

4. *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 УНЦ РАН. 2007. Т. 13, № 1. С. 89–98.
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. *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.
7. *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.
8. *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.
9. *Hanson D.* On a theorem of Sylvester and Schur // Canad. Math. Bull. 1973. V. 16. P. 195–199.
10. *Rohrbach H., Weis J.* Zum finiten Fall des Bertrandschen Postulates // J. Reine Angew. Math. 1964/5. Bd 214/5. S. 432–440.
11. *Мазуров В. Д.* О множестве порядков элементов конечной группы // Алгебра и логика. 1994. Т. 33, № 1. С. 81–89.
12. *Zavarnitsine A. V.* Recognition of the simple groups $L_3(q)$ by element orders // J. Group Theory. 2004. V. 7, N 1. P. 81–97.
13. *Jantzen J. C.* Representations of algebraic groups. Second edition. Providence, RI: Amer. Math. Soc., 2003. (Math. Surveys Monogr.; 107).
14. *Suprunenko I. D., Zalesskii A. E.* Fixed vectors for elements in modules for algebraic groups // Internat. J. Algebra Comput. 2007. V. 17, N 5–6. P. 1249–1261.
15. Bourbaki N. Éléments de mathématique. Fasc. XXXVIII: Groupes et algèbres de Lie. Chapitre VII: Sous-algèbres de Cartan, éléments réguliers. Chapitre VIII: Algèbres de Lie semi-simples déployées. Paris: Hermann, 1975. (Actualités Sci. Industr.; N 1364).
16. *Стейнберг Р.* Лекции о группах Шевалле. М.: Мир, 1975.

Статья поступила 20 ноября 2007 г.

Заварницин Андрей Витальевич
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
zav@math.nsc.ru