Сибирский математический журнал
Сентябрь—октябрь, 2024. Том 65, № 5

УДК 512.542

СИЛЬНАЯ π–ТЕОРЕМА СИЛОВА ДЛЯ ГРУПП $\mathrm{PSL}_2(q)$

Д. О. Ревин, В. Д. Шепелев

Аннотация. Пусть π — некоторое множество простых чисел. Конечная группа называется *π-группой*, если все простые делители ее порядка принадлежат π. Следуя Виланду, говорят, что для конечной группы G верна π-теорема Силова, если в G сопряжены все максимальные π-подгруппы; если же π-теорема Силова верна для каждой подгруппы группы G, то говорят, что для G верна сильная π-теорема Силова. Известно, что сильная π-теорема Силова верна для группы тогда и только тогда, когда она верна для всякого неабелева композиционного фактора этой группы. Вопрос о том, для каких конечных простых неабелевых групп верна сильная π-теорема Силова, поставлен Виландом в 1979 г. К настоящему времени ответ известен для спорадических и знакопеременных групп. В статье дается арифметический критерий справедливости сильной π-теоремы Силова для групп $\mathrm{PSL}_2(q)$.

DOI 10.33048/smzh.2024.65.517

Ключевые слова: π-теорема Силова, сильная π-теорема Силова, проективная специальная линейная группа.

Введение

Рассматриваются только конечные группы и термин «группа» всюду означает «конечная группа». Пусть π — некоторое множество простых чисел. Через π' обозначается множество $\mathbb{P} \setminus \pi$, где $\mathbb{P}$ — множество всех простых чисел. Для натурального числа n символом $\pi(n)$ обозначается множество всех простых делителей n. Для группы G полагаем $\pi(G) = \pi(|G|)$. Группа G, для которой $\pi(G) \subseteq \pi$, называется *π-группой.* Подгруппа H группы G называется *холловой π-подгруппой*, если H является π-группой и $\pi(|G : H|) \subseteq \pi'$.

Используя терминологию Ф. Холла [1], будем говорить, что конечная группа G *обладает свойством* D_π (пишем $G \in D_\pi$), если все ее максимальные π-подгруппы сопряжены. В терминологии Виланда [2] о группе со свойством D_π говорят также, что для нее *верна π-теорема Силова.* Из теоремы Силова легко вытекает, что $G \in D_\pi$ тогда и только тогда, когда выполнены следующие условия:

- группа G содержит холлову π-подгруппу;
- все холловы π-подгруппы группы G сопряжены;
- всякая π-подгруппа группы G содержится в некоторой холловой π-подгруппе.

Таким образом, свойство D_π означает выполнение в группе полного аналога теоремы Силова для π-подгрупп, причем при $\pi = \{p\}$, где $p \in \mathbb{P}$, максимальные

Работа выполнена за счет РНФ, проект № 24-21-00163, https://rscf.ru/project/24-21-00163/.

π-подгруппы и холловы π-подгруппы — это в точности силовские p-подгруппы, и π-теорема Силова верна для любой группы. В [3, 4] доказано, что группа одновременно для всех множеств π обладает свойством D_π тогда и только тогда, когда она разрешима. В частности, для любой неразрешимой группы G найдется множество π такое, что $G \notin D_\pi$. Например, $A_5 \notin D_{\{3,5\}}$, поскольку в A_5 нет подгрупп порядка 15, а всякая холлова $\{3,5\}$-подгруппа в A_5 должна была бы иметь порядок 15. В общем случае свойство D_π не наследуется подгруппами, что подтверждает следующий

Пример. Рассмотрим группу $\mathrm{SL}_2(16)$, имеющую порядок, равный $4080 = 2^4 \cdot 3 \cdot 5 \cdot 17$. Подгруппа H всех диагональных матриц в ней имеет порядок 15 и является холловой $\{3,5\}$-подгруппой. Любая группа, порядок которой делит 15, как известно, должна быть циклической. Из очевидных соображений линейной алгебры подгруппа в $\mathrm{SL}_2(16)$, порядок которой делит 15, сопряжена с подгруппой из H. Тем самым $\mathrm{SL}_2(16)$ обладает свойством $D_{\{3,5\}}$. Однако в $\mathrm{SL}_2(16)$ есть подгруппа, изоморфная $\mathrm{SL}_2(4) \simeq A_5$, которая, как было показано ранее, не обладает свойством $D_{\{3,5\}}$.

В 1979 г. Виланд на конференции по конечным группам в г. Санта-Круз поставил следующую проблему.

Проблема А [5, вопрос (h)]. *В каких простых конечных группах верна сильная π-теорема Силова: все подгруппы обладают свойством D_π?*

Следуя [6], через W_π будем обозначать класс всех конечных групп, для которых справедлива сильная π-теорема Силова. Если конечная группа G обладает свойством W_π, то для краткости будем писать $G \in W_\pi$. Проблема А может быть переформулирована эквивалентным образом: *какие простые конечные группы обладают свойством W_π?*

Для фиксированного множества π свойство W_π, как и свойство D_π, является обобщением свойства разрешимости группы, поскольку означает выполнение для π-подгрупп данной группы аналога теоремы Силова, который в случае разрешимых групп гарантируется теоремой Холла, а подгруппа разрешимой группы всегда разрешима. Более того, в отличие от свойства D_π свойство W_π наследуется подгруппами.

Известно [6, следствие 6.7], что группа обладает свойством W_π тогда и только тогда, когда любой ее композиционный фактор обладает данным свойством. Поэтому полное решение проблемы А позволило бы о любой конечной группе с известным композиционным строением сказать, обладает она свойством W_π или нет.

Проблема А к настоящему моменту решена для спорадических [7] и знакопеременных групп [8, теорема 3]. Ни одной серии групп лиева типа, для которой была бы решена проблема А, до настоящего момента не было известно. В данной статье будет предложено решение проблемы Виланда для серии групп $\mathrm{PSL}_2(q)$.

Всюду символом (a,b) будем обозначать наибольший общий делитель целых чисел a и b.

Пусть $m > 1$ и a — целые числа, причем $(a,m) = 1$. *Мультипликативным порядком числа a по модулю m* будем называть число

$$\mathrm{ord}_m\, a = \min\{d \in \mathbb{N} : a^d \equiv 1 \pmod{m}\}.$$

Для формулировки основного результата статьи понадобится следующее обозначение. Пусть r — простое число и a — целое число, взаимно простое с r. По определению полагаем

$$\operatorname{ord}^*_r a := \operatorname{ord}_{r\cdot(2,r)} a = \begin{cases} \operatorname{ord}_r a, & \text{если } r \text{ нечетно,} \\ \operatorname{ord}_4 a, & \text{если } r = 2. \end{cases}$$

Теорема. *Пусть p — простое число, $q = p^{2^k m}$ для некоторых нечетного числа m и неотрицательного целого числа k. Положим также $q_0 := p^m$ и $\tau := \pi \cap \pi(\mathrm{PSL}_2(q))$. Тогда $\mathrm{PSL}_2(q) \in W_\pi$, если и только если выполнено одно из следующих условий:*

(W_1) $\pi(\mathrm{PSL}_2(q)) \subseteq \pi$;

(W_2) $p = 2$, $\tau = \{2\}$;

(W_3) $2 \notin \pi$, $p \in \pi$, $|\tau \cap \{3,5\}| \leq 1$ *и* $\tau \subseteq \{p\} \cup \pi(q_0 - 1)$;

(W_4) $p \notin \pi$, $|\tau \cap \{2,3,5\}| \leq 1$ *и* $\operatorname{ord}^*_r q_0 = \operatorname{ord}^*_s q_0$ *для любых* $r, s \in \tau$.

Отметим, что за исключением группы ${}^2B_2(q)$ любая группа L лиева типа с базовым полем из q элементов содержит секцию[1)], изоморфную $\mathrm{PSL}_2(q)$. Поскольку свойство W_π наследуется секциями (см. лемму 2 ниже), выполнение одного из условий (W_1)–(W_4) является необходимым для того, чтобы L обладала свойством W_π.

Приведем примеры, показывающие, что условия (W_3) и (W_4) действительно могут выполняться для определенных множеств π и бесконечных серий q.

Пример. Пусть n — натуральное число. Тогда для группы $\mathrm{PSL}_2(7^n)$ и множества $\pi = \{3,7\}$ справедливо условие (W_3). Тем самым $\mathrm{PSL}_2(7^n) \in W_\pi$.

Пример. Пусть n — натуральное число. Тогда для группы $\mathrm{PSL}_2(3^n)$ и множества $\pi = \{2,7\}$ справедливо условие (W_4). Тем самым $\mathrm{PSL}_2(3^n) \in W_\pi$.

В самом деле, $7 \in \tau$, если и только если $3^{2n} \equiv 1 \pmod 7$, т. е. n кратно 3. Таким образом, если n не делится на 3, то $\tau = \{2\}$ и условие (W_4) выполнено. Если же n делится на 3, запишем n в виде $n = 2^k \cdot 3 \cdot (2s-1)$. Имеем

$$q_0 = 3^{3(2s-1)} = 27^{2s-1},$$

откуда q_0 сравнимо с -1 по модулям 4 и 7 и

$$\operatorname{ord}^*_2 q_0 = \operatorname{ord}^*_7 q_0 = 2.$$

Условие (W_4) снова выполнено.

Таким образом, существуют бесконечные серии проективных специальных групп степени 2, удовлетворяющие сильной π-теореме Силова, холловы π-подгруппы которых отличны от силовских подгрупп и самих групп.

Обозначения и предварительные результаты

Утверждения, использующие классификацию конечных простых групп, помечены символом (mod CFSG).

Через q всегда обозначается степень некоторого фиксированного простого числа p. В соответствии с обозначениями из Атласа [9] проективная специальная линейная группа $\mathrm{PSL}_2(q)$ над полем из q элементов будет также обозначаться символом $L_2(q)$.

[1)] Под секциями группы понимаются гомоморфные образы ее подгрупп.

Известно, что

$$|L_2(q)| = \frac{q(q-1)(q+1)}{(2, q-1)}.$$

Отсюда

$$\pi(L_2(q)) = \{p\} \cup \pi(q-1) \cup \pi(q+1).$$

Лемма 1. *Если G — разрешимая группа, то $G \in W_\pi$ для любого множества простых чисел π.*

Лемма 2 [10, лемма 2, (mod CFSG)]. *Класс W_π замкнут относительно взятия подгрупп, гомоморфных образов и расширений.*

Из леммы 2, в частности, вытекает, что $\mathrm{PGL}_2(q) \in W_\pi$, если и только если $L_2(q) \in W_\pi$.

Лемма 3 [11, гл. II, теорема 8.27]. *Любая подгруппа группы $L_2(p^n)$, где p — простое число и n — натуральное число, принадлежит следующему списку:*

(1) *элементарная абелева p-группа;*
(2) *циклическая группа порядка z, где $z \mid \frac{p^n \pm 1}{e}$ и $e = (p^n - 1, 2)$;*
(3) *группа диэдра порядка $2z$, где z из (2);*
(4) *знакопеременная группа A_4 при условии $p > 2$ или $p = 2$ и $n \equiv 0 \pmod 2$;*
(5) *симметрическая группа S_4 при условии $p^{2n} - 1 \equiv 0 \pmod{16}$;*
(6) *знакопеременная группа A_5 при условии $p = 5$ или $p^{2n} - 1 \equiv 0 \pmod 5$;*
(7) *полупрямое произведение элементарной абелевой группы порядка p^l и циклической группы порядка t при условии, что $l \leq n$, $t \mid p^l - 1$ и $t \mid p^n - 1$;*
(8) *группа $L_2(p^l)$, если $l \mid n$;*
(9) *группа $\mathrm{PGL}_2(p^l)$, если $2l \mid n$.*

В частности, группа $L_2(q)$ содержит подгруппу, изоморфную A_5, если и только если $5 \in \pi\,(L_2(q))$.

Лемма 4 [8, теорема 3]. *Пусть π — некоторое множество простых чисел. Положим $\sigma := \pi \cap \pi(L_2(q))$. Группа $L_2(q)$, где $q = p^n$, p — простое число и n — натуральное число, обладает свойством D_π, если и только если выполнено одно из следующих условий:*

(D_1) *$\pi(L_2(q)) \subseteq \pi$ или $|\sigma| \leq 1$;*
(D_2) *$2 \notin \pi, p \in \pi$ и $\sigma \subseteq \{p\} \cup \pi(q-1)$;*
(D_3) *$2, p \notin \pi$ и $\sigma \subseteq \pi(q-\varepsilon)$ для некоторого $\varepsilon = \pm 1$;*
(D_4) *$2 \in \pi, 3, p \notin \pi$ и $\sigma \subseteq \pi(q-\varepsilon)$, где $\varepsilon = \pm 1$ таково, что $4 \mid q - \varepsilon$.*

В частности, если $2, 3 \in \pi$, то $L_2(q) \in D_\pi$ тогда и только тогда, когда $L_2(q)$ — π-группа.

Отметим, что неравенство $|\sigma| \leq 1$, фигурирующее в условии (D_1) леммы 4, не исключает выполнения одного из условий (D_2)–(D_4). Кроме того, поскольку $L_2(4) \simeq A_5$, из леммы 4 следует, что $A_5 \in D_\pi$, если и только если либо $|\pi \cap \{2, 3, 5\}| \leq 1$, либо $\{2, 3, 5\} \subseteq \pi$.

Доказательство теоремы

Группы $L_2(2)$ и $L_2(3)$ являются разрешимыми, а потому согласно лемме 1 обладают свойством W_π для любого множества простых чисел π. В табл. 1

указано, какое именно из условий (W_1)–(W_4) теоремы выполнено для каждой из групп $L_2(2)$ и $L_2(3)$ в зависимости от множества π. Поэтому в дальнейшем будем считать, что $q > 3$.

Таблица 1. Выполнение условий (W_1)–(W_4) для групп $L_2(2)$ и $L_2(3)$

G	$\pi(G)$	(W_1)	(W_2)	(W_3)	(W_4)
$L_2(2)$	$\{2,3\}$	$2,3\in\tau$	$2\in\tau, 3\notin\tau$	—	$2\notin\tau$
$L_2(3)$	$\{2,3\}$	$2,3\in\tau$	—	$3\in\tau, 2\notin\tau$	$3\notin\tau$

Напомним, что $q = p^{2^k\cdot m}$, где p — простое число и m — нечетное число. Положим $n = 2^k \cdot m$. Докажем, что $L_2(q) \in W_\pi$, если и только если выполнено условие $(*)$:

$(*_1)$ $L_2(q)$ — π-группа

или

$(*_2)$ $|\tau \cap \{2,3,5\}| \leq 1$ и $L_2(p^t) \in D_\pi$ для любого $t \mid n$.

Докажем необходимость условия $(*)$ для того, чтобы группа $L_2(q)$ обладала свойством W_π.

Согласно п. (8) леммы 3 для любого $t \mid n$ группа $L_2(q)$ содержит подгруппу, изомофную $L_2(p^t)$. Поэтому из условия $L_2(q) \in W_\pi$ следует, что $L_2(p^t) \in D_\pi$ для любого $t \mid n$.

Допустим, что $A_5 \leq L_2(q)$. Тогда из условия $L_2(q) \in W_\pi$ вытекает, что $A_5 \in D_\pi$. В силу замечания после леммы 4 это означает, что $|\tau \cap \{2,3,5\}| \leq 1$ или $\{2,3,5\} \subseteq \tau$. Последнее с учетом леммы 4 выполняется для $L_2(q) \in D_\pi$ в том и только том случае, когда $\pi(L_2(q)) \subseteq \pi$, т. е. выполнено $(*_1)$. Если же $|\tau \cap \{2,3,5\}| \leq 1$, то с учетом сказанного в предыдущем абзаце выполнено $(*_2)$.

Допустим теперь, что $L_2(q)$ не содержит подгруппы, изоморфной A_5, т. е. $5 \notin \pi(L_2(q))$ (см. лемму 3). Тогда согласно лемме 4 условие $L_2(q) \in W_\pi$ влечет, что либо $\{2,3\} \subseteq \tau$ и тем самым выполнено условие $(*_1)$, либо $|\tau \cap \{2,3\}| = |\tau \cap \{2,3,5\}| \leq 1$ и с учетом сказанного выполнено $(*_2)$. Необходимость установлена. Докажем достаточность.

Условие $(*_1)$ очевидно достаточно. Кроме того, из леммы 1 следует, что $L_2(q) \in W_\pi$ тогда и только тогда, когда все неразрешимые подгруппы группы $L_2(q)$ обладают свойством D_π. В качестве таковых согласно лемме 3 могут возникнуть только A_5 и подполевые подгруппы (группы из пп. (8), (9) леммы 3). Требование $|\tau \cap \{2,3,5\}| \leq 1$ в условии $(*_2)$ означает, что $A_5 \in D_\pi$, а из того, что $L_2(p^t) \in D_\pi$ для любого $t \mid n$, следует, что все неабелевы композиционные факторы подполевых подгрупп обладают свойством D_π и тем самым этим свойством обладают сами подполевые подгруппы (см. лемму 2). Достаточность условия $(*)$ установлена.

Таким образом, теорема будет доказана, если установим, что условие $(*)$ равносильно выполнению одного из условий (W_1)–(W_4). Поскольку $(*_1)$ — это в точности условие (W_1), будем доказывать эквивалентность

$$(*_2) \quad \Leftrightarrow \quad (W_2) \vee (W_3) \vee (W_4). \tag{1}$$

Оставшаяся часть доказательства разбита на две части, представляющие собой обоснование необходимости $(\Rightarrow)$ и достаточности $(\Leftarrow)$ дизъюнкции $(W_2)\vee(W_3)\vee(W_4)$ в эквивалентности (1).

В случае $|\tau| \leq 1$, во-первых, выполнено одно из условий (W_2)–(W_4), а во-вторых, $L_2(q) \in W_\pi$, т. е. эквивалентность (1) имеет место. Поэтому в дальнейшем, если не оговорено особо, будем считать, что $|\tau| > 1$.

Необходимость. Случай 1: $p \in \pi$. Если $p = 2$, то в соответствии с леммой 4 и сделанными ранее предположениями группа $L_2(q)$ обладает свойством D_π тогда и только тогда, когда $\tau = \{2\}$, вопреки предположению о том, что $|\tau| > 1$.

Допустим теперь, что $p \neq 2$. Тогда для $L_2(q)$ выполнено условие (D_2) в лемме 4 и множество τ состоит только из нечетных чисел. Покажем, что для справедливости условия $(*_2)$ необходимо, чтобы выполнялось (W_3). От противного: пусть утверждение (W_3) неверно. Тогда существует число $r \in \tau$ такое, что

$$r \notin \{p\} \cup \pi(q_0 - 1).$$

Ввиду условия (D_2) имеем $r \in \pi(q-1) \setminus \pi(q_0 - 1)$. Число $\operatorname{ord}_r q_0$ делит 2^k, так как $q_0^{2^k} = q$ сравнимо с 1 по модулю r. Значит, $\operatorname{ord}_r q_0 = 2^c$ для некоторого числа $c \geq 0$, причем $c \neq 0$, поскольку иначе $r \in \pi(q_0 - 1)$. Число r делит $q_0^{2^c} - 1$, откуда

$$r \in \pi \cap \pi\big(L_2\big(q_0^{2^{c-1}}\big)\big)$$

и r не делит $q_0^{2^{c-1}} - 1$ по определению $\operatorname{ord}_r q_0$. Но так как $p \in \pi$, для $L_2\big(q_0^{2^{c-1}}\big)$ справедливо условие (D_2) в лемме 4, означающее, что r делит $q_0^{2^{c-1}} - 1$; противоречие.

Случай 2: $p \notin \pi$. В рассматриваемом случае $L_2(q) \in D_\pi$ означает справедливость условия (D_3) леммы 4, т. е. $2, p \notin \pi$ и $\tau \subseteq \pi(q - \varepsilon)$ для некоторого числа $\varepsilon = \pm 1$. Поскольку $L_2(p^t) \in D_\pi$ для любого $t \mid n$, из сказанного следует, что для такого t группа $L_2(p^t)$ также удовлетворяет условию (D_3) (даже если $|\pi \cap \pi(L_2(p^t))| \leq 1$). Покажем, что выполняется условие (W_4).

Допустим, $\varepsilon = -1$. Заметим, что поскольку $2 \notin \pi$, любое число, принадлежащее τ, нечетно. Поэтому $\operatorname{ord}^*_r q_0 = \operatorname{ord}_r q_0$ для любого $r \in \tau$. Так как

$$\tau \subseteq \pi(q - \varepsilon) = \pi(q + 1) = \pi\big(q_0^{2^k} + 1\big) \subseteq \pi\big(q_0^{2^{k+1}} - 1\big),$$

можем заключить, что для любого числа $r \in \tau$ справедливо соотношение

$$\operatorname{ord}_r q_0 \mid 2^{k+1}.$$

Допустим, что существуют число $r \in \tau$ и неотрицательное число c такие, что

$$\operatorname{ord}_r q_0 = 2^c < 2^{k+1}.$$

Тогда, во-первых, r делит $q_0^{2^c} - 1$ и, во-вторых, $c < k + 1$, т. е. $c \leq k$. Отсюда следует, что r делит $q_0^{2^k} - 1 = q - 1$. Поскольку r нечетно, это противоречит тому, что $\tau \subseteq \pi(q + 1)$. Значит, для любых $r, s \in \tau$ имеет место равенство $\operatorname{ord}^*_r q_0 = \operatorname{ord}^*_s q_0 = 2^{k+1}$ и условие (W_4) в случае $\varepsilon = -1$ выполнено.

Пусть теперь $\varepsilon = 1$. Предположим, что условие (W_4) неверно, т. е. существуют числа $r, s \in \tau$ такие, что $\operatorname{ord}^*_r q_0 \neq \operatorname{ord}^*_s q_0$. Так как $2 \notin \pi$, вновь заключаем, что $\operatorname{ord}^*_r q_0 = \operatorname{ord}_r q_0$ и $\operatorname{ord}^*_s q_0 = \operatorname{ord}_s q_0$. Числа $\operatorname{ord}_r q_0$ и $\operatorname{ord}_s q_0$ делят 2^k, так как число $q_0^{2^k} = q$ сравнимо с 1 по модулям r и s. Положим

$$\operatorname{ord}_r q_0 = 2^a \quad \text{и} \quad \operatorname{ord}_s q_0 = 2^b$$

для некоторых различных неотрицательных целых чисел a и b. Можем считать, что $a < b$, т. е. $a \le b-1$. Тогда $r \mid q_0^{2^a} - 1$ и потому $r \mid q_0^{2^{b-1}} - 1$. Кроме того, s делит число

$$q_0^{2^b} - 1 = \big(q_0^{2^{b-1}} - 1\big)\big(q_0^{2^{b-1}} + 1\big)$$

и не делит $q_0^{2^{b-1}} - 1$ по определению $\operatorname{ord}_s q_0$. Следовательно, $s \mid q_0^{2^{b-1}} + 1$. Тем самым $r, s \in \pi \cap \pi\big(L_2\big(q_0^{2^{b-1}}\big)\big)$. Теперь, с одной стороны, для $L_2\big(q_0^{2^{b-1}}\big)$ имеет место (D_3), а с другой стороны, $r \in \pi\big(q_0^{2^{b-1}} - 1\big)$ и $s \in \pi\big(q_0^{2^{b-1}} + 1\big)$ вопреки (D_3); противоречие.

Случай 3: $2 \in \pi$, $p \notin \pi$. В рассматриваемом случае выполнено условие (D_4): $2 \in \pi$, $3, p \notin \pi$ и $\tau \subseteq \pi(q - \varepsilon)$, где число $\varepsilon = \pm 1$ таково, что $4 \mid q - \varepsilon$. Ясно также, что число p должно быть нечетным. Так как

$$2 \in \pi \cap \pi(L_2(p^t)) \quad \text{и} \quad L_2(p^t) \in D_\pi \quad \text{для любого } t \mid n,$$

заключаем, что для всех таких t группа $L_2(p^t)$ удовлетворяет условию (D_4) (даже если $\pi \cap \pi(L_2(p^t)) = \{2\}$). Покажем, что выполняется условие (W_4).

Если $\varepsilon = -1$, то из соотношения

$$4 \mid q - \varepsilon = q + 1$$

следует, что число n нечетно и тем самым $q = q_0$. Включение $\tau \subseteq \pi(q+1)$ эквивалентно тому, что для любых чисел $r, s \in \tau$ выполнено соотношение $\operatorname{ord}_r^* q = \operatorname{ord}_s^* q = 2$, поэтому условие (W_4) в данном случае выполнено.

Пусть теперь $\varepsilon = 1$. Повторяя рассуждения, использованные при доказательстве условия (W_4) в случае $2, p \notin \pi$, заключаем, что найдется неотрицательное целое число c с тем свойством, что $\operatorname{ord}_r q_0 = 2^c$ для всех $r \in \tau \setminus \{2\}$ (иначе найдутся $r, s \in \tau \setminus \{2\}$ и $t \mid n$ такие, что $r \in \pi(p^t - 1)$ и $s \in \pi(p^t + 1)$ вопреки условию (D_4) для группы $L_2(p^t)$). Предположим, что $c > 1$. Тогда, как легко видеть, $\tau \subseteq \pi\big(q_0^{2^{c-1}} + 1\big)$. Из того, что $|\tau| > 1$, следует, что τ содержит по крайней мере одно нечетное число. Заметим, что при $c > 1$ число $q_0^{2^{c-1}}$ является полным квадратом нечетного числа и потому сравнимо с 1 по модулю 4. Получили противоречие с условием (D_4) для группы $L_2\big(q_0^{2^{c-1}}\big)$. Следовательно, $c \in \{0, 1\}$.

Из того, что квадрат нечетного числа сравним с 1 по модулю 4, вытекает также включение $\operatorname{ord}_2^* q_0 \in \{1, 2\}$. К тому же с учетом сказанного в предыдущем абзаце справедливо также соотношение $\operatorname{ord}_r^* q_0 \in \{1, 2\}$ для любого $r \in \tau$. Докажем, что $\operatorname{ord}_r^* q_0 = \operatorname{ord}_s^* q_0$ для всех $r, s \in \tau$.

Заметим, что для любого простого числа $r \in \tau$ выполнены эквивалентности

$$\begin{aligned} \operatorname{ord}_r^* q_0 = 1 \quad &\Leftrightarrow \quad r(2, r) \mid q_0 - 1, \\ \operatorname{ord}_r^* q_0 = 2 \quad &\Leftrightarrow \quad r(2, r) \mid q_0 + 1. \end{aligned} \tag{2}$$

Из вышесказанного следует, что

$$\tau \subseteq \pi(q_0 - 1) \cup \pi(q_0 + 1) \subseteq \pi(L_2(q_0)).$$

В рассматриваемом случае $2 \in \pi$ и $p \notin \pi$. Из условия $L_2(q_0) \in D_\pi$ и условия (D_4) заключаем, что существует $\varepsilon_0 = \pm 1$ такое, что $r(2, r) \mid q_0 - \varepsilon_0$ для всех $r \in \tau$. С учетом эквивалентностей (2) это означает, что

$$\operatorname{ord}_r^* q_0 = \operatorname{ord}_s^* q_0 \quad \text{для всех} \quad r, s \in \tau.$$

Учитывая условия $p \notin \pi$ и $|\{2,3,5\} \cap \tau| \leq 1$, заключаем, что справедливо утверждение (W_4).

Достаточность. Легко заметить, что любое из условий (W_2)–(W_4) влечет неравенство

$$|\tau \cap \{2,3,5\}| \leq 1.$$

Поэтому импликация «$\Leftarrow$» будет доказана, если докажем, что выполнения любого из условий (W_2)–(W_4) достаточно для того, чтобы утверждение

$$L_2(p^t) \in D_\pi \quad \text{для всех } t \mid n$$

оказалось верным.

Достаточность (W_2). Из условия (W_2) следует, что $L_2(p^t) \in D_\pi$ для всех $t \mid n$ по теореме Силова. Отметим, что из тех же соображений $L_2(p^t) \in D_\pi$ во всех случаях, когда $|\tau| \leq 1$. Поэтому, как и ранее, в дальнейшем предполагаем, что $|\tau| > 1$.

Достаточность (W_3). Из условия (W_3) следует, что $2 \notin \pi$ и $p \in \pi$. Допустим, что существует число $t \mid n$ такое, что $L_2(p^t) \notin D_\pi$. Тогда в силу того, что $p \in \pi$, для $L_2(p^t)$ не выполняется условие (D_2) леммы 4, т. е. существует число $r \in \pi \cap \pi(L_2(p^t))$ такое, что $r \notin \{p\} \cup \pi(p^t - 1)$. Ясно, что $r \in \pi(p^t + 1)$. Число t имеет вид $t = 2^a \cdot b$, где $0 \leq a \leq k$ и $b \mid m$. С одной стороны,

$$r \mid p^{2^a \cdot b} + 1,$$

откуда

$$r \mid p^{2^a \cdot m} + 1 = q_0^{2^a} + 1.$$

С другой стороны, $r \in \tau \subseteq \{p\} \cup \pi(q_0 - 1)$ согласно условию (W_3), причем $r \neq p$ в силу выбора r. Тогда

$$r \mid q_0 - 1 \quad \text{и потому} \quad r \mid q_0^{2^a} - 1.$$

Значит, $r \mid (q_0^{2^a} + 1) - (q_0^{2^a} - 1) = 2$. Но тогда $r = 2 \notin \pi$; противоречие.

Достаточность (W_4). Из условия (W_4) следует, что $p \notin \pi$ и поэтому любое число из $\pi \cap \pi(L_2(p^t))$ будет принадлежать либо $\pi(p^t - 1)$, либо $\pi(p^t + 1)$, причем обоим множествам одновременно может принадлежать только 2. Кроме того, утверждается, что $\tau \subseteq \pi(q - \varepsilon)$ для некоторого $\varepsilon = \pm 1$. Чтобы показать это, достаточно установить, что любые два нечетных простых числа из τ одновременно делят число $q-1$ или одновременно делят число $q+1$. В силу того, что согласно условию (W_4) для любых двух нечетных чисел $r, s \in \tau$ мультипликативные порядки числа q_0 по модулям r и s равны, для каждого натурального i выполнено также равенство $\operatorname{ord}_r q_0^i = \operatorname{ord}_s q_0^i$. И если бы существовали нечетные числа $r, s \in \tau$ такие, что $r \in \pi(q-1)$ и $s \in \pi(q+1)$, то была бы верна следующая цепочка равенств:

$$1 = \operatorname{ord}_r q = \operatorname{ord}_r q_0^{2^k} = \operatorname{ord}_s q_0^{2^k} = \operatorname{ord}_s q = 2;$$

противоречие.

В дальнейшем всюду число $\varepsilon = \pm 1$ таково, что $\tau \subseteq \pi(q - \varepsilon)$.

Допустим сначала, что $2 \notin \pi$. Предположим, что существует некоторое число $t \mid n$ такое, что $L_2(p^t) \notin D_\pi$. В частности, для $L_2(p^t)$ не выполняется условие (D_3) леммы 4. Поэтому, так как $2, p \notin \pi$, найдутся (нечетные) числа $r, s \in \pi \cap \pi(L_2(p^t))$ такие, что $r \in \pi(p^t - 1)$ и $s \in \pi(p^t + 1)$. В силу условия (W_4) возможны два случая.

Первый случай: $\varepsilon = 1$. Тогда $r, s \in \tau \subseteq \pi(q-1)$. Из условия (W_4) и из нечетности чисел r и s следует, что $\mathrm{ord}_r\, q_0 = \mathrm{ord}_s\, q_0 = 2^c$ для некоторого $0 \le c \le k$. Имеем $t = 2^a \cdot b$, где $0 \le a \le k$ и $b \mid m$. Из того, что

$$s \mid p^{2^a \cdot b} + 1 \text{ и } r \mid p^{2^a \cdot b} - 1,$$

вытекают соотношения

$$s \mid p^{2^a \cdot m} + 1 = q_0^{2^a} + 1 \text{ и } r \mid p^{2^a \cdot m} - 1 = q_0^{2^a} - 1.$$

Из сказанного следует, что

$$2^c = \mathrm{ord}_r\, q_0 \le 2^a,$$

откуда $c \le a$. Поскольку $s \mid q_0^{2^c} - 1$, имеем $s \mid q_0^{2^a} - 1$. Значит, $s \mid (q_0^{2^a} + 1) - (q_0^{2^a} - 1) = 2$, следовательно, $s = 2 \notin \pi$; противоречие.

Второй случай: $\varepsilon = -1$. Тогда $r, s \in \tau \subseteq \pi(q+1)$. Так как число r делит $p^t - 1$, оно делит также $p^n - 1 = q - 1$. Но тогда r делит одновременно $q-1$ и $q+1$, что невозможно, так как $2 \notin \pi$; противоречие.

Тем самым доказано, что если $2 \notin \pi$, то из условия (W_4) следует $(*_2)$.

Теперь допустим, что $2 \in \pi$. Тогда с учетом условия (W_4) имеем $3, p \notin \pi$ и $p \ne 2$. Можно считать, что $\tau \setminus \{2\} \ne \varnothing$. Заметим также, что $\mathrm{ord}_2^*\, q_0 \in \{1, 2\}$, и с учетом эквивалентностей (2) условие (W_4) означает, что либо $\tau \subseteq \pi(q_0 - 1)$ и $4 \mid q_0 - 1$, либо $\tau \subseteq \pi(q_0 + 1)$ и $4 \mid q_0 + 1$.

Рассмотрим ситуацию, когда $\varepsilon = 1$. В соответствии со сделанным замечанием разберем два возможных случая.

Первый случай: $\tau \subseteq \pi(q_0 - 1)$ и $4 \mid q_0 - 1$. С одной стороны, $4 \mid p^2 - 1$ в силу нечетности p и число $\mathrm{ord}_4\, p$ делит 2. С другой стороны, число $\mathrm{ord}_4\, p$ делит m, так как $p^m = q_0$ сравнимо с 1 по модулю 4. Поскольку m нечетно, заключаем, что $\mathrm{ord}_4\, p = 1$. Значит, 4 делит число $p - 1$ и, следовательно, число $p^t - 1$ для любого $t \mid n$. Учитывая, что $\tau \subseteq \pi(q_0 - 1)$, и повторяя рассуждения, проделанные при доказательстве достаточности условия (W_3), получаем включение

$$\pi \cap \pi(L_2(p^t)) \subseteq \pi(p^t - 1) \quad \text{для любого} \quad t \mid n.$$

Значит, для всех групп $L_2(p^t)$, где $t \mid n$, выполнено условие (D_4) леммы 4 и потому справедливо условие $(*_2)$.

Второй случай: $\tau \subseteq \pi(q_0 + 1)$ и $4 \mid q_0 + 1$. Очевидно, что тогда число n должно быть четным (иначе число ε было бы равно -1). Несложно понять также, что если $t \mid n$ и t нечетно, то $t \mid m$, откуда $\pi \cap \pi(L_2(p^t)) \subseteq \pi(p^t + 1)$ и $4 \mid p^t + 1$. Докажем, что если t четно и $t \mid n$, то $\pi \cap \pi(L_2(p^t)) \subseteq \pi(p^t - 1)$ и $4 \mid p^t - 1$. Последнее верно в силу того, что квадрат нечетного числа сравним с 1 по модулю 4. Предположим, что существует некоторое число $t \mid n$, для которого $\pi \cap \pi(L_2(p^t)) \not\subseteq \pi(p^t - 1)$. Тогда существует нечетное число $r \in \pi \cap \pi(L_2(p^t))$ такое, что $r \in \pi(p^t + 1)$. Число t запишем в виде $t = 2^a \cdot b$, где $1 \le a \le k$ и $b \mid m$. Из того, что r делит число $p^{2^a \cdot b} + 1$, следует, что r делит также

$$p^{2^a \cdot m} + 1 = q_0^{2^a} + 1.$$

Но в силу условий $a \geq 1$ и $r \in \pi(q_0+1)$ число r будет делителем числа $q_0^{2^a}-1$. Тем самым r делит одновременно числа $q_0^{2^a}-1$ и $q_0^{2^a}+1$, что невозможно, так как r нечетно; противоречие.

Из сказанного следует, что в рассматриваемом случае для любого $t \mid n$ выполнены соотношения

$$\pi \cap \pi(L_2(p^t)) \subseteq \pi(p^t - \varepsilon_t) \quad \text{и} \quad 4 \mid p^t - \varepsilon_t, \quad \text{где } \varepsilon_t = (-1)^t.$$

Поэтому для любой группы $L_2(p^t)$, где $t \mid n$, выполняется условие (D_4) леммы 4, откуда следует $(*_2)$.

Пусть, наконец, $\varepsilon = -1$. Ситуация, когда $\tau \subseteq \pi(q_0-1)$, невозможна, так как иначе множество τ содержалось бы в $\pi(q-1)$ вопреки тому, что $\varepsilon = -1$. Следовательно, $\tau \subseteq \pi(q_0+1)$ и 4 делит q_0+1. Отметим, что число n должно быть нечетным, т. е. $q = q_0$, поскольку в противном случае были бы справедливы соотношения

$$\tau \subseteq \pi(q_0+1) \subseteq \pi(q_0^2-1) \subseteq \pi(q-1).$$

Поэтому $\tau \subseteq \pi(q_0+1) = \pi(q+1)$. Отсюда и из нечетности n следует, что для любого $t \mid n$ никакое число из $\pi \cap \pi(L_2(p^t)) \setminus \{2\}$ не делит $p^t - 1$. Кроме того, $4 \mid p+1$, так как иначе число $\mathrm{ord}_4\, p$ равнялось бы 1, откуда бы следовало, что 4 делит $q-1$, а это противоречило бы тому, что 4 делит число $q_0+1 = q+1$. Значит, для любого $t \mid n$ имеют место соотношения

$$\pi \cap \pi(L_2(p^t)) \subseteq \pi(p^t+1) \quad \text{и} \quad 4 \mid p^t+1,$$

которые с учетом того, что $2 \in \pi$ и $3, p \notin \pi$, означают справедливость для $L_2(p^t)$ условия (D_4) в лемме 4. Значит, $L_2(p^t) \in D_\pi$ и выполнено условие $(*_2)$.

Теорема доказана. □

Благодарности. Авторы благодарны А. А. Бутурлакину и рецензенту за внимательное чтение рукописи и замечания, позволившие улучшить ее первоначальный вариант.

ЛИТЕРАТУРА

1. *Hall P.* Theorems like Sylow's // Proc. London Math. Soc. (3). 1956. V. 6. P. 286–304.
2. *Wielandt H.* Entwicklungslinien in der Strukturtheorie der endlichen Gruppen // Proc. Intern. Congress Math., Edinburgh, 1958. London: Cambridge Univ. Press, 1960. P. 268–278.
3. *Hall P.* A note on soluble groups // J. London Math. Soc. 1928. V. 3. P. 98–105.
4. *Hall P.* A characteristic property of soluble groups // J. London Math. Soc. 1937. V. 12. P. 198–200.
5. *Wielandt H.* Zusammengesetzte Gruppen: Hölders Programm heute // The Santa Cruz conf. on finite groups, Santa Cruz, 1979. Proc. Sympos. Pure Math. Providence RI: Am. Math. Soc., 1980. V. 37. P. 161–173.
6. *Вдовин Е. П., Ревин Д. О.* Теоремы силовского типа // Успехи мат. наук. 2011. Т. 66, № 5. С. 3–46.
7. *Манзаева Н. Ч.* Решение проблемы Виланда для спорадических групп // Сиб. электрон. мат. изв. 2012. Т. 9. С. 294–305.
8. *Ревин Д. О.* Свойство D_π в конечных простых группах // Алгебра и логика. 2008. Т. 47, № 3. С. 364–394.
9. *Conway J. H., Curtis R. T., Norton S. P., Parker R. A., Wilson R. A.* Atlas of finite groups. Oxford: Clarendon Press, 1985.
10. *Вдовин Е. П., Манзаева Н. Ч., Ревин Д. О.* О наследуемости свойства D_π подгруппами // Тр. ИММ УрО РАН. 2011. Т. 17, № 4. С. 44–52.

11. *Huppert B.* Endliche Gruppen I. Berlin: Springer-Verl., 1967.

Поступила в редакцию 10 апреля 2024 г.
После доработки 11 июня 2024 г.
Принята к публикации 20 июня 2024 г.

Ревин Данила Олегович (ORCID 0000-0002-8601-0706)
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
revin@math.nsc.ru

Шепелев Виталий Денисович (ORCID 0000-0002-8411-2805)
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090;
Новосибирский государственный университет,
ул. Пирогова, 1, Новосибирск 630090
v.shepelev@g.nsu.ru