

УДК 512.542

О КОНЕЧНЫХ ГРУППАХ С ХОЛЛОВЫМИ $\{2, r\}$ -ПОДГРУППАМИ

*д-р физ.-мат. наук, проф. Э.М. ПАЛЬЧИК, С.Ю. БАШУН, канд. физ.-мат. наук А.В. КАПУСТО
(Полоцкий государственный университет)*

Описываются конечные группы из множества $\text{Chev}(2)$, которые имеют холловы $\{2, r\}$ -подгруппы для всех нечетных простых делителей r порядков групп, кроме двух из них.

1. Введение

Пусть X – конечная группа четного порядка, t и s – различные простые нечетные делители ее порядка $|X|$, σ – множество остальных нечетных простых делителей числа $|X|$. Пусть X имеет холловы $\{2, r\}$ -подгруппы, где r пробегает множество σ . Что можно сказать о строении группы X ? В этой статье мы рассмотрим часть этой задачи, когда $X \in \text{Chev}(2)$.

В работе используются стандартные обозначения и терминология теории конечных групп, которые можно найти в [1 – 4]. Кроме [4] для групп лиевского типа используются обозначения из [5 и 6].

Отметим, что основные результаты о существовании холловых подгрупп в конечных группах получены Ф. Холлом [7], С.А. Чунихиным [8], Ф. Гроссом [9 – 11], Д.О. Ревиным [12, 13], Е.П. Вдовиным и Д.О. Ревиным [14, 6].

2. Обозначения и терминология

Для удобства чтения приведем основные обозначения:

- π – множество некоторых простых чисел;
- π' – множество простых чисел, такое, что $\pi' \cap \pi = \emptyset$;
- $\pi(n)$ – множество различных простых делителей натурального числа n ;
- $|X|$ – порядок конечной группы X ;
- $\pi(X) = \pi(|X|)$;
- S_π -подгруппа – холлова π -подгруппа A группы X , такая, что $\pi(A) \subseteq \pi$ и индекс $|X:A|$ ее в X есть π' -число;
- $\text{Syl}_p(X)$ – множество S_p -подгрупп группы X ;
- следуя [7], будем говорить, что группа X удовлетворяет свойству (или обладает свойством):
 - E_π , если она обладает холловой π -подгруппой;
 - C_π , если она удовлетворяет свойству E_π и любые две ее холловы π -подгруппы сопряжены в X ;
 - D_π , если она удовлетворяет свойству C_π и любая ее π -подгруппа лежит в некоторой холловой π -подгруппе;
- $[n]$ – целая часть рационального числа n ;
- (m, n) – наибольший общий делитель чисел m и n ;
- a/b – a делит b ($a \nmid b$ – a не делит b);
- $AwrB$ – сплетение группы A с помощью группы B ;
- Z_n, D_n, E_n – соответственно циклическая, диэдральная, элементарная абелева группа порядка n ;
- $GF(q)$ – поле Галуа порядка $q = p^n$, где p – характеристика поля;
- под группой Шевалле понимается любая фактор-группа универсальной группы Шевалле;
- любая группа Шевалле X рассматривается над конечным полем K характеристики p и с X ассоциируется система корней Φ , обозначения типов систем корней стандартны [4, 5];
- поле K считается равным полю $GF(q^2)$, если Φ имеет тип ${}^2A_1, {}^2D_1, {}^2E_6$; полю $GF(q^3)$, если Φ имеет тип 3D_4 ; полю $GF(q)$ в остальных случаях. Во всех случаях поле $GF(q)$ называют полем определения группы X ;
- всякая группа Шевалле X обладает двумя характерными подгруппами B и N такими, что $X = BNB$, $B = N_X(P)$, где $P \in \text{Syl}_p(X)$; $H = B \cap N$ – абелева p' -группа, $B = P\lambda H$, $H \triangleleft N$, $N/H = W$ – группа

Вейля системы корней Φ для X и ассоциируется далее с X . H называют подгруппой Картана, B – подгруппой Бореля, а N – мономиальной подгруппой группы X . Группа W порождается s инволюциями w_i , $1 \leq i \leq s$, с полным множеством определяющих соотношений $(w_i \cdot w_j)^{k_{ij}} = 1$, $1 \leq i, j \leq s$. Число s называется рангом группы W и левым рангом группы X ;

- параболической подгруппой группы X называется любая подгруппа, содержащая $N_X(P) = B$;

- все конечные группы Шевалле с полем определения $GF(p^n) = GF(q)$ (нормальные и скрученные типы) мы обозначаем символом $Chev(p)$. Если мы желаем подчеркнуть, что речь идет о присоединенной версии группы $X \in Chev$ (с $Z(X) = 1$), то условимся писать $X \in Chev^a$ (или $X \in Chev^a(p)$);

- S^n – симметрическая группа перестановок и символов;
- A_n – знакопеременная группа перестановок и символов;
- X' – коммутант группы X .

3. Используемые результаты

3.1. ЛЕММА. Пусть x – натуральное число. Тогда

- (1) $(x-1, x+1) \in \{1, 2\}$;
- (2) $(x-1, x^2+x+1) \in \{1, 3\}$;
- (3) $(x-1, x^2+1) \in \{1, 2\}$;
- (4) $(x+1, x^2+1) \in \{1, 2\}$;
- (5) $(x-1, x^2-x+1) = 1$;
- (6) $(x^2 \pm x+1, x^2+1) = 1$;
- (7) $(x+1, x^2-x+1) \in \{1, 3\}$;
- (8) $(x+1, x^2+x+1) = 1$;
- (9) $(x^3+1, x^2+x+1) = 1$.

Доказательство

Эти утверждения хорошо известны и легко доказываются.

Докажем, например, (7) и (9).

Предположим, что $(x+1, x^2-x+1) = d \neq 1$. Тогда d делит их сумму: $d \mid (x^2+2)$. Кроме того, d делит $x+1$ и x^2-1 . Поэтому d делит $x^2+2-x^2+1=3$. Этим (7) доказано.

Аналогично, если $(x^3+1, x^2+x+1) = d \neq 1$, то d делит x^2-x-1 . Тогда d должно делить $(x^2+x+1)+(x^2-x-1)=2x^2$, т.е. $d \mid 2$. Но это невозможно, так как x^2+x+1 есть нечетное число. Этим (9) доказано. Лемма доказана.

3.2. ТЕОРЕМА [16].

(1) Если p – простое число, $n \geq 2$ – натуральное число, то существует простое число z такое, что $z \mid (p^n-1)$, но $z \nmid (p^i-1)$ для $1 \leq i < n$, исключая два случая: (а) $n=6$, $p=2$; (б) $n=2$, $p=2^q-1$, q – простое число (z называют примитивным делителем числа p^n-1).

(2) Если $p^m-r^n=1$, где p и r – простые числа, m и n – натуральные числа, то $(p^m, r^n) \in \{(3^2, 2^3); (3, 2); (p, 2^{2^k}); (2^m, r), m$ – простое число, k – натуральное число или $k=0\}$.

3.3. ТЕОРЕМА [17]. Если $\frac{x^a-1}{x-1} = r^b$, где r – простое число, x – натуральное число, a и b – натуральные числа, то a – простое число, $r \equiv 1 \pmod{a}$ или $a=2=r$. (Отметим, что если x – простое число, то это утверждение есть в [16]).

3.4. ЛЕММА. Пусть p, r, s – попарно различные простые числа, $q = p^k$, k – натуральное число, $k \geq 1$. Предположим, что $(q+1)(q^2+q+1) = r^n \cdot s^m$, где m и n – натуральные числа. Тогда

$$(1) \quad n > 0, \quad m > 0;$$

$$(2) \quad p^k \in \{2, 3, 8\}.$$

Доказательство

(1) Предположим, что $m = 0$ (случай $n = 0$ исключается аналогично). Тогда $q+1 = r^l$, $l \leq n$, $q^2+q+1 = r^{n-l}$. По теореме 3.2 (2) тогда

$$(r^l, p^k) \in \{(3^2, 2^3); (3, 2); (r, 2^{2^k}); (2^m, p)\}. \quad (3.1)$$

Если $r \neq 2$, то по теореме 3.3 $r \equiv 1 \pmod{3}$, так как $a = 3$ во втором соотношении $\frac{q^3-1}{q-1} = r^{n-l}$.

Поэтому в (3.1) первые две возможности отпадают. Так как $q^2+q+1 = r^{n-l}-1 = (r-1)(r^{n-l-1}+\dots+1) = q(q+1)$, то 3 делит либо q , либо $q+1$. Если $3/q$, то в (3.1) третья возможность дает противоречие, так как $p = 2$.

Если $3/(q+1)$, то $r = 3$ ввиду $q+1 = r^l$. Но эти возможности из (3.1) уже исключены ранее.

Итак, пусть $r = 2$. По теореме 3.3 тогда $a = 2$, хотя выше показано, что $a = 3$. Поэтому и четвертая возможность в (3.1) исключается и (1) доказано.

(2) Из леммы 3.1 (8) следует, что $q+1 = s^m$, а $q^2+q+1 = r^n$ (случай $q+1 = r^n$, $q^2+q+1 = s^m$ рассматривается аналогично). По теореме 3.2 (2)

$$(s^m, p^k) \in \{(3^2, 2^3); (3, 2); (s, 2^{2^k}); (2^m, p), m - \text{простое число}\}. \quad (3.2)$$

Из $\frac{q^3-1}{q-1} = q^2+q+1 = r^n$ и теоремы 3.3 следует, что $r \equiv 1 \pmod{3}$. Поэтому $q(q+1) = r^n-1 = (r-1)(r^{n-1}+\dots+1)$ и либо 3 делит q , либо $3/(q+1)$.

Если $3/q$, то из (3.2) следует, что $q = p = 3 \in \{2, 3, 8\}$.

Если $3/(q+1)$, то из $q+1 = s^m$ следует, что $s = 3$. Из (3.2) теперь следует, что (2) доказано. Лемма доказана.

3.5. ТЕОРЕМА ([11, теорема 3.1]). Пусть $X \in \text{Chev}(p)$, A – холлова π -подгруппа в X , $3 \notin \pi$, $p \in \pi$. Тогда $p = 2$ или $2 \notin \pi$; A содержится в подгруппе Бореля из X , либо $A = X \cong {}^2B_2(2^{2k+1})$. X удовлетворяет свойству C_π .

3.6. ЛЕММА. Пусть $q = p^n$, где p – простое число, n – натуральное число. Пусть r и s – различные простые числа, a и b – натуральные числа. Предположим, что

$$\frac{q^4-1}{q \pm 1} = r^a \cdot s^b. \quad (3.3)$$

Тогда

$$1) \quad a > 0, \quad b > 0 \text{ или } q = 2, \quad q+1 = 3, \quad r \cdot s = 5;$$

$$2) \text{ если в (3.3) } \frac{q^4-1}{q-1} = r^a \cdot s^b, \text{ то имеет место одна из возможностей:}$$

$$2.1) \quad q = 2, \quad s = 3, \quad r = 5, \quad a = 1 = b;$$

$$2.2) \quad q = p, \quad s = 2, \quad q+1 = 2^{b-1}, \quad q^2+1 = 2 \cdot r^a, \quad b-1 - \text{простое число};$$

$$2.3) \quad q = 2^{2^k}, \quad q+1 = s, \quad q^2+1 = r, \quad a = 1 = b, \quad k - \text{натуральное число};$$

3) если в (3.3) $\frac{q^4-1}{q+1} = r^a \cdot s^b$, то имеет место одна из возможностей:

3.1) $q = 4, r = 17, s = 3, a = 1 = b$;

3.2) $q = 3, s^b = 4, r^a = 5$;

3.3) $q = 9, s^b = 2^4, r^a = 41$;

3.4) $q = p, s = 2, s^b = 2^{2^k+1}$ для некоторого натурального числа $k, q^2+1 = 2 \cdot r^a$.

Всюду r и s могут меняться ролями.

Доказательство

1) Предположим, что $b = 0$ (случай $a = 0$ рассматривается аналогично). Тогда $(q \mp 1)(q^2+1) = r^a$. По лемме 3.1 (3, 4) $r = 2$ или $q = 2$. Тогда или $q \mp 1 = 2$, а $q^2+1 = 2^{a-1}$, или $q \mp 1 = 2^{a-1}$, а $q^2+1 = 2$. Так как $q^2 \neq 1$, то пусть $q \mp 1 = 2$ и $q = 3$. Но тогда $q^2+1 = 10 = 2 \cdot 5 \neq 2^{a-1}$. Этим 1) доказано.

2) Пусть $(q+1)(q^2+1) = r^a \cdot s^b$. По теореме 3.2 (1) число $q^4 - 1$ имеет примитивный делитель t , который не делит $q^2 - 1$, т.е. t не делит $(q-1)$ и $(q+1)$.

Пусть для определенности $t = r$ (случай $t = s$ рассматривается аналогично). Так как $r \nmid (q+1)$, то $q+1 = s^m, m \leq b$. По теореме 3.2 (2)

$$(s^m, p^n) \in \{(3^2, 2^3); (3, 2); (s, 2^{2^k}); (2^m, p)\}. \tag{3.4}$$

По лемме 3.1 (4) $(q+1, q^2+1) \in \{1, 2\}$. Предположим сначала, что $(q+1, q^2+1) = 1$. Тогда $q^2+1 = r^a, m = b$. Из теоремы 3.2 (2) следует, что $(r^a, p^{2n}) \in \{(r, 2^{2^{k+1}})\}$. Из (3.4) теперь следует, что имеем заключение 2.3). Пусть теперь $(q+1, q^2+1) = 2$. Тогда, так как $t \nmid (q+1)$, то $s = 2$. Поэтому (3.4) дает нам единственную возможность $s^m = 2^m, p^n = p, q^2+1 = 2 \cdot r^a, q+1 = 2^{b-1}$. Это дает нам заключение 2.2).

Заключение 2.1) следует из 2.3) при $k = 0$. Тогда $q = 2, s^m = s = 3, r = 5, a = 1, b = 1$.

3) Пусть теперь $(q-1)(q^2+1) = r^a \cdot s^b$. Так как $r \nmid (q-1)$, то $q-1 = s^m, m \leq b$. Из теоремы 3.2 (2) следует, что

$$(p^n, s^m) \in \{(3^2, 2^3); (3, 2); (p, 2^{2^k}); (2^n, s)\}. \tag{3.5}$$

По лемме 3.1 (3) $(q-1, q^2+1) \in \{1, 2\}$. Если $(q-1, q^2+1) = 1$, то $q^2+1 = r^a, m = b$. По теореме 3.2 (2) $(r^a, p^{2n}) \in \{(r, 2^{2^l})\}$. Вместе с (3.5) это дает, что $2^n = 2^{2^{l-1}}$. Так как n – простое число, то $2^{l-1} = 2$ или 1, т.е. $q = 4$, или 2. Если $q = 2$, то $q^2+1 = 5 = r, s^b = 1$, и это отмечено в заключении 3.5 (1). Если $q = 4$, то $q^2+1 = 17 = r, s^m = s = 3$. Этот случай имеется в заключении 3.1).

Если $(q-1, q^2+1) = 2$, то $q^2+1 = 2 \cdot r^a, q-1 = 2^{b-1}$. Из теоремы 3.2 (2) тогда следует, что $(p^n, 2^{b-1})$ находится среди первых трех возможностей, указанных в (3.5). Если $q = 9$, то имеем заключение 3.3). Если $q = 3$, то имеем заключение 3.2). Если $q = p$, то имеем заключение 3.4) леммы. Лемма доказана.

3.7. ЛЕММА. Пусть $q = 2^n, n$ – натуральное число. Предположим, что $q^2 \mp q + 1 = p^m$ для простого числа p и натурального числа m . Тогда $m = 1$.

Доказательство

Предположим сначала, что $m = 2 \cdot k$. Тогда $q^2 \mp q + 1 = p^{2k} - 1 = (p^k - 1)(p^k + 1)$. По лемме 3.1 (1) можно считать, что $p^k - 1 = 2 \cdot a, p^k + 1 = 2^{n-1} \cdot b$ для целых нечетных чисел a и b (случай $p^k - 1 = 2^{n-1} \cdot a, p^k + 1 = 2 \cdot b$

аналогичен). Тогда $p^{k+1} = \frac{1}{2} \cdot 2^n \cdot b = \frac{1}{2} \cdot q \cdot b$, $p^{k-1} = p^{k+1} - 2 = \frac{1}{2} \cdot q \cdot b - 2$. Тогда $q(q \pm 1) = \frac{1}{2} qb(\frac{1}{2} qb - 2)$,
 $q \pm 1 = \frac{1}{2} b(\frac{1}{2} qb - 2) = \frac{1}{4} qb^2 - b$,

$$q = \frac{1}{4} qb^2 - b \pm 1. \quad (3.6)$$

Если $q = 2$, то $2 = \frac{1}{2} b^2 - b \pm 1$ и $1 = \frac{1}{2} b^2 - b$, $b^2 - 2b = 2$ $b(b-2) = 2$ (или $3 = \frac{1}{2} b^2 - b$, $b^2 - 2b = 6$, $b(b-2) = 6$), что невозможно, так как b и $b-2$ – нечетные числа.

Если $q = 4$, то $4 = b^2 - b \pm 1$ и $3 = b(b-1)$, (или $5 = b(b-1)$), что невозможно. Поэтому $q \geq 8$.

Из (3.6) видно, что $b \mp 1 = \frac{1}{4} qb^2 - q = \frac{qb^2 - 4q}{4} = \frac{1}{4} q(b^2 - 4) = \frac{1}{4} q \cdot r$, где $r = b^2 - 4$ – нечетное целое число. Итак, $\frac{1}{4} qr - b \pm 1 = 0$, $b = \frac{1}{4} qr \pm 1$, $r = b^2 - 4 = \frac{1}{16} q^2 r^2 \pm 2 \cdot \frac{1}{4} qr + 1 - 4 = \frac{1}{16} q^2 r^2 \pm \frac{1}{2} qr - 3$, или

$$\frac{1}{16} r^2 q^2 \pm \frac{1}{2} rq - (3+r) = 0. \quad (3.7)$$

(3.7) есть квадратное уравнение относительно q с неотрицательным корнем $q = 2^n \geq 8$. Поэтому

$$q = \frac{\mp \frac{1}{2} r + \sqrt{\frac{1}{4} r^2 + 4 \cdot \frac{1}{16} r^2 (3+r)}}{\frac{1}{8} r^2} \geq 8.$$

Откуда $\frac{\mp 1 + \sqrt{r+4}}{\frac{1}{4} r} \geq 8$, $\mp 1 + \sqrt{r+4} \geq 2r$, $\sqrt{r+4} \geq 2r \pm 1$. Это противоречивое неравенство, и слу-

чай $m = 2 \cdot k$ исключается из рассмотрения.

Предположим теперь, что $m = 2k+1$. Тогда $q^2 \mp q = p^{2k+1} - 1 = (p-1)(p^{2k} + \dots + 1)$. Во второй скобке сумма четного числа слагаемых и 1 дает нам нечетное число. Поэтому $q = 2^n$ делит $(p-1)$, т.е. $s \cdot 2^n = (p-1)$. С другой стороны, $q \mp 1 = s \cdot (p^{2k} + \dots + 1)$ и $q \mp 1 \geq p^{2k} + \dots + 1$. Итак, $p^{2k} + \dots + 1 < q \leq p-1$. Если $2k \neq 0$, то $p^{2k} < p-2$. Или $p^{2k} + \dots + p \leq q \leq p-1$ и $p^{2k} \leq p-1$. Это противоречие доказывает утверждение, что $m = 1$. Лемма доказана.

3.8. ЛЕММА. Пусть $q = p^n$, где p – простое число, n – натуральное число. Предположим, что $(q+1)(q^2 - q + 1) = r^a \cdot s^b$, где r и s – различные простые числа, a и b – натуральные числа. Тогда

- (1) $a > 0$, $b > 0$; или $q = 2$, r^a или s^b равно 3^2 ;
- (2) $3 \in \{r, s\}$, или $q = p = r^a - 1 = 2^a - 1$, $2^{2a} - 3 \cdot 2^a + 3 = s^b$;
- (3) $r = 3$, $q = 8$, $s = 19$ (или $r = 19$, $s = 3$).

Доказательство

(1) Предположим, что $b = 0$ (случай $a = 0$ аналогичен). Тогда $q^3 + 1 = r^a$. По теореме 3.2 (2) $(r^a, p^{3n}) \in \{(3^2, 2^3)\}$ и $n = 1$. Этим (1) доказано.

(2) Предположим, что $3 \notin \{r, s\}$. По лемме 3.1 (7) тогда $q+1 = r^a$, $q^2 - q + 1 = s^b$ (случай $q+1 = s^b$, $q^2 - q + 1 = r^a$ рассматривается аналогично). По теореме 3.2 (2)

$$(r^a, p^n) \in \{(3^2, 2^3); (3, 2); (r, 2^{2^k}); (2^a, p)\}. \quad (3.8)$$

1) Если $t \neq 3$ и $s \neq 3$, то $3 \mid |H|$ (если $3 \nmid |H|$, то $3 \nmid |X|$, $X \cong {}^2B_2(2^{2k+1})$ и X не имеет собственных холловых подгрупп четного порядка по теореме 3.5). По теореме 4.2 в [12] X обладает холловой $\{2, 3\}$ -подгруппой с $2 \in \{2, 3\}$ тогда и только тогда, когда $q = 2^n = 2^{2m}$ для некоторого целого m и $X \cong A_1(q)$, $B_2(q)$, ${}^2A_2(q)$, ${}^2A_3(q)$ или ${}^2A_4(q)$, $\{2, 3\} \subseteq \pi(q-1) \cup \{2\}$. Так как из условия теоремы следует, что $|X : B|$ делит $t^a \cdot s^b$, то из числового значения $|X : B|$ для указанных выше групп (смотри, например, [12, табл. 1]) имеем следующие соотношения:

$$\text{для } A_1(q) \quad |X : B| = \frac{q^2-1}{q-1} = t^\alpha \cdot s^\beta, \quad \alpha \leq a, \beta \leq b; \tag{4.1}$$

$$\text{для } B_2(q) \quad |X : B| = \frac{q^2-1}{q-1} \cdot \frac{q^4-1}{q-1} = t^\alpha \cdot s^\beta; \tag{4.2}$$

$$\text{для } {}^2A_2(q) \quad |X : B| = \frac{q^2-1}{q-1} \cdot \frac{q^3+1}{q+1} = t^\alpha \cdot s^\beta; \tag{4.3}$$

$$\text{для } {}^2A_3(q) \quad |X : B| = \frac{q^2-1}{q-1} \cdot \frac{q^3+1}{q+1} \cdot \frac{q^4-1}{q-1} = t^\alpha \cdot s^\beta; \tag{4.4}$$

$$\text{для } {}^2A_4(q) \quad |X : B| = \frac{q^2-1}{q-1} \cdot \frac{q^3+1}{q+1} \cdot \frac{q^4-1}{q-1} \cdot \frac{q^5+1}{q+1} = t^\alpha \cdot s^\beta. \tag{4.5}$$

В случае (4.1) $q+1 = t^\alpha \cdot s^\beta$, что есть в заключении теоремы.

В случае (4.2) по 2) леммы 3.6 $q = 2^{2^k}$, $(q+1)^2(q^2+1) = t^2 \cdot s$. Эти группы есть в заключении теоремы.

Случай (4.3) не может иметь места в силу леммы 3.8, так как $3 \notin \{t, s\}$. По этой же причине не могут иметь места и случаи (4.4) и (4.5).

2) Пусть теперь $3 \in \{t, s\}$. Пусть для определенности $t = 3$.

По теореме 3.5 можно считать, что все холловы $\{2, r\}$ -подгруппы из X лежат в подгруппе Бореля $B = N(P)$. Как и выше, $|X : B|$ делит $3^a \cdot s^b$.

Рассмотрим отдельно следующие 14 возможностей ($X \cong {}^2B_2(2^{2k+1})$, ${}^2G_2(3^{2k+1})$).

$$2.1) X \cong A_l(q), \quad l \geq 1, \quad |X : B| = \prod_{i=1}^l \frac{q^{i+1}-1}{q-1} = 3^\alpha \cdot s^\beta, \quad 0 \leq \alpha \leq a, \quad 0 \leq \beta \leq b.$$

Если $l \geq 2$, то $\frac{q^2-1}{q-1} \cdot \frac{q^3-1}{q-1} = (q+1)(q^2+q+1)$ делит $3^\alpha \cdot s^\beta$. Тогда по (2) леммы 3.4 $q \in \{2, 8\}$.

Если $l \geq 3$, то по 2) леммы 3.6 $q = 2$, $s = 5$, $r = 3$ (ввиду (2) леммы 3.4). $l \geq 4$, так как $\frac{q^5-1}{q-1} = 31 \in \{3, 5\}$ (ввиду (2) леммы 3.4 и 2) леммы 3.6). Итак, X может быть $A_3(2)$, $A_2(2)$, $A_2(8)$ или

$$A_1(q) \text{ с } q+1 = 3^\alpha \cdot s^\beta, \quad 1+2^n = 3^\alpha \cdot s^\beta.$$

Если $X \cong A_2(2)$, то $|\pi(X)| = 3$ и группа отпадает. Если $X \cong A_2(8)$, то $|X : B| = 3^2 \cdot 73$.

Если $X \cong A_3(2)$, то $|X : B| = \frac{q^2-1}{q-1} \cdot \frac{q^3-1}{q-1} \cdot \frac{q^4-1}{q-1} = 3^a \cdot 5^b$ и $\frac{2^3-1}{2-1} = 7$. Поэтому группа $A_3(2)$ отпадает.

$$2.2) X \cong B_l(q), X \cong C_l(q), \quad l > 1, \quad |X : B| = \prod_{i=1}^l \frac{q^{2i}-1}{q-1} = 3^\alpha \cdot s^\beta, \quad 0 \leq \alpha \leq a, \quad 0 \leq \beta \leq b.$$

Так как $l \geq 2$, то $\frac{q^4-1}{q-1}$ делит $3^\alpha \cdot s^\beta$. По лемме 3.6 тогда $q = 2, s = 5, r = 3, \alpha = 1, \beta = 1$, или $q = 2^{2^k}$,

$\alpha = 1, \beta = 1, l \geq 3$ невозможно, так как тогда $\frac{q^6-1}{q-1}$ делит $3^\alpha \cdot s^\beta$ и если $q = 2$, то $s = 7 \neq 5$, а если $q = 2^{2^k}$,

$k > 0$, то $\frac{q^6-1}{q-1} = \frac{(2^{2^k})^6-1}{2^{2^k}-1} = 3^m \cdot s^n$ для некоторых натуральных чисел m и n , что невозможно по теореме 3.2 (1) и лемме 3.8. Итак, $l = 2, q = 2, r = 3, s = 5$ или $q = 2^{2^k}, k > 0, r = q+1, s = q^2+1$. Эти группы есть в заключении теоремы.

$$2.4) X \cong D_l(q), l \geq 4, \quad |X:B| = \frac{q^l-1}{q-1} \cdot \prod_{i=1}^{l-1} \frac{q^{2i}-1}{q-1} = 3^\alpha \cdot s^\beta, \quad 0 \leq \alpha \leq a, \quad 0 \leq \beta \leq b.$$

Так как $l \geq 4$, то $l-1 \geq 3$ и эта возможность исключается, как и в случаях 2.2) и 2.3).

$$2.5) X \cong {}^2D_l(q), l \geq 4. \quad |X:B| \text{ содержит множитель } \prod_{i=1}^{l-1} \frac{q^{2i}-1}{q-1}, \text{ который делит } 3^\alpha \cdot s^\beta. \text{ Эта возможность исключается, как и в 2.4).}$$

$$2.6) X \cong E_6(q). \quad |X:B| = \frac{q^{12}-1}{q-1} \cdot \frac{q^9-1}{q-1} \cdot \frac{q^8-1}{q-1} \cdot \frac{q^6-1}{q-1} \cdot \frac{q^5-1}{q-1} \cdot \frac{q^2-1}{q-1} = 3^\alpha \cdot s^\beta. \text{ По теореме 3.2 (1)}$$

число $q^{12}-1$ имеет простой делитель z , который не делит q^m-1 для $1 \leq m < 12$. Тогда $z \in \{3, s\}$. Точно так q^9-1 имеет простой делитель t , отличный от z , который не делит q^n-1 для $1 \leq n < 9$. Ясно, что $\{t, z\} \in \{3, s\}$. Но тогда для q^8-1 нельзя найти примитивный простой делитель, так как множество $\{3, s\}$ исчерпано. Противоречие с теоремой 3.2 (1) исключает эти группы из рассмотрения.

2.7), 2.8) $X \cong E_7(q), E_8(q)$. Эти группы исключаются из рассмотрения, как и в случае 2.6).

2.9) $X \cong F_4(q)$. Эти группы исключаются, как и группы в случае 2.8), так как $\frac{(q^{12}-1)(q^8-1)(q^6-1)(q^2-1)}{(q-1)^4}$ делит $3^\alpha \cdot s^\beta$, и если даже (q^6-1) не имеет своего примитивного делителя,

отличного от примитивных делителей $(q^{12}-1), (q^8-1)$, то $q = 2, n = 6$ и $s = 7$, что невозможно, так как $\{3, s\}$ – примитивные делители чисел $(q^{12}-1)$ и (q^8-1) .

$$2.10) X \cong G_2(q), \quad |X:B| = \frac{1}{(q-1)^2} (q^6-1)(q^2-1) = 3^\alpha \cdot s^\beta. \quad q^6-1 = (q^3-1)(q^3+1), \text{ поэтому}$$

$(q^2+q+1)(q^3+1)$ делит $3^\alpha \cdot s^\beta$. По лемме 3.8 $q = 2$ или 8. Если $q = 2$, то $(2^2+2+1)(2^3+1)(2+1) = 7 \cdot 3^3$. Если $q = 8$, то $(8^2+8+1)(8^3+1)(8+1) = (64+9) \cdot 513 \cdot 9 = 73 \cdot 3^3 \cdot 171 = 73 \cdot 3^5 \cdot 19$. Это не число вида $3^\alpha \cdot s^\beta$. Поэтому $X \cong G_2(2), |X:B| = 7 \cdot 3^3$. Но $|\pi(X)| = 3$. Поэтому группа не удовлетворяет условию теоремы.

$$2.11) X \cong {}^2A_l(q^2), \quad |X:B| = \prod_{i=1}^l \frac{q^{i+1}-(-1)^{i+1}}{q-(-1)^{i+1}} = 3^\alpha \cdot s^\beta.$$

Если $l \geq 3$, то $\frac{q^2-1}{q-1} \cdot \frac{q^3+1}{q+1} \cdot \frac{q^4-1}{q-1}$ делит $3^\alpha \cdot s^\beta$. Из лемм 3.8 и 3.6 следует, что $q = 2$. Тогда

$3 \cdot \frac{9}{3} \cdot 15 = 3^2 \cdot 5$ и группа ${}^2A_3(2^2)$ удовлетворяет условию, $s = 5$.

Если $l \geq 4$, то $\frac{q^5+1}{q+1} = \frac{33}{3} = 11$ не делит $3^\alpha \cdot 5^\beta$. Поэтому $l \leq 3$. Пусть теперь $l = 2$. Тогда $(q+1)(q^2-q+1)$

делит $3^\alpha \cdot s^\beta$ и по лемме 3.8 $q = 8, 9 \cdot (64-8+1) = 9 \cdot 57 = 3^3 \cdot 19$ и группа ${}^2A_2(8^2)$ удовлетворяет условию.

2.12) $X \cong {}^3D_4(q^3)$. $|X : B| = (q+1)(q^3+1)(q^8+q^4+1) = 3^\alpha \cdot s^\beta$. Из леммы 3.8 следует, что $q = 8$, $s = 19$. Но $(8^8+8^4+1) = (16777216+4096+1) = 16781313 = 5593771 \cdot 3 = 294409 \cdot 19 \cdot 3$ и число 294409 имеет простой делитель, отличный от 19. Поэтому $|X : B| \neq 3^\alpha \cdot 19^\beta$. Группа не удовлетворяет условию.

2.13) $X \cong {}^2E_6(q^2)$. $|X : B| = \frac{q^{12}-1}{q-1} \cdot \frac{q^9+1}{q+1} \cdot \frac{q^8-1}{q-1} \cdot \frac{q^6-1}{q-1} \cdot \frac{q^5+1}{q+1} \cdot \frac{q^2-1}{q-1} = 3^\alpha \cdot s^\beta$. Эта группа исключается из рассмотрения, как и $F_4(q)$ в 2.9).

2.14) $X \cong {}^2E_7(q^2)$. $|X : B| = (q^6+1)(q^3+1)(q^2+1)(q+1) = 3^\alpha \cdot s^\beta$.

Так как $q^3+1 = (q+1)(q^2-q+1)$, то из леммы 3.8 следует, что $q = 8$, $s = 19$. Но это невозможно, так как $q^2+1 = 65 = 5 \cdot 13$ и $13 \nmid 3^\alpha \cdot 19^\beta$. Группа не удовлетворяет условию.

Теорема доказана.

ЛИТЕРАТУРА

1. Huppert B. Endliche Gruppen, I. – Berlin: Springer – Verlag, 1967. – 793 S.
2. Huppert B., Blackburn N. Finite groups, III. – Berlin: Springer – Verlag, 1982. – 454 S.
3. Горенштейн Д. Конечные простые группы. Введение в их классификацию. – М.: Мир. – 1985. – 352 с.
4. Carter R. Simple groups of Lie type. – London: J. Wiley and Sons, 1972. – 333 p.
5. Кондратьев А.С. Подгруппы конечных групп Шевалле // Успехи матем. наук. – 1986. – Т. 41, № 1. – С. 57 – 96.
6. Vdovin E.P., Revin D.O. Hall subgroups of finite groups (Препринт № 134 / Ин-т математики, Сиб. отделение РАН), 2004. – 40 с.
7. Hall Ph. Theorems like Sylow's // Proc. London Math. Soc. – 1956. – V. 6, № 2. – P. 286 – 304.
8. Чунихин С.А. Подгруппы конечных групп. – Мн.: Наука и техника, 1964. – 154 с.
9. Gross F. On a conjecture of Philip Hall // Proc. London Math. Soc. – 1986. – V. 52, № 3. – P. 464 – 494.
10. Gross F. Conjugacy of odd order Hall subgroups // Bull. London Math. Soc. – 1987. – V. 19, № 4. – P. 311 – 319.
11. Gross F. Hall subgroups of order not divisible by 3 // Rocky Mountain J. Math. – 1993. – V. 23, № 2. – P. 569 – 591.
12. Ревин Д.О. Холловы π -подгруппы конечных групп Шевалле, характеристика которых принадлежит π // Математические труды. – 1999. – Т. 2, № 1. – С. 160 – 208.
13. Ревин Д.О. Свойство D_π в одном классе конечных групп // Алгебра и логика. – 2002. – Т. 41, № 3. – С. 335 – 370.
14. Вдовин Е.П., Ревин Д.О. Холловы подгруппы нечетного порядка в конечных группах // Алгебра и логика. – 2002. – Т. 41, № 1. – С. 15 – 56.
15. Atlas of finite groups / J.H. Conway, R.T. Curtis, S.P. Norton, R.A. Parker, R.A. Wilson. – London: Clarendon Press, 1985. – 252 p.
16. Zsigmondy K. Zur Theorie der Potenzreste // Monatsh. Math. Phys. – 1892. – V. 3, № 2. – S. 265 – 284.
17. Suryanarayana D. Certain Diophantine equation // Math. Stud. – 1967 (1969). – V. 35, № 1 – 4. – P. 197 – 199.