МАТЕМАТИКА

УДК 512.542

О КОНЕЧНЫХ ГРУППАХ С КОПРОСТЫМ АВТОМОРФИЗМОМ, ИНДЕКС СТАБИЛИЗАТОРА КОТОРОГО ЕСТЬ ЧИСЛО ВИДА $p^{\alpha}q^{\beta}$

доктор физ.- мат. наук, профессор Э.М. ПАЛЬЧИК, С.Ю. БАШУН

Исследуется строение конечной группы X, допускающей автоморфизм y простого порядка r, $(|X|, r) = 1$, причем $|X : C_X(y)| = p^{\alpha}q^{\beta}$. Доказывается, что $C = C_X(y)$, где $\Pi = \{p, q\}$.

1. Введение

Используются стандартные обозначения и терминология теории конечных групп, которые можно найти в [1 – 5]. Наиболее часто встречающиеся понятия будут приведены ниже.

Если X – конечная Π-группа, A – ее Π'-группа автоморфизмов, то говорят, что A действует копростым образом на X, а $1 \neq y \in A$ называют копростым автоморфизмом группы X. $C = C_X(y)$ иногда называют стабилизатором автоморфизма y в группе X.

В [6] показано, что если $y^r = 1$, где r – простое число и $|X{:}C| = p^{\alpha}$, то $X = C \cdot O_p(X)$.

Целью настоящей работы является доказательство того, что если $|X{:}C| = p^{\alpha} \cdot q^{\beta}$, где p и q – различные простые делители порядка группы X, $\alpha \neq 0$, $\beta \neq 0$, то $X = C \cdot O_{\Pi}(X)$, где $\Pi = \{p, q\}$.

2. Обозначения и терминология

p – простое число.

$|X|$ – число различных элементов множества X.

S_p-подгруппа – силовская p-подгруппа.

$|X{:}Y|$ – индекс подгруппы Y в группе X, т.е. $|X|/|Y|$.

$|X|_p$ – порядок S_p-подгруппы X_p группы X.

Π – множество простых чисел.

Π' – дополнительное к Π множество простых чисел.

$\Pi(B)$ – множество простых делителей числа $|B|$.

Если $\Pi(B) \subseteq \Pi$, то B называют Π-группой.

$O_p(X)$ $(O_{\Pi}(X))$ – наибольшая нормальная p-подгруппа (Π-подгруппа) группы X.

$T^x = x^{-1}Tx$.

$N_K(T)$, $C_K(T)$ – соответственно нормализатор и централизатор множества T в подгруппе K из X (если $K = X$, то значок внизу условимся не писать).

$\mathrm{Aut}(B)$ – группа всех автоморфизмов группы B.

$Out(B)$ – группа всех внешних автоморфизмов группы B.

Секцией группы называют фактор-группу ее некоторой подгруппы.

K-свободной группой называют группу, у которой нет секций, изоморфных группе K.

$T \lhd X (T \lhd\lhd X)$ означает, что T есть нормальная (субнормальная) подгруппа в X.

K-группа – это группа, у которой простые неабелевы композиционные факторы являются известными простыми группами (из множеств $Chev \cup Spor \cup \{An / n \geq 5\}$).

3. Некоторые сведения о группах лиевского типа

Пусть $K = GF(q)$ – конечное поле Галуа, состоящее из $q = p^n$ элементов, где p – простое число, n – натуральное число.

Пусть L_C – конечномерная простая алгебра Ли над полем C комплексных чисел; L_K – соответствующая L_C простая алгебра Ли над K.

Известно, что любая конечномерная простая алгебра Ли над C характеризуется диаграммой Дынкина (связным графом с l вершинами) одного из видов:

$$A_l, l \geq 1;\ B_l, l \geq 2;\ \ C_l, l \geq 3;\ D_l, l \geq 4;\ G_2;\ F_4;\ E_6;\ E_7;\ E_8, \tag{3.1}$$

где значок внизу означает число вершин в диаграмме Дынкина.

В соответствии с этим простые алгебры Ли подразделяются на 9 типов. Соответственно имеется 9 семейств комплексных простых групп Ли, являющихся группами автоморфизмов этих простых алгебр Ли L_C (Картан).

Конечные аналоги этих групп (автоморфизмов L_K) построил Шевалле [7]:

$$A_l(q); B_l(q); C_l(q); D_l(q); G_2(q); F_4(q); E_6(q); E_7(q); E_8(q). \tag{3.2}$$

Их называют группами Шевалле нормального типа.

Позже Стейнбергом [8], Сузуки [9] и Ри [10, 11] построили так называемые скрученные типы конечных групп лиевского типа (${}^k X_l(q)$):

$$\begin{gathered} {}^2A_l(q), l \geq 2; {}^2D_l(q), l \geq 4; {}^2E_6(q); {}^3D_4(q); \\ {}^2B_2(q), q = 2^{2m+1}; {}^2G_2(q), q = 3^{2m+1}; {}^2F_4(q), q = 2^{2m+1}, \end{gathered} \tag{3.3}$$

где k = 2 или 3 и означает порядок симметрии соответствующей диаграммы Дынкина. Если k = 1, то $X_l(q)$ – типа (3.2).

Группы Шевалле (3.2) вместе с вариациями Стейнберга, Сузуки-Ри (3.3) образуют множество конечных групп лиевского типа (или множество конечных групп Шевалле, обозначаемое символом $Chev = \bigcup\limits_p Chev(p)$, где p – характеристика поля K).

Группа X называется квазипростой, если $X = X'$ и $X/Z(X)$ – простая неабелева группа. Тогда говорят также, что X есть накрывающая группа для группы изоморфной $X/Z(X)$. Каждая простая неабелева группа X обладает «универсальной» накрывающей группой $\hat{X}$ такой, что любая накрывающая для X есть гомоморфный образ $\hat{X}$. Тогда $Z(\hat{X})$ называют мультипликатором Шура группы X [2, теорема 3.2].

Под группой Шевалле мы будем понимать как группу с единичным центром (присоединенные версии), так и любую фактор-группу «универсальной» версии по центральной подгруппе.

Если $X \in Chev(p)$, то группа $X/Z(X)$ за исключением 8 случаев [2, теорема 2.13] является простой неабелевой группой.

4. Используемые результаты

4.1. ТЕОРЕМА [5, теорема 7.1.2]. Пусть $X \in Chev(p)$, X – простая группа, допускающая такую группу автоморфизмов, что $(|A|, |X|) = 1$. Тогда A сопряжена с некоторой подгруппой всех автоморфизмов основного поля, над которым определена группа X (то есть можно считать, что A состоит из полевых автоморфизмов группы X).

4.2. ЛЕММА [13, теорема 9-1]. Пусть $X \in Chev(p)$, X – простая группа; y – полевой автоморфизм группы X; $y^r = 1$; r – простое число; $(|X|, r) = 1$; $C = C_X(y)$. Пусть $X \cong {}^k X_l(p^n)$. Тогда $C_o = O^{p'}(C) \cong {}^k X_l(p^{n/r})$, изоморфна подгруппе из $Inndiag\ (C_o)$.

4.3. ЛЕММА [5, теорема 2.5.12]. Пусть $X \in Chev(p)$; $q = p^n, X$ – простая группа. Тогда группа $O = Outdiag\ (X)$ нетривиальна в следующих случаях:

$O \cong Z_{(l+1, q-1)}$, если $X \in A_l(q)$;

$O \cong Z_{(l+1, q+1)}$, если $X \in {}^2A_l(q)$;

$O \cong Z_{(2, q-1)}$, если $X \in \{B_l(q); C_l(q); {}^2D_l(q), l = 2m; F_7(q)\}$;

$O \cong E^2_{(2, q-1)}$, если $X \in \{D_l(q), l = 2m\}$;

$O \cong Z_{(4, q^l-1)}$, если $X \in \{D_l(q), l = 2m+1\}$;

$O \cong Z_{(4, q^l+1)}$, если $X \in \{{}^2D_l(q), l = 2m+1\}$;

$O \cong Z_{(3, q-1)}$, если $X \in \{E_6(q)\}$;

$O \cong Z_{(3, q+1)}$, если $X \in \{{}^2E_6(q)\}$.

4.4. ТЕОРЕМА [12, 14]. Пусть p – простое число и $n \geq 2$. Тогда существует простое число z, такое, что z делит $(p^n - 1)$, но z не делит $(p^m - 1)$ для $1 \leq m < n$, исключая возможности:

(1) $p = 2$, $n = 6$; или

(2) $p = 2^q - 1$ – простое число Мерсенна (в частности, q – простое число) и $n = 2$.

4.5. ТЕОРЕМА [12]. Пусть p и q – два простых числа; m и n – натуральные числа, $m \geq 1$, $n \geq 1$. Предположим, что $p^m = q^n + 1$. Тогда имеет место одна из возможностей:

(1) $q = 2, p = 3, n = 3, m = 2$;

(2) $q = 2, m = 1$, n – степень числа 2, $p = q^n + 1$ – простое число Ферма;

(3) $p = 2, n = 1, q = p^m - 1$ – простое число Мерсенна (в частности, m – простое число).

4.6. ТЕОРЕМА [13, теорема 9-2]. Пусть $X \in Chev(p)$; y – полевой автоморфизм простого порядка r группы X. Если p и r – нечетные числа, то $|X : C_X(y)|$ – нечетное число.

5. Предварительные леммы

5.1. СОГЛАШЕНИЕ. Запись $(X, y, C, r,\ p^a s^b) \in 5.1.$ всюду ниже означает, что X – конечная группа, допускающая копростой автоморфизм y простого порядка r, $C = C_X(y)$ и $|X : C| = p^a s^b$, где p и s – различные простые числа, делящие число $|X|$), $a \neq 0$, $b \neq 0$.

5.2. ЛЕММА. Пусть p и r – простые числа; l, m, n – целые числа. Предположим, что m есть делитель числа $(l+1, p^{n/r} - 1)$. Тогда $(p^{kn} - 1)/(p^{kn/r} - 1)$ не делит m для любого целого числа $k \geq 1$ и $r > 2$.

Доказательство. Предположим противное, то есть, что $(p^{kn} - 1)/(p^{kn/r} - 1)$ делит m. Но тогда $(p^{kn} - 1)/(p^{kn/r} - 1) \leq p^{n/r} - 1$. Пусть $p^{kn/r} = x$. Тогда $\dfrac{x^r - 1}{x - 1} = x^{r-1} + x^{r-2} + \ldots + x + 1 = p^{\frac{kn}{r}(r-1)} +$ $+ p^{\frac{kn}{r}(r-2)} + \ldots + p^{\frac{kn}{r}} + 1 \leq p^{n/r} - 1$. Это неравенство невозможно. Лемма доказана.

5.3. ЛЕММА. Пусть p, r, l, m, n такие же числа, как и в условии леммы 5.2, и $r < n$. Предположим, что m есть делитель числа $(l+1, p^{n/r} + 1)$. Тогда $(p^{kn} \pm 1)/(p^{kn/r} \pm 1)$ не делит m для любого целого числа $k \geq 1$ и $r > 2$.

Доказательство. Предположим, что $(p^{kn} \pm 1)/(p^{kn/r} \pm 1)$ делит m. Тогда $(p^{kn} \pm 1)/(p^{kn/r} \pm 1) \leq$ $\leq p^{n/r} + 1$. Пусть $p^{kn/r} = x$. Рассмотрим два случая. Пусть $(x^r + 1)/(x + 1) = x^{r-1} - x^{r-2} + \ldots$ $- x + 1 = p^{\frac{kn}{r}(r-1)} - p^{\frac{kn}{r}(r-2)} + \ldots - p^{\frac{kn}{r}} + 1 \leq p^{n/r} + 1$. Откуда, после сокращения на $p^{\frac{kn}{r}}$, получаем $p^{\frac{kn}{r}(r-2)} - p^{\frac{kn}{r}(r-3)} + \ldots + p^{\frac{kn}{r}} - 1 \leq p^{\frac{n}{r}(1-k)} \leq 1$. Но в левой части полученного неравенства имеется $r - 1$ слагаемых, которые образуют $(r - 1) / 2$ пар положительных слагаемых, каждое из которых имеет вид $p^{\frac{kn}{r}(r-i)} - p^{\frac{kn}{r}(r-i-1)} = p^{\frac{kn}{r}(r-i-1)}(p^{\frac{kn}{r}} - 1) > 1$ при r > 2. Получили противоречие, исключающее этот случай из рассмотрения. Во втором случае $(x^r - 1)(x - 1) = x^{r-1} + x^{r-2} + \ldots + x + 1 = p^{\frac{kn}{r}(r-1)} + \ldots$ $+ p^{\frac{kn}{r}} + 1 \leq p^{n/r} + 1$. Это, очевидно, невозможно. Лемма доказана.

5.4. ЛЕММА. Пусть $(X, y, C, r, p^a s^b) \in 5.1$; $q = p^n$, где p – простое число; $X \in Chev(p)$; X – простая группа. Тогда $X \notin A_l(q)$.

Доказательство. Предположим противное, то есть, что $X \in A_l(q)$. Тогда известно [2, с. 145], что
$|X| = \frac{1}{(l+1, p^n - 1)} \cdot p^{nl(l+1)/2}\left(p^{2n} - 1\right)\left(p^{3n} - 1\right)\ldots\left(p^{(l+1)n} - 1\right)$.

Из лемм 4.2 и 4.3 следует, что $|C| = \left|O^{p'}(C)\right| \cdot m$, где m – делитель числа $\left|OutdiagA_l(p^{n/r})\right| = (l+1, p^{n/r} - 1)$. Из условия леммы и $r > 3$ следует, что $p^{nl(l+1)/2} > p^{nl(l+1)/2r}$. Поэтому из $O^{p'}(C) \cong A_l(p^{n/r})$ и условия леммы имеем:

$$\frac{1 \cdot (l+1, p^{n/r} - 1)}{(l+1, p^n - 1) \cdot m} \cdot \frac{(p^{2n} - 1)(p^{3n} - 1)\ldots(p^{(l+1)n} - 1}{(p^{2n/r} - 1)(p^{3n/r} - 1)\ldots(p^{(l+1)n/r} - 1)} = s^b. \tag{5.1}$$

Пусть $(l+1, p^{n/r} - 1) = d, (l+1, p^n - 1) = d \cdot b$. Тогда

$$(b, d) = 1 = (b, p^{n/r} - 1), \tag{5.2}$$

ибо в противном случае $(l+1, p^{n/r} - 1) \succ d$. Тогда (5.1) можно переписать в виде:

$$\frac{1}{b} \cdot \frac{(p^{2n} - 1)}{(p^{2n/r} - 1)} \cdots \frac{(p^{(l+1)n} - 1)}{(p^{(l+1)n/r} - 1)} = m \cdot s^b. \tag{5.3}$$

По теореме 4.4 существует такой простой делитель t числа $p^{(l+1)n} - 1$, который не делит $p^i - 1$ для $i < (l + 1)n$, либо $(l + 1)n = 2$ или 6. Ввиду выражения для $|C|$ r делит n. Так как по условию $(|X|, r) = 1$, то $r \neq 2, 3$. Поэтому $(l+1) \cdot n \notin \{2,6\}$.

Рассмотрим выражение

$$\frac{p^{2n} - 1}{b \cdot (p^{2n/r} - 1)} = \frac{(p^n + 1)(p^n - 1)}{b \cdot (p^{n/r} + 1)(p^{n/r} - 1)}. \tag{5.4}$$

Так как r – простое (нечетное) число, то $(p^n + 1)/(p^{n/r} + 1)$ – целое число. Тогда ввиду (5.2) также $\frac{p^n - 1}{b \cdot (p^{n/r} - 1)}$ – целое число. На это число разделим обе части равенства (5.3.) получаем:

$$\frac{(p^{3n} - 1)\ldots(p^{(l+1)n} - 1)}{(p^{3n/r} - 1)\ldots(p^{(l+1)n/r} - 1)} = m_1 \cdot s^a, \tag{5.5}$$

где m_1 есть делитель m, а $a \leq b$.

Из леммы 5.2 следует, что s делит любой множитель в числителе левой части равенства (5.5). Поэтому, если $(l+1)n > 3n$, то $t \neq S$. Но тогда t делит m_1, m_1 делит m, m делит $p^{n/r} - 1$ и получаем противоречие с теоремой 4.4.

Пусть теперь $3n \geq (l+1)n$, $l+1 \leq 3$, $l \leq 2$.

Если $l = 2$, то (5.5) принимает вид:

$$\frac{p^{3n} - 1}{p^{3n/r} - 1} = m_1 \cdot s^a. \tag{5.6}$$

Тогда $(l+1, p^n - 1) = (3, p^n - 1) \in \{1,3\}$, $(3, p^{n/r} - 1) \in \{1,3\}$.

Рассмотрим три представляющиеся возможности:

(1) $(3, p^{n/r}-1)=1, (3, p^n-1)=1$;

(2) $(3, p^{n/r}-1)=1, (3, p^n-1)=3$;

(3) $(3, p^{n/r}-1)=3, (3, p^n-1)=3$.

Если имеет место возможность (1), то (5.1) принимает вид:

$$\frac{(p^{2n}-1)(p^{3n}-1)}{(p^{2n/r}-1)(p^{3n/r}-1)}=s^b. \tag{5.7}$$

Тогда s делит и $p^{3n}-1$ и $p^{2n}-1$. Это невозможно по теореме 4.4, если $3n \notin \{2,6\}$. Но выше было показано, что $3n \notin \{2,6\}$.

Если имеет место возможность (2), то (5.1) принимает вид:

$$\frac{(p^{2n}-1)(p^{3n}-1)}{3(p^{2n/r}-1)(p^{3n}-1)}=s^b, \quad \frac{p^{2n}-1}{p^{2n/r}-1}\cdot\frac{p^{3n}-1}{p^{3n}-1}=3\cdot s^b. \tag{5.8}$$

Так как $3n \notin \{2,6\}$, то по теореме 4.4 существует простой делитель t, который делит $p^{3n}-1$, но не делит p^i-1 для $i \prec 3n$. Ясно, что $t=s$ или 3. Если $t=$ s, то $\frac{p^{2n}-1}{p^{2n/r}-1}=3$.

Из $\frac{(p^n-1)}{(p^{n/r}-1)}\cdot\frac{(p^n+1)}{(p^{n/r}+1)}=3$ следует, что при $r \neq 1$ это невозможно. Если $t=$ 3, то $\frac{p^{2n}-1}{p^{2n/r}-1}=s^c$, $c \leq b$. Тогда s делит p^n-1 и p^n+1. Поэтому s = 2. Но тогда $p > 2$. Ввиду $r > 2$ имеем противоречие с теоремой 4.6.

Если имеет место возможность (3), то (5.1) принимает вид:

$$\frac{3}{3\cdot m}\cdot\frac{(p^{2n}-1)(p^{3n}-1)}{(p^{2n/r}-1)(p^{3n/r}-1)}=s^b, \text{ где } m=1 \text{ или } 3. \tag{5.9}$$

Если $m=1$, то (5.9) совпадает с (5.7). Если m = 3, то (5.9) совпадает с (5.8). Эти случаи исключены.

Пусть теперь $l=1$. Тогда $(l+1, p^{n/r}-1)\in\{1,2\}$, $(l+1, p^n-1)\in\{1,2\}$, а (5.1) принимает вид (5.4) с $b\in\{1,2\}$. (Это следует из (5.1) при рассмотрении трех возможных случаев: (1) $(l+1, p^{n/r}-1)=1$, $(l+1, p^n-1)=1$; (2) $(l+1, p^{n/r}-1)=1, (l+1, p^n-1)=2$; (3) $(l+1, p^{n/r}-1)=2, (l+1, p^n-1)=2$, m = 1 или 2).

Рассмотрим случай, когда в (5.4) $b=1$. Тогда $\frac{(p^n+1)(p^n-1)}{(p^{n/r}+1)(p^{n/r}-1)}=s^b$. Тогда s делит p^n+1 и p^n-1. Поэтому $s=2$, $p>2$ и имеем противоречие с теоремой 4.6.

Пусть теперь $b=2$ в (5.4). Тогда

$$\frac{(p^n+1)(p^n-1)}{(p^{n/r}+1)(p^{n/r}-1)}=2\cdot s^b. \tag{5.10}$$

Если s делит p^n+1 и p^n-1, то опять $s=2$, $p>2$ и имеем противоречие с теоремой 4.6.

Поэтому пусть s делит только p^n+1. Тогда $\frac{p^n-1}{p^{n/r}-1}=2, p^n-1=2p^{n/r}-2$. Тогда $p^n-2p^{n/r}=-1$, откуда $p^n< 2p^{n/r}$, $p^{n-\frac{n}{r}}<2$, $p^{\frac{nr-n}{r}}=p^{\frac{n(r-1)}{r}}<2$. Это невозможно при $r>3$ и r, делящем n.

Пусть теперь s делит только p^n-1. Тогда $\frac{p^n+1}{p^{n/r}+1}=2, p^n+1=2p^{n/r}+2, p^n-2p^{n/r}=1$, $p^{n/r}(p^{n-\frac{n}{r}}-2)=1$. Откуда $p^{\frac{n(r-1)}{r}}-2<1$, $p^{\frac{n(r-1)}{r}}<3$. Это невозможно при $p>1$, $r>3$, делящем n.

Лемма доказана.

5.5. ЛЕММА. Пусть $(X, y, C, r, p^a s^b) \in 5.1$, $q=p^n$, где p – простое число, X – простая группа. Тогда $X \notin {}^2A_l(q)$.

Доказательство. Предположим, что $X \in {}^2A_l(q)$.

Тогда [2, с. 145], $|X|=\frac{1}{(l+1,p^n+1)}\cdot p^{\frac{nl(l+1)}{2}}(p^{2n}-1)(p^{3n}+1)\ldots(p^{(l+1)n}-(-1)^{l+1})$.

Из лемм 4.2 и 4.3 тогда следует, что $|C|=|O^{p'}(C)|\cdot m$, где m есть делитель числа $|Outdiag({}^2A_l(p^{n/r}))|=(l+1,p^{n/r}+1), O^{p'}(C)\cong {}^2A_l(p^{n/r})$. Так как 6 делит $|X|$, то $r>3$, и r делит n. Так как силовская p-подгруппа из $O^{p'}(C)$ имеет порядок $p^{\frac{nl(l+1)}{2r}}<p^{\frac{nl(l+1)}{2}}$, то из условия леммы получаем, что

$$\frac{l+1,p^{n/r}+1}{m(l+1,p^n+1)}\cdot\frac{(p^{2n}-1)}{(p^{2n/r}-1)}\cdot\frac{(p^{3n}+1)}{(p^{3n/r}+1)}\cdots\frac{(p^{(l+1)n}-(-1)^{l+1})}{(p^{(l+1)n/r}-(-1)^{l+1})}=s^b. \tag{5.11}$$

Пусть $(l+1,p^{n/r}+1)=d,(l+1,p^n+1)=db,(b,p^{n/r}+1)=(b,d)=1$. Поэтому (5.11) можно переписать в виде:

$$\frac{1}{b}\cdot\frac{(p^{2n}-1)}{(p^{2n/r}-1)}\cdot\frac{(p^{3n}+1)}{(p^{3n/r}+1)}\cdots\frac{(p^{(l+1)n}-(-1)^{l+1})}{(p^{(l+1)n/r}-(-1)^{l+1})}=m\cdot s^b. \tag{5.12}$$

Число $\frac{p^{2n}-1}{b\cdot(p^{n/r}-1)}=\frac{(p^n-1)(p^n+1)}{b\cdot(p^{n/r}-1)(p^{n/r}+1)}$ является целым числом ввиду $(b,d)=1$ и $r>3$. Поэтому, после сокращения обеих частей (5.12) на это число, получаем:

$$\frac{(p^{3n}+1)}{(p^{3n/r}+1)}\cdot\frac{(p^{4n}-1)}{(p^{4n/r}-1)}\cdots\frac{(p^{(l+1)n}-(-1)^{l+1})}{(p^{(l+1)n/r}-(-1)^{l+1})}=m_1\cdot s^a, a\le b. \tag{5.13}$$

В силу леммы 5.3 $a\neq 0$, так как $l\ge 2$. Из лемм 5.2 и 5.3 следует, что s делит любой множитель в числителе левой части выражения (5.13).

Предположим, что $l\ge 5$. Тогда в числителе левой части (5.13) имеются множители $p^{4n}-1$ и $p^{6n}-1$. По теореме 4.4 существует такой простой делитель t числа $p^{6n}-1$, который не делит p^i-1 для $i<6n$, либо $6n\in\{2,6\}$. Но, если $6n\in\{2,6\}$, то $n=3$ или 1, что невозможно для полевого автоморфизма y порядка r поля Галуа порядка p^3 или p ввиду $r>3$. Поэтому t существует и по предыдущему замечанию, что s делит и $p^{4n}-1$, $t\neq s$. Тогда из (5.13) следует, что t делит m_1, которое делит $p^{n/r}+1$, так как $\frac{p^{6n}-1}{p^{6n/r}-1}$ есть целое число, делящее $m_1\cdot s^a$ и $t\neq s$. Кроме того, $p^{6n}-1 = (p^{3n}+1)(p^{3n}-1)$ и поэтому (по теореме 4.4) t делит $p^{3n}+1$. Тогда t делит разность $(p^{3n}+1)-(p^{n/r}+1)=p^{3n}-p^{n/r}=p^{n/r}(p^{\frac{n(3r-1)}{r}}-1)$. Но тогда $\frac{n(3r-1)}{r}=6n$ по теореме 4.4. Тогда $3r-1=6r$, что невозможно.

Пусть теперь $l < 5$ ($l = 2, 3, 4$). Если $l = 4$, то $l + 1 = 5$ и $(5, p^{n/r} + 1) \in \{5,1\}, (5, p^n + 1) \in \{5,1\}$.

Пусть сначала $(5, p^{n/r} + 1) = 5$. Тогда и $(5, p^n + 1) = 5$, $m = 5$ или 1. Если $m = 5$, то (5.11) принимает вид:

$$\frac{p^{2n}-1}{p^{2n/r}-1} \cdot \frac{p^{3n}+1}{p^{3n/r}+1} \cdot \frac{p^{4n}-1}{p^{4n/r}-1} \cdot \frac{p^{5n}+1}{p^{5n/r}+1} = 5 \cdot s^b. \tag{5.14}$$

По теореме 4.4 существует простой делитель t, который делит $p^{4n} - 1$, но не делит $p^i - 1$ для $i < 4n$, так как $4n \notin$ (5.6). Так как 5 делит $p^n + 1$, то 5 делит $p^{2n} - 1$. Поэтому $t \neq 5$. Значит, $t = s$. Но тогда $\frac{p^{2n}-1}{p^{2n/r}-1} = 5$, s делит $p^{5n} + 1$ и $p^{3n} + 1$. Значит, t делит их разность $p^{5n} - p^{3n} = p^{3n}(p^{2n} - 1)$, что противоречит теореме 4.4.

Если $m = 1$, то (5.11) принимает вид:

$$\frac{p^{2n}-1}{p^{2n/r}-1} \cdot \frac{p^{3n}+1}{p^{3n/r}+1} \cdot \frac{p^{4n}-1}{p^{4n/r}-1} \cdot \frac{p^{5n}+1}{p^{5n/r}+1} = s^b. \tag{5.15}$$

(5.15) невозможно по теореме 4.4.

Пусть теперь $(5, p^{n/r} + 1) = 1$, $(5, p^n + 1) = 5$, $m = 1$. Тогда (5.11) принимает вид (5.14), что исключено выше. Если же $(5, p^{n/r} + 1) = 1$, $(5, p^n + 1) = 1$, $m = 1$, то (5.11) принимает вид (5.15) и это также исключено выше.

Если $l = 3$, то $l + 1 = 4$ и $(4, p^{n/r} + 1) \in \{1, 2, 4\}$, $(4, p^n + 1) \in \{1, 2, 4\}$, $m \in \{1, 2, 4\}$.

Пусть сначала $(4, p^{n/r} + 1) = 4$. Тогда $(4, p^n + 1) = 4$, $m \in \{1, 2, 4\}$.

Если $m = 1$, то (5.11) принимает вид:

$$\frac{p^{2n}-1}{p^{2n/r}-1} \cdot \frac{p^{3n}+1}{p^{3n/r}+1} \cdot \frac{p^{4n}-1}{p^{4n/r}-1} = s^b. \tag{5.16}$$

Но по теореме 4.4, ввиду $4n \notin \{2, 6\}$ это невозможно.

Если $m \in \{2, 4\}$, то (5.11) принимает вид:

$$\frac{p^{2n}-1}{p^{2n/r}-1} \cdot \frac{p^{3n}+1}{p^{3n/r}+1} \cdot \frac{p^{4n}-1}{p^{4n/r}-1} = m \cdot s^b, \quad m \in \{2, 4\}. \tag{5.17}$$

По теореме 4.4 ввиду $4n \notin \{2, 6\}$ существует такой простой делитель t числа $p^{4n} - 1$, который не делит $p^i - 1$, $i < 4n$. Из (5.17) следует, что $t \in \{2, s\}$. Так как $(4, p^n + 1) = 4$, то $p^{2n} - 1$ делится на 4. Значит, $t = s$. Но тогда $(p^{2n} - 1)/(p^{2n/r} - 1) \in \{2, 4\}$. Откуда $p^{2n} - 1 = 2p^{2n/r} - 2$ или $p^{2n} - 1 = 4p^{2n/r} - 4$. Тогда $p^{2n} - 2p^{2n/r} = -1$ или $p^{2n} - 4p^{2n/r} = -3$. Откуда $p^{2n/r}(p^{\frac{2n(r-1)}{r}} - 2) = -1$ или $p^{2n/r}(p^{\frac{2n(r-1)}{r}} - 4) = -3$. Это невозможно, так как r делит n и $r > 3$.

Пусть далее $(4, p^{n/r} + 1) = 2$, $(4, p^n + 1) = 2$ или 4, $m = 1$ или 2.

Если $(4, p^{n/r} + 1) = 2$, $(4, p^n + 1) = 2$, то (5.11) принимает вид:

$$\frac{p^{2n}-1}{p^{2n/r}-1} \cdot \frac{p^{3n}+1}{p^{3n/r}+1} \cdot \frac{p^{4n}-1}{p^{4n/r}-1} = m \cdot s^b, \quad m \in \{1, 2\}. \tag{5.18}$$

Если в (5.18) $m = 1$, то имеем противоречие с теоремой 4.4 ввиду $4n \notin \{2, 6\}$ и леммы 5.3.

Поэтому пусть в (5.18) $m = 2$. Так как $(4, p^n + 1) = 2$, то 2 делит $p^{2n} - 1 = (p^n + 1)(p^n - 1)$.
По теореме 4.4 существует простой делитель t, который делит $p^{4n} - 1$, но не делит $p^i - 1$ для $i < 4n$. Поэтому из (5.18) следует, что $t = s$, $\frac{p^{2n} - 1}{p^{2n/r} - 1} = 2$. Этот случай исключен из рассмотрения в рассуждениях после (5.17).

Если $(4, p^{n/r} + 1) = 2$, $(4, p^n + 1) = 4$, то (5.11) принимает вид:

$$\frac{p^{2n} - 1}{p^{2n/r} - 1} \cdot \frac{p^{3n} + 1}{p^{3n/r} + 1} \cdot \frac{p^{4n} - 1}{p^{4n/r} - 1} = m \cdot 2 \cdot s^b, \ m \in \{1, 2\}. \tag{5.19}$$

Если в (5.19) $m = 1$, то (5.19) совпадает с (5.18) при $m = 2$ и этот случай исключен выше.
Поэтому пусть в (5.19) $m = 2$. Тогда (5.19) совпадает с (5.17) с $m = 4$ и этот случай также исключен из рассмотрения выше.

Пусть теперь $(4, p^{n/r} + 1) = 1$. Тогда и $m = 1$. $(4, p^n + 1) \in \{1, 2, 4\}$.

Тогда (5.11) принимает вид (5.16), если $(4, p^n + 1) = 1$, вид (5.17) с $m = 2$, если $(4, p^n + 1) = 2$ и вид (5.17) с $m = 4$, если $(4, p^n + 1) = 4$. Все эти возможности исключены из рассмотрения выше. Этим лемма полностью доказана.

5.6. ЛЕММА. Пусть $(X, y, C, r, s^b \cdot p^a) \in 5.1$, $q = p^n$, p – простое число, X – простая неабелева группа. Тогда $X \notin B_l(q)$.

Доказательство. Предположим, что $X \in B_l(q)$. Тогда [2, с. 145]:

$$|X| = \frac{1}{(2, p^n - 1)} \cdot (p^n)^{l^2} \cdot (p^{2n} - 1)(p^{4n} - 1)\ldots(p^{2nl} - 1), l \geq 2.$$

Из лемм 4.2 и 4.3 тогда следует, что $|C| = |O^{p'}(C)| \cdot m$, где m есть делитель числа $(2, p^{n/r} - 1)$,

$$|C| = \frac{m}{(2, p^{n/r} - 1)} \cdot (p^{n/r})^{l^2} (p^{2n/r} - 1)(p^{4n/r} - 1)\ldots(p^{2nl/r} - 1).$$

Так как $(|X|, r)) = 1$, то $r > 3$, поэтому $p^{nl^2} > p^{nl^2/r}$. Поэтому

$$|X : C| = \frac{(2, p^{n/r} - 1)}{m \cdot (2, p^n - 1)} \cdot \frac{(p^{2n} - 1)}{(p^{2n/r} - 1)} \ldots \frac{(p^{2nl} - 1)}{(p^{2nl/r} - 1)} = s^b. \tag{5.20}$$

Тогда

$$\frac{(p^{2n} - 1)}{(p^{2n/r} - 1)} \cdot \frac{(p^{4n} - 1)}{(p^{4n/r} - 1)} \ldots \frac{(p^{2nl} - 1)}{(p^{2nl/r} - 1)} = m \cdot s^b, \text{ где m = 1 или 2.} \tag{5.21}$$

Так как $l \geq 2$, то в левой части (5.21) имеется, по крайней мере, 2 множителя. По теореме 4.4 существует такой простой делитель t числа $p^{2nl} - 1$, который не делит $p^i - 1$ для $i < 2nl$, либо $2nl \in \{2, 6\}$. Так как $r > 3$ и r делит n ввиду выражения для $|C|$, то $2nl \notin \{2, 6\}$. Поэтому t не делит $p^{2n} - 1$. Если $t = s$, то из (5.21) следует, что $\frac{p^{2n} - 1}{p^{2n/r} - 1} = 2$ ($\frac{p^{2n} - 1}{p^{2n/r} - 1} \neq 1$). Это, очевидно, невозможно.

Если $t \neq s$, то $t = 2$ ввиду (5.21). Но тогда $\frac{p^{2nl} - 1}{p^{2nl/r} - 1} = 2$, что также невозможно. Лемма доказана.

5.7. ЛЕММА. Пусть $(X, y, C, r, s^b \cdot p^a) \in 5.1$, $q = p^n$, p – простое число, X – простая группа. Тогда $X \notin {}^2B_2(q)$.

Доказательство. Предположим, что $X \in {}^2B_2(q)$, $p = 2$. Тогда по теореме 9-1 из [13] имеем:

$$|X| = p^{2n}(p^n - 1)(p^{2n} + 1), \quad |C| = |O^{p'}(C)| = p^{2n/r}(p^{n/r} - 1)(p^{2n/r} + 1), \; r > 2.$$

Поэтому

$$\frac{2^n - 1}{2^{n/r} - 1} \cdot \frac{2^{2n} + 1}{2^{2n/r} + 1} = s^b. \tag{5.22}$$

Тогда s делит $2^n - 1$ и $2^{2n} + 1$. Поэтому s делит их сумму $2^{2n} + 2^n = 2^n(2^n + 1)$. Тогда s делит $2^n + 1$ и $(2^n + 1) + (2^n - 1) = 2^{n+1}$, что противоречит тому, что $s > 2$. Лемма доказана.

5.8. ЛЕММА. Пусть $(X, y, C, r, s^b \cdot p^a) \in 5.1$. Тогда $X \notin C_l(q)$, $l \geq 3$, $q = p^n$.

Доказательство. Известно [2, с. 145], что

$$|X| = \frac{1}{(2, p^n - 1)} \cdot p^{nl^2} \cdot (p^{2n} - 1)(p^{4n} - 1)\ldots(p^{2nl} - 1).$$

Поэтому лемма доказывается, как и лемма 5.6. Лемма доказана.

5.9. ЛЕММА. Пусть $(X, y, C, r, p^a \cdot s^b) \in 5.1$, $q = p^n$, где p – простое число, $X \in Chev(p)$, X – простая группа. Тогда $X \notin D_l(q)$, $l \geq 4$.

Доказательство. Известно [2, с. 145], что если $X \in D_l(q)$, то

$$|X| = \frac{1}{(4, p^{nl} - 1)} \cdot p^{nl(l-1)}(p^{nl} - 1)(p^{2n} - 1)(p^{4n} - 1)\ldots(p^{2n(l-1)} - 1).$$

По лемме 4.2 тогда $|C| = |O^{p'}(C)| \cdot m$, где m есть делитель числа $(4, p^{nl/r} - 1)$ ввиду леммы 4.3. Таким образом, $m \in \{1, 2, 4\}$. Ввиду r > 3 $p^{nl(l-1)} > p^{nl(l-1)/r}$. Поэтому условие леммы дает нам, что |X : C| есть число вида:

$$\frac{(4, p^{nl/r} - 1)}{m \cdot (4, p^{nl} - 1)} \cdot \frac{p^{nl} - 1}{p^{nl/r} - 1} \cdot \frac{p^{2n} - 1}{p^{2n/r} - 1} \cdots \frac{p^{2n(l-1)} - 1}{p^{2n(l-1)/r} - 1} = s^b. \tag{5.23}$$

Пусть сначала $(4, p^{nl/r} - 1) = 4$. Тогда и $(4, p^{nl} - 1) = 4$, $m \in \{1, 2, 4\}$. Тогда (5.23) можно переписать в виде

$$\frac{p^{nl} - 1}{p^{nl/r} - 1} \cdot \frac{p^{2n} - 1}{p^{2n/r} - 1} \cdots \frac{p^{2n(l-1)} - 1}{p^{2n(l-1)/r} - 1} = m \cdot s^b, \; m \in \{1, 2, 4\}. \tag{5.24}$$

Если $m = 1$, то имеем противоречие с теоремой 4.4 и леммой 5.2, так как $2n(l - 1) \notin \{2, 6\}$ ввиду того, что $r > 3$ делит n (так как $< y >$ есть подгруппа циклической группы порядка n). Пусть теперь $m \in \{2, 4\}$. Так как m делит $p^{nl/r} - 1$, то m делит и $p^{nl} - 1$. По теореме 4.4 существует простой делитель t, который делит $p^{2n(l-1)} - 1$, но не делит $p^i - 1$ для $i < 2n(l - 1)$. Так как $nl < 2n(l - 1)$, то из (5.24) следует, что $t = s$. Из $l - 1 \geq 3$ следует, что в левой части (5.24) не менее четырех сомножителей. Поэтому из (5.24) следует, что s делит, по крайней мере, два из них (ввиду $m = 2$ или $2 \cdot 2$). Опять имеем противоречие с теоремой 4.4.

Пусть теперь $(4, p^{nl/r} - 1) = 2$. Тогда $(4, p^{nl} - 1) \in \{2, 4\}$, $m \in \{1, 2\}$. Если $(4, p^{nl} - 1) = 2$, $m = 1$, то имеем случай (5.24) с $m = 1$, который исключен. Если $m = 2$, то имеем случай (5.24) с $m = 2$, который также исключается. Если $(4, p^{nl} - 1) = 4$, то при $m = 1$ имеем случай (5.24) с $m = 2$, который исключен. Если $m = 2$, то имеем случай (5.24) с $m = 4$, который также исключается, как и выше.

Пусть теперь $(4, p^{nl/r}) = 1$, $(4, p^{nl} - 1) \in \{1, 2, 4\}$, $m = 1$. Ясно, что тогда из (5.23) следует аналог (5.24), что исключено. Лемма доказана.

5.10. ЛЕММА. Пусть $(X, y, C, r, p^a \cdot s^b) \in 5.1$. Тогда $X \notin {}^2D_l(q)$, где $q = p^n$, $l \geq 4$, p – простое число.

Доказательство. Если $X \in {}^2D_l(q)$, то [2, с. 145]:

$$|X| = \frac{1}{(4, p^{nl}+1)} \cdot p^{nl(l-1)} \cdot (p^{nl}+1)(p^{2n}-1)(p^{4n}-1)\ldots(p^{2n(l-1)}-1).$$

Из лемм 4.2 и 4.3 тогда следует, что $|C| = |O^{p'}(C)| \cdot m$, где m есть делитель числа $(2, p^n - 1)$ или $(4, p^{nl}+1)$. Поэтому $m \in \{1, 2, 4\}$.

Из условия леммы следует, что $|X : C|$ есть число вида:

$$\frac{(4, p^{nl/r}+1)}{m \cdot (4, p^{nl}+1)} \cdot \frac{p^{nl(l-1)}}{p^{nl(l-1)/r}} \cdot \frac{p^{2n}-1}{p^{2n/r}-1} \cdot \frac{p^{4n}-1}{p^{4n/r}-1} \cdots \frac{p^{2n(l-1)}-1}{p^{2n(l-1)/r}-1} \cdot \frac{p^{nl}+1}{p^{nl/r}+1} = p^a \cdot s^b. \qquad (5.25)$$

Из $r > 3$ следует, что $\dfrac{p^{nl(l-1)}}{p^{nl(l-1)/r}} = p^a$. Поэтому (5.25) можно переписать в виде:

$$\frac{(4, p^{nl/r}+1)}{(4, p^{nl}+1)} \cdot \frac{p^{nl}+1}{p^{nl/r}+1} \cdot \frac{p^{2n}-1}{p^{2n/r}-1} \cdot \frac{p^{4n}-1}{p^{4n/r}-1} \cdots \frac{p^{2n(l-1)}-1}{p^{2n(l-1)/r}-1} = m \cdot s^b,\ m \in \{1, 2, 4\}. \qquad (5.26)$$

Ясно, что $\dfrac{(4, p^{nl}+1)}{(4, p^{nl/r}+1)} \in \{1, 2, 4\}$. Поэтому (5.26) можно переписать в виде:

$$\frac{p^{nl}+1}{p^{nl/r}+1} \cdot \frac{p^{2n}-1}{p^{2n/r}-1} \cdots \frac{p^{2n(l-1)}-1}{p^{2n(l-1)/r}-1} = 2^c \cdot s^b,\ c \leq 4. \qquad (5.27)$$

Ясно, что $2n(l-1) \notin \{2,6\}$ ввиду $l - 1 \geq 3$ и того, что $r > 3$ делит n. Поэтому из теоремы 4.4 следует, что существует простой делитель t числа $p^{2n(l-1)} - 1$, который не делит $p^i - 1$ для $i < 2n(l-1)$.

Если $t = s$, то s не делит $p^{2n(l-2)} - 1$ и тогда $\dfrac{p^{2n(l-2)}-1}{p^{2n(l-2)/r}-1} = 2^e$, $\dfrac{p^{2n(l-2)}-1}{p^{2n(l-2)/r}-1} = 2^f$, $\dfrac{p^{2n(l-3)}-1}{p^{2n(l-3)/r}-1} = 2^k$, $e + f + k \leq c \leq 4$.

В частности, $p > 2$. Тогда и $\dfrac{p^{nl}+1}{p^{nl/r}+1} = 2^h \neq 1$. Поэтому $e + f + k + h \leq c \leq 4$ и $h = 1$. Тогда

$$p^{nl}+1 = 2p^{nl/r}+2,\ p^{nl} - 2p^{nl/r} = 1,\ p^{nl/r}(p^{nl - \frac{nl}{r}} - 2) = 1.$$

Это невозможное равенство ввиду $nl > \dfrac{nl}{r}$ и $r > 3$. Лемма доказана.

5.11. ЛЕММА. Пусть $(X, y, C, r, p^a \cdot s^b) \in 5.1$, $q = p^n$, p – простое число. Тогда $X \notin G_2(q)$.

Доказательство. Если $X \in G_2(q)$, то [2, с. 145]:

$$|X| = p^{6n}(p^{2n}-1)(p^{6n}-1),\ |C| = |O^{p'}(C)| = p^{6n/r}(p^{2n/r}-1)(p^{6n/r}-1)$$

по теореме 9-1 (1) (с) в [13].

По условию (ввиду $r > 3$):

$$\frac{p^{2n}-1}{p^{2n/r}-1} \cdot \frac{p^{6n}-1}{p^{6n/r}-1} = s^b. \qquad (5.28)$$

Так как $r > 3$ делит n, то $6n \notin \{2, 6\}$. По теореме 4.4 существует простой делитель t, который делит $p^{6n}-1$ и не делит p^i-1 для $i < 6n$. Из (5.28) следует, что $t \neq s$. Но тогда t делит $|C|$. Противоречие с выбором t по теореме 4.4 доказывает лемму.

5.12. ЛЕММА. Пусть $(X, y, C, r, p^a \cdot s^b) \in 5.1$, $q = p^n$, p – простое число. Тогда $X \notin {}^2G_2(q)$.

Доказательство. $p = 3$. Известно [2, с. 145], что

$$|X| = p^{3n}(p^n-1)(p^{3n}+1),\quad |C| = |O^{p'}(C)| = p^{3n/r}(p^{n/r}-1)(p^{3n/r}+1)$$

по теореме 9-1 из [13].

По условию

$$\frac{p^n-1}{p^{n/r}-1}\cdot\frac{p^{3n}+1}{p^{3n/r}+1} = s^b. \tag{5.29}$$

Из (5.29) следует, что s делит p^n-1 и $p^{3n}+1$. Поэтому s делит $p^{3n}+p^n = p^n(p^{2n}+1)$, то есть s делит $p^{2n}+1$. Тогда s делит $(p^{2n}+1)+(p^n-1) = p^n(p^n+1)$, то есть s делит p^n+1. Тогда s делит $(p^n+1)-(p^n-1) = 2$, то есть $s = 2$. Но $p = 3 > 2$ и по теореме 9-2 (5) из [13] $s > 2$. Это противоречие показывает, что $X \notin {}^2G_2(q)$ и лемма доказана.

5.13. ЛЕММА. Пусть $(X, y, C, r, p^a \cdot s^b) \in 5.1$, $q = p^n$, где p – простое число. Тогда $X \notin \{F_4(q)\}$.

Доказательство. Если $X \in \{F_4(q)\}$, то известно [2, с. 145], что

$$|X| = p^{24n}(p^{2n}-1)(p^{6n}-1)(p^{8n}-1)(p^{12n}-1),$$

$$|C| = |O^{p'}(C)| = p^{24n/r}(p^{2n/r}-1)(p^{6n/r}-1)(p^{8n/r}-1)(p^{12n/r}-1)$$

по теореме (9-1) в [13] и $|X : C| = p^a \cdot s^b$ влечет

$$\frac{p^{2n}-1}{p^{2n/r}-1}\cdot\frac{p^{6n}-1}{p^{6n/r}-1}\cdot\frac{p^{8n}-1}{p^{8n/r}-1}\cdot\frac{p^{12n}-1}{p^{12n/r}-1} = s^b. \tag{5.30}$$

$12n \notin \{2, 6\}$. Поэтому по теореме 4.4 существует простой делитель t, который делит $p^{12n}-1$, но не делит p^i-1, $i < 12n$. Из (5.29) следует, что $t \neq s$. Но тогда t делит $|C|$, что опять противоречит выбору t по теореме 4.4. Лемма доказана.

5.14. ЛЕММА. Пусть $(X, y, C, r, p^a \cdot s^b) \in 5.1$, $q = p^n$, p – простое число. Тогда $X \notin \{{}^2F_4(q)\}$.

Доказательство. Если $X \in {}^2F_4(q)$, то известно [2, с. 145], что $p = 2$,

$$|X| = p^{12n}(p^n-1)(p^{3n}+1)(p^{4n}-1)(p^{6n}+1),$$

$$|C| = |O^{p'}(C)| = p^{12n/r}(p^{n/r}-1)(p^{3n/r}+1)(p^{4n/r}-1)(p^{6n/r}+1)$$

по теореме 9-1 в [13] и из условия следует, что

$$\frac{p^n-1}{p^{n/r}-1}\cdot\frac{p^{3n}+1}{p^{3n/r}+1}\cdot\frac{p^{4n}-1}{p^{4n/r}-1}\cdot\frac{p^{6n}+1}{p^{6n/r}+1} = s^b. \tag{5.31}$$

Но тогда из (5.30) следует, что s делит $p^n-1, p^{3n}+1$ и $p^{4n}-1$. Поэтому s делит $p^{4n}+p^{3n} = p^{3n}(p^n+1)$. Тогда s делит $(p^n+1)-(p^n-1) = 2$. То есть $s = 2$. Это невозможно, так как $p = 2$. Лемма доказана.

5.15. ЛЕММА. Пусть $(X, y, C, r, p^a \cdot s^b) \in 5.1$, p – простое число. Тогда $X \notin \{E_6(q)\}$.

Доказательство. Если $X \in \{E_6(q)\}$, то известно [2, с. 145], что

$$|X| = \frac{1}{(3, p^n - 1)} p^{36n}(p^{2n} - 1)(p^{5n} - 1)(p^{6n} - 1)(p^{8n} - 1)(p^{9n} - 1)(p^{12n} - 1),$$

и по теореме 9-1 в [13]:

$$|C| = |O^{p'}(C)| \cdot m = \frac{m}{(3, p^{n/r} - 1)} \cdot p^{36n/r}(p^{2n/r} - 1)(p^{5n/r} - 1)(p^{6n/r} - 1)(p^{8n/r} - 1)(p^{9n/r} - 1)(p^{12n/r} - 1)$$

где m делит $(3, p^{n/r} - 1)$, т.е. $m = 1$ или 3, $r > 3$.

По условию

$$\frac{(3, p^{n/r})}{m \cdot (3, p^n - 1)} \cdot \frac{p^{2n} - 1}{p^{2n/r} - 1} \cdot \frac{p^{5n} - 1}{p^{5n/r} - 1} \cdot \frac{p^{6n} - 1}{p^{6n/r} - 1} \cdot \frac{p^{8n} - 1}{p^{8n/r} - 1} \cdot \frac{p^{9n} - 1}{p^{9n/r} - 1} \cdot \frac{p^{12n} - 1}{p^{12n/r} - 1} = s^b. \quad (5.32)$$

Из теоремы 4.4 следует, что существует простой делитель t числа $p^{12n} - 1$ такой, что t не делит $p^i - 1$ для $i < 12n$ ($12n \notin \{2, 6\}$). Из (5.31) следует, что $t \neq s$ (s и t не делят числа $\frac{(3, p^{n/r} - 1)}{m(3, p^n - 1)}$, которые могут принимать только значения 1 и $\frac{1}{3}$). Но тогда t должно делить $|C|$, что ввиду $r > 3$ противоречит теореме 4.4. Лемма доказана.

5.16. ЛЕММА. Пусть $(X, y, C, r, p^a \cdot s^b) \in 5.1$, p – простое число, $q = p^n$. Тогда $X \notin \{{}^2E_6(q)\}$.

Доказательство. Если $X \in \{{}^2E_6(q)\}$, то известно [2, с. 145; 13, теорема 9-1, леммы 4.2, 4.3], что

$$|X : C| = \frac{(3, p^{n/r} + 1)}{m \cdot (3, p^n + 1)} \cdot \frac{p^{36n}}{p^{36n/r}} \cdot \frac{p^{2n} - 1}{p^{2n/r} - 1} \cdot \frac{p^{5n} + 1}{p^{5n/r} + 1} \cdot \frac{p^{6n} - 1}{p^{6n/r} - 1} \cdot$$

$$\cdot \frac{p^{8n} - 1}{p^{8n/r} - 1} \cdot \frac{p^{9n} + 1}{p^{9n/r} + 1} \cdot \frac{p^{12n} - 1}{p^{12n/r} - 1} = p^a \cdot s^b, \quad (5.33)$$

где m делит $(3, p^{n/r} + 1)$. Очевидно $\frac{p^{36n}}{p^{36n/r}} = p^a$. Ясно, что $\frac{(3, p^{n/r} + 1)}{m \cdot (3, p^n + 1)} \in \{1, 1/3\}$. Поэтому $s \neq 3$ в (5.33) ввиду теоремы 4.4 и $12n \notin \{2, 6\}$. Поэтому s делит все множители числителя левой части (5.33) вида $p^i \pm 1$. Поэтому s делит $(p^{9n} + 1) + (p^{8n} - 1) = p^{8n}(p^n + 1)$ и $\frac{p^{2n} - 1}{p^{2n/r} - 1} = \frac{(p^n - 1)(p^n + 1)}{(p^{n/r} - 1)(p^{n/r} + 1)}$.

В частности, s делит $\frac{p^n - 1}{p^{n/r} - 1}$ и $p^n - 1$. Но тогда s делит $p^n + 1 + p^n - 1 = 2p^n$, то есть $s = 2$. Ввиду $s \neq p$ $|X : C|$ должно быть нечетным числом по теореме 4.6. Поэтому $s \neq 2$. Противоречие доказывает лемму.

5.17. ЛЕММА. Пусть $(X, y, C, r, p^a \cdot s^b) \in 5.1$, p – простое число, $q = p^n$. Тогда $X \notin \{E_7(q)\}$.

Доказательство. Если $X \in \{E_7(q)\}$, то из лемм 4.1, 4.2 и [2, с. 145] следует, что

$$|X| = \frac{1}{(2, p^n - 1)} p^{63n}(p^{2n} - 1)(p^{6n} - 1)(p^{8n} - 1)(p^{10n} - 1)(p^{12n} - 1)(p^{14n} - 1)(p^{18n} - 1),$$

$$|C|=|O^{p'}(C)|\cdot m=\frac{m}{(2,p^{n/r}-1)}p^{63n/r}(p^{2n/r}-1)(p^{6n/r}-1)(p^{8n/r}-1)(p^{10n/r}-1)(p^{12n/r}-1)\times$$
$$\times(p^{14n/r}-1)(p^{18n/r}-1),$$

где m делит $(2,p^{n/r}-1)$. По условию

$$\frac{(2,p^{n/r}-1)}{m\cdot(2,p^n-1)}\cdot\frac{p^{2n}-1}{p^{2n/r}-1}\cdot\frac{p^{6n}-1}{p^{6n/r}-1}\cdot\frac{p^{8n}-1}{p^{8n/r}-1}\cdot\frac{p^{10n}-1}{p^{10n/r}-1}\cdot\frac{p^{12n}-1}{p^{12n/r}-1}\times$$
$$\times\frac{p^{14n}-1}{p^{14n/r}-1}\cdot\frac{p^{18n}-1}{p^{18n/r}-1}=s^b. \tag{5.34}$$

Числа $\dfrac{m}{(2,p^{n/r}-1)}$ и $\dfrac{(2,p^{n/r})}{m\cdot(2,p^n-1)}$ принимают значения 1 или 1/2. Поэтому t не делит эти числа, где t – простой делитель числа $p^{18n}-1$, который не делит p^i-1 для $i<18n$, который существует по теореме 4.4 ввиду $18n\notin\{2,6\}$. Но тогда из (5.34) следует, что $t\neq s$. Значит t делит $|C|$, что опять противоречит выбору t по теореме 4.4 ввиду $r>3$. Лемма доказана.

5.18. ЛЕММА. Пусть $(X, y, C, r, p^a\cdot s^b)\in 5.1$, p – простое число, $q=p^n$. Тогда $X\notin\{E_8(q)\}$.

Доказательство. Если $X\in\{E_8(q)\}$, то $r>3$ и $|X:C|=p^b\cdot s^a$ дает нам [2, с. 145, леммы 4.2, 4.3]), что

$$\frac{p^{2n}-1}{p^{2n/r}-1}\cdot\frac{p^{8n}-1}{p^{8n/r}-1}\cdot\frac{p^{12n}-1}{p^{12n/r}-1}\cdot\frac{p^{14n}-1}{p^{14n/r}-1}\cdot\frac{p^{18n}-1}{p^{18n/r}-1}\times$$
$$\times\frac{p^{20n}-1}{p^{20n/r}-1}\cdot\frac{p^{24n}-1}{p^{24n/r}-1}\cdot\frac{p^{30n}-1}{p^{30n/r}-1}=s^b. \tag{5.35}$$

Из (5.35) следует, что $t\neq s$, где t – простой делитель числа $p^{30n}-1$, который не делит p^i-1 для $i<30n$ (ввиду теоремы 4.4). Но тогда t делит $|C|$, что опять противоречит теореме 4.4. Лемма доказана.

5.19. ЛЕММА. Пусть $(X, y, C, r, p^a\cdot s^b)\in 5.1$, p – простое число, $q=p^n$. Тогда $X\notin\{{}^3D_4(q)\}$.

Доказательство. Предположим противное, то есть, что $X\cong{}^3D_4(q)$. Тогда известно [2, с. 145; 13, теорема 9-1], что

$$|X|=p^{12n}(p^{2n}-1)(p^{8n}+p^{4n}+1)(p^{6n}-1),$$

$$|C|=|O^{p'}(C)|=p^{12n/r}(p^{2n/r}-1)(p^{8n/r}+p^{4n/r}+1)(p^{6n/r}-1)$$

и по условию леммы ввиду $r>3$ имеем:

$$\frac{p^{2n}-1}{p^{2n/r}-1}\cdot\frac{p^{8n}+p^{4n}+1}{p^{8n/r}p^{4n/r}+1}\cdot\frac{p^{6n}-1}{p^{6n/r}-1}=s^b. \tag{5.36}$$

Ясно, что $6n\notin\{2,6\}$, так как $r>3$ делит n. По теореме 4.4 существует простой делитель t, который делит $p^{6n}-1$, но не делит p^i-1 для $i<6n$. Но из (5.36) следует, что s делит $p^{2n}-1$. Противоречие, доказывающее, что $X\notin\{{}^3D_4(q)\}$. Лемма доказана.

5.20. ТЕОРЕМА [15, теорема 9.1.11; 16, леммы 2.2, 2.3; 17, следствия 0.3, 0.4, 0.5; 18, лемма 2.12]. Пусть A есть Π'-группа автоморфизмов Π-группы X, обладающей свойством B_σ (в смысле Ф. Холла), $B=C_X(A)$. Тогда:

(1) по крайней мере, одна S_σ-подгруппа из X A-инвариантна;

(2) любые две A-инвариантные S_σ-подгруппы из X сопряжены элементами из B;

(3) любая A-инвариантная σ-подгруппа из X содержится в A-инвариантной S_σ-подгруппе из X;

(4) если $K \lhd X$ и K есть A-инвариантная подгруппа, то $C_{X/K}(A) = C_X(A)K/K$;

(5) если $H \subseteq B$, то $N_X(H) = C_X(H)(N_X(H) \cap B)$;

(6) если $y \in A$, $y^p = 1$ и H есть y-инвариантная нормальная в X подгруппа, K – y-инвариантная подгруппа в X и $X = HK$, то $C_X(y) = C_H(y)C_K(y)$;

(7) если H есть A-инвариантная подгруппа из X, то $N_X(H)$ и $C_X(H)$ являются A-инвариантными подгруппами.

6. Основной результат

6.1. ТЕОРЕМА. Пусть X – конечная K-группа; y – ее копростой автоморфизм простого порядка r; $C = C_X(y)$. Если $|X:C| = p^{\alpha} \cdot q^{\beta}$, где p и q – различные простые числа; $\alpha \neq 0 \neq \beta$; $\Pi = \{p, q\}$, то $X = C \cdot O_{\Pi}(X)$.

Доказательство. Предположим, что X – простая неабелева группа. Так как X есть K-группа, то $X \in Chev \cup Spor \cup \{An/n \geq 5\}$ [2, с. 145 – 146].

Из теорем 4.239 и 4.240 в [2] следует, что, возможно $X \in Chev$. Из лемм 5.4 – 5.19 следует, что $X \notin Chev$. Поэтому пусть $1 \neq N \lhd X$ и $N \subset X$. Пусть $Y = X\lambda <y>$, M – минимальная нормальная подгруппа группы Y, лежащая в X. Тогда M есть прямое произведение изоморфных простых групп.

Рассмотрим отдельно два случая.

I. M – элементарная абелева группа. Тогда $|M| = s^k$, где s – простое число, k – целое число. Группа $\overline{X} = X/M$ удовлетворяет условию теоремы по теореме 5.20 (4). (Если $|\overline{X}:\overline{C}| = p^a$ или $|\overline{X}:\overline{C}| = q^b$, то $\overline{X} = \overline{C} \cdot O_{\Pi}(\overline{X})$, где $\Pi = \{p\}$ или $\Pi = \{q\}$ по [6]). По индуктивному заключению $\overline{X} = \overline{C} \cdot O_{\Pi}(\overline{X})$. Если $s \in \Pi$, то все доказано. Если $s \notin \Pi$, то прообраз K группы $O_{\Pi}(\overline{X})$ содержит M. Ясно, что K – разрешимая группа, так как $|K/M| = p^{\alpha} \cdot q^{\beta}$. Если $K < X$, то из $K \lhd Y$ следует, что $C \cap K$ имеет в K Π-индекс и применение индукции к K дает нам, что $K = (C \cap K) \cdot O_{\Pi}(K)$. Из $O_{\Pi}(K) \leq O_{\Pi}(X)$ тогда следует, что $X = C \cdot K = C \cdot O_{\Pi}(X)$ и все доказано.

Поэтому пусть $K = X$. Но тогда M есть силовская S-подгруппа в X. Из $s \notin \Pi$ следует, что $C = M$. Тогда по следствию из [19], $X = K = C \cdot F(K) = C \cdot F(X)$. В частности, из рассмотренного случая вытекает, что мы можем считать, что

в X нет разрешимых нормальных y-инвариантных подгрупп. (6.1)

II. M – прямое произведение простых неабелевых групп. Если $M \subset X$, то ясно, что M удовлетворяет условию теоремы ($|M : C \cap M| \in \Pi$). Применение индукции дает нам, что $M = (C \cap M) \cdot O_{\Pi}(M)$. Из разрешимости $O_{\Pi}(M)$ и $M \lhd Y$ следует, что в X имеется и минимальная нормальная s-подгруппа для некоторого простого числа S. Это противоречит (6.1). Поэтому рассмотрим возможность, когда $O_{\Pi}(M) = 1$, то есть $M = C \cap M$, $M \leq C$. По теореме 5.20 (4) группа $\overline{X} = X/M$ удовлетворяет условию теоремы. Поэтому применение индукции дает нам, что $\overline{X} = \overline{C} \cdot O_{\Pi}(\overline{X})$. Из условия теоремы следует, что $O_{\Pi}(\overline{X}) \neq 1$. Пусть L – прообраз группы $O_{\Pi}(\overline{X})$ в X. Тогда L/M – группа порядка $p^a \cdot q^b$, $a \neq 0 \neq b$.

Если $M = C$, то $\overline{X}$ – нильпотентная группа по известной теореме Д. Томпсона [2, теорема 4.115]. В этом случае в $\overline{X}$ есть характеристическая p-подгруппа R/M, $R \subset X$, $C \subset R$. Если $M \subset C$, то $O_{\Pi}(\overline{X}) \subset \overline{X}$. Итак, в любом случае в X имеется собственная y-инвариантная подгруппа $R \neq C$. По индуктивному заключению $R = (R \cap C) \cdot O_{\Pi}(R)$ и $O_{\Pi}(R) \neq 1$. Из $R \lhd Y$ следует, что и $O_{\Pi}(R) \lhd Y$, и мы опять имеем противоречие с (6.1).

Итак, пусть $M = X$. Но тогда при $X = L_1 X \times \ldots \times L_k$, $k > 1$, $C \cong L_1$ [4, предложение 3.27 (vii)]. Это невозможно по условию теоремы. Значит, $X \cong L_1$. Но это противоречит тому, что X – не простая группа. Этим теорема доказана.

ЛИТЕРАТУРА

1. Huppert B. Endliche Gruppen, I. // Berlin, Heidelberg, New York: Springer – Verlag. – 1967. – 793 p.
2. Горенстейн Д. Конечные простые группы. Введение в их классификацию. – М.: Мир, 1985. – 352 с.
3. Gorenstein D., Lyons R., Solomon R. The classification of the finite simple groups // Math. Surveys and monogr. – 1994. – V. 40. – № 1. – Providence, RJ; AMS. – 165 p.
4. Gorenstein D., Lyons R., Solomon R. The classification of the finite simple groups // Math. Surveys and monogr. – 1994. – V. 40. – № 2. – Providence, RJ; AMS. – 218 p.
5. Gorenstein D., Lyons R., Solomon R. The classification of the finite simple groups // Math. Surveys and monogr. – 1994. – V. 40. – № 3. – Providence, RJ; AMS. – 419 p.
6. Логинов В.И. Замечание о конечных группах, допускающих копростые автоморфизмы // Вестник МГУ. Сер. I. Мат., мех. – 1980. – № 6. – С. 58 – 61.
7. C. Chevalley. Sur certains groupes simples, Tohoku Math. – 1955. – V. 7. – № 1 – 2. – P. 14 – 66.
8. R. Steinberg, Variations on a theme of Chevalley, Paciic J. Math. – 1959. – V. 9. – № 3. – P. 875 – 891.
9. M. Suzuki, A new type of simple groups of finite order, Proc. Nat. Acad. Sci. USA. – 1960. – V. 46. – № 2. – P. 868 – 870.
10. R. Ree, A family of simple groups associated with the simple Lie algebra of type (F_4), Amer. J. Math. – 1961. – V. 83. – № 3. – P. 401 – 420.
11. R. Ree, A family of simple groups associated with the simple Lie algebra of type (G_2), Amer. J. Math. – 1961. – V. 83. – № 3. – P. 432 – 462.
12. Zsigmondy K. Zur theorie der Potenzrests // Monatsh. Math. Phys. – 1892. – V. 3. – № 2. – P. 265 – 284.
13. Gorenstein D., Lyons R. The local structure of finite groups of characterictic 2 type // Memoirs AMS. – 1983. – № 276. – P. 1 – 731.
14. Luneburg H. Ein infacher Beweis fur den Satz von Zsigmondy uber primitive Primteibr von $A^n - 1$, Sprinder Lecture Notes in Mathematics. – 1981. – № 893. – P. 219 – 222.
15. Huppert B., Blackburn N. Finite groups, II. Berlin: Springer – Verlag, 1982. – 531 p.
16. Rickman B. Groups which admit a fixed-point-free automorphism of order p^2 // I. Algebra. – 1959. – V. 53. – № 1. – P. 77 – 171.
17. Гаген Т.М. Некоторые вопросы теории конечных групп // В кн.: К теории конечных групп. – М.: Мир, 1979. – С. 13 – 97.
18. Глауберман Дж. О разрешимых сигнализаторных функторах на конечных группах // В кн.: К теории конечных групп. – М.: Мир, 1979. – С. 112 – 143.
19. Пальчик Э.М., Шмидт А.М. О конечных группах, допускающих копростой автоморфизм // Весці НАНБ. Сер. фіз.-мат. н., – 2001. – № 4. – С. 15 – 18.