Сибирский математический журнал
Ноябрь—декабрь, 2007. Том 48, № 6

УДК 512.542

КВАЗИРАСПОЗНАВАЕМОСТЬ ПО МНОЖЕСТВУ ПОРЯДКОВ ЭЛЕМЕНТОВ ГРУПП $E_6(q)$ И ${}^2E_6(q)$

А. С. Кондратьев

Аннотация. Доказано, что если L — одна из простых групп ${}^2E_6(q)$ или $E_6(q)$, а G — конечная группа с множеством порядков элементов как у L, то коммутант группы $G/F(G)$ изоморфен L, а фактор-группа G/G' есть циклическая $\{2,3\}$-группа.

Ключевые слова: конечная группа, простая группа, множество порядков элементов, квазираспознаваемость, граф простых чисел.

Пусть G — конечная группа. Обозначим через $\omega(G)$ множество всех порядков элементов группы G. Множество $\omega(G)$ определяет *граф простых чисел* (*граф Грюнберга — Кегеля*) $GK(G)$ группы G, в котором вершинами служат простые делители порядка группы G и две различные вершины p и q соединены ребром тогда и только тогда, когда G содержит элемент порядка pq. Обозначим число компонент связности графа $GK(G)$ через $t(G)$, а множество его связных компонент — через $\{\pi_i(G) \mid 1 \leq i \leq t(G)\}$; при этом для группы G четного порядка считаем, что $2 \in \pi_1(G)$. Множество $\omega(G)$ частично упорядочено относительно делимости и однозначно определяется подмножеством $\mu(G)$ своих максимальных элементов.

Грюнберг и Кегель доказали следующую структурную теорему для конечных групп с несвязным графом простых чисел.

Теорема Грюнберга — Кегеля [1, теорема A]. *Если G — конечная группа с несвязным графом $GK(G)$, то верно одно из следующих утверждений:*

(а) *G — группа Фробениуса;*

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

(в) *G является расширением нильпотентной $\pi_1(G)$-группы посредством группы A, где $\operatorname{Inn}(P) \leq A \leq \operatorname{Aut}(P)$, P — простая неабелева группа с $t(G) \leq t(P)$ и $A/\operatorname{Inn}(P)$ — $\pi_1(G)$-группа.*

Конечные простые неабелевы группы с несвязным графом простых чисел описаны в [1, 2].

Результаты о конечных группах с несвязным графом Грюнберга — Кегеля нашли большое применение в исследованиях распознаваемости конечных групп по множеству порядков элементов (см., например, последний обзор В. Д. Мазурова [3]). Конечная группа G называется *распознаваемой* (по множеству порядков элементов), если для любой конечной группы H с условием $\omega(H) = \omega(G)$ имеем $H \cong G$.

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 04–01–00463) и РФФИ–ГФЕН Китая (код проекта 05–01–39000).

Первый этап решения вопроса распознаваемости конечных простых групп с несвязным графом Грюнберга — Кегеля заключается в доказательстве условия квазираспознаваемости, более слабого, чем распознаваемость. Конечная простая неабелева группа P называется *квазираспознаваемой*, если любая конечная группа G с условием $\omega(G) = \omega(P)$ имеет композиционный фактор, изоморфный P. Заметим, что для квазираспознаваемой конечной простой группы положительно решается вопрос 12.39 Ши из [4] о распознаваемости конечных простых групп по множеству порядков элементов и порядку.

В [5, 6] показано, что все конечные простые неабелевы группы P с $t(P) \geq 3$ квазираспознаваемы, за исключением случая, когда P изоморфна группе A_6. В [7] доказана квазираспознаваемость простых групп ${}^2D_{2^m}(2^k)$, ${}^2D_{2^m+1}(2)$ $(m > 1)$, $C_{2^m}(2^k)$ $(m > 2)$, в [8, 9] — квазираспознаваемость простых групп ${}^3D_4(q)$ и $F_4(q)$.

В данной работе получена следующая

Теорема. *Если L — одна из простых групп $E_6(q)$ или ${}^2E_6(q)$, а G — конечная группа с условием $\omega(G) = \omega(L)$, то коммутант группы $G/F(G)$ изоморфен L, а фактор-группа G/G' есть циклическая $\{2, 3\}$-группа.*

Тем самым завершается доказательство квазираспознаваемости всех простых исключительных групп лиева типа с несвязным графом Грюнберга — Кегеля, кроме групп $G_2(q)$, где q не делится на 3.

Наши обозначения и терминология в основном стандартны, их можно найти в [10–14]. Если n — натуральное число и p — простое число, то через n_p и $\pi(n)$ обозначаются соответственно p-часть и множество всех простых делителей числа n. Для конечной группы G положим $\pi(G) = \pi(|G|)$ и $\mu_i(G) = \{n \in \mu(G) \mid \pi(n) \subseteq \pi_i(G)\}$. Через δ, ϵ обозначаются переменные, принимающие значения $+$ или $-$. Группы $L_n^\epsilon(q)$, $SL_n^\epsilon(q)$, $GL_n^\epsilon(q)$ и $E_6^\epsilon(q)$ обозначают соответственно через $L_n(q)$, $SL_n(q)$, $GL_n(q)$ и $E_6(q)$ при $\epsilon = +$ и $U_n(q)$, $SU_n(q)$, $GU_n(q)$ и ${}^2E_6(q)$ при $\epsilon = -$.

В доказательстве теоремы используются шесть предварительных лемм.

Лемма 1 [15, лемма 4]. *Пусть P — конечная простая группа с несвязным графом Грюнберга — Кегеля. Тогда*

(а) *$|\mu_i(P)| = 1$ для $i > 1$, пусть $n_i = n_i(P)$ обозначает единственный элемент из $\mu_i(P)$ для $i > 1$;*

(б) *для каждого $i > 1$ группа P содержит изолированную абелеву холлову $\pi(n_i)$-подгруппу X_i, причем эта подгруппа циклическая порядка n_i, за исключением следующих случаев:*

(1) *$P \cong L_3(4)$, $n_i(P) = 3$ и подгруппа X_i элементарная абелева порядка 9;*

(2) *$P \cong L_2(q)$, где q — непростая степень нечетного простого числа p, $n_i(P) = p$ и подгруппа X_i элементарная абелева порядка q;*

(в) *P, $\pi_1(P)$, n_i для $2 \leq i \leq t(P)$ такие, как в приведенных ниже табл. 1–3, где p — нечетное простое число.*

Лемма 2. *Пусть G — конечная группа с несвязным графом Грюнберга — Кегеля, для которой выполняется случай* (в) *теоремы Грюнберга — Кегеля, и P — неабелев композиционный фактор в G. Тогда для каждого $i \in \{2, \dots, t(G)\}$ существует $j \in \{2, \dots, t(P)\}$ такое, что $\mu_i(G) = \{n_j(P)\}$.*

Доказательство очевидно.

Лемма 3 [16, теорема Жигмонди]. *Пусть q и n — натуральные числа, $q \geq 2$, $n \geq 3$. Если $(q,n) \neq (2,6)$, то существует простое число, делящее $q^n - 1$ и не делящее $q^i - 1$ при любом натуральном $i < n$.*

Лемма 4 [17]. *Пусть p, q — простые числа такие, что $p^a - q^b = 1$ для некоторых натуральных чисел a, b. Тогда пара (p^a, q^b) равна $(3^2, 2^3)$, $(p, 2^b)$ или $(2^a, q)$.*

Лемма 5 [13, часть G; 18, табл. 1]. (а) *Порядки максимальных торов группы $E_6(q)$ принимают следующие значения: $(q-1)^6/d$, $(q-1)^5(q+1)/d$, $(q^2-1)^2(q\pm1)^2/d$, $(q^2-1)^3/d$, $(q^4-1)(q\pm1)^2/d$, $(q^4\pm1)(q^2-1)/d$, $(q^2+1)^2(q-1)^2/d$, $(q^3-1)(q-1)^3/d$, $(q^3-1)(q^2-1)(q\pm1)/d$, $(q^3-1)^2/d$, $(q^3+1)(q^2\pm1)(q-1)/d$, $(q^6-1)/d$, $(q^2+q+1)^2(q^2-1)/d$, $(q^2+q+1)^3/d$, $(q^3+1)(q^2+q+1)(q+1)/d$, $(q^5-1)(q\pm1)/d$, $(q^4-q^2+1)(q^2+q+1)/d$, $(q^6+q^3+1)/d$, $(q^2+q+1)(q^2-q+1)^2/d$, где $d=(3,q-1)$.*

(б) *Порядки максимальных торов группы ${}^2E_6(q)$ принимают следующие значения: $(q+1)^6/d$, $(q+1)^5(q-1)/d$, $(q^2\pm1)^2(q+1)^2/d$, $(q^2-1)^3/d$, $(q^2-1)^2(q-1)^2/d$, $(q^4-1)(q\pm1)^2/d$, $(q^4\pm1)(q^2-1)/d$, $(q^3+1)(q+1)^3/d$, $(q^3+1)(q^2-1)(q\pm1)/d$, $(q^3+1)^2/d$, $(q^3-1)(q^2\pm1)(q+1)/d$, $(q^6-1)/d$, $(q^2-q+1)^2(q^2-1)/d$, $(q^2-q+1)^3/d$, $(q^3-1)(q^2-q+1)(q-1)/d$, $(q^5+1)(q\pm1)/d$, $(q^4-q^2+1)(q^2-q+1)/d$, $(q^6-q^3+1)/d$, $(q^2-q+1)(q^2+q+1)^2/d$, где $d=(3,q+1)$.*

Лемма 6. (а) *Группа $L_n(q)$, где $n \geq 2$, содержит циклические подгруппы порядков $(q^{n-1}-1)/(n,q-1)$ и $q^{n-2}-1$ при $n \geq 3$.*

(б) *Группа $L_n^-(q)$, где $n \geq 3$, содержит циклическую подгруппу порядка $(q^{n-1}-1)/(n,q+1)$ при нечетном n и циклическую подгруппу порядка $q^{n-2}-1$ при четном n.*

(в) *Группа $PSp_{2n}(q)$, где $n \geq 2$, содержит циклические подгруппы порядков $(q^n-1)/(2,q-1)$ и $q^{n-1}-1$.*

(г) *Группа $P\Omega_{2n+1}(q)$, где q нечетно и $n \geq 2$, содержит циклические подгруппы порядков $(q^n-1)/2$ и $q^{n-1}-1$.*

(д) *Группа $P\Omega_{2n}^+(q)$, где $n \geq 2$, содержит циклические подгруппы порядков $(q^{n-2}-1)$, $(q^{n-1}-1)/(2,q-1)$ и $(q^n-1)/f$, где f равно 4, если q нечетно и $n(q-1)/2$ четно, и $(2,q-1)$ в противном случае.*

(е) *Группа $P\Omega_{2n}^-(q)$, где $n \geq 2$, содержит циклическую подгруппу порядка $(q^{n-1}-1)/f$, где f равно 4, если q нечетно и $(n-1)(q-1)/2$ четно, и $(2,q-1)$ в противном случае. Если $n = 2^m \geq 4$, то группа $P\Omega_{2n}^-(q)$ содержит циклическую подгруппу порядка $(q^n-1)/(2,q-1)$.*

Доказательство. (а), (б) Рассмотрим в $SL_n^\epsilon(q)$, где $n \geq 2$, подгруппу H, состоящую из всех $n \times n$-матриц вида $\begin{pmatrix} A & O_{1,n-1} \\ O_{n-1,1} & d^{-1} \end{pmatrix}$, где $A \in GL_{n-1}^\epsilon(q)$, $O_{m,n}$ обозначает нулевую $m \times n$-матрицу и $d = \det(A)$. Тогда H изоморфна группе $GL_{n-1}^\epsilon(q)$. Ясно, что группа H содержит подгруппу H_1, изоморфную $SL_{n-1}^\epsilon(q)$, причем $H_1 \cap Z(SL_n^\epsilon(q)) \leq Z(H_1) \cap Z(SL_n^\epsilon(q)) = 1$.

Пусть $\epsilon = +$. Тогда по теореме II.7.3 из [12] группа H содержит циклическую подгруппу Z порядка $q^{n-1}-1$ (это цикл Зингера в $GL_{n-1}(q)$) и аналогично при $n \geq 3$ группа H_1 содержит циклическую подгруппу Z_1 порядка $q^{n-2}-1$. Рассматривая образы подгрупп Z и Z_1 при естественном гомоморфизме группы $SL_n(q)$ на $L_n(q)$, получим утверждение п. (а).

Пусть $\epsilon = -$. Предположим, что n нечетно. Тогда по утверждению 4.2.4 из [19] группа H содержит подгруппу H_2, изоморфную группе $GL_{\frac{n-1}{2}}(q^2)$ (это

Таблица 1. Конечные простые группы P с $t(P) = 2$

P	Ограничения на P	$\pi_1(P)$	n_2
A_n	$6 < n = p, p+1, p+2$; одно из $n, n-2$ не просто	$\pi((n-3)!)$	p
$A_{p-1}(q)$	$(p,q) \neq (3,2), (3,4)$	$\pi\left(q\prod_{i=1}^{p-1}(q^i-1)\right)$	$\frac{q^p-1}{(q-1)(p,q-1)}$
$A_p(q)$	$(q-1)\vert(p+1)$	$\pi\left(q(q^{p+1}-1)\prod_{i=1}^{p-1}(q^i-1)\right)$	$\frac{q^p-1}{q-1}$
${}^2A_{p-1}(q)$		$\pi\left(q\prod_{i=1}^{p-1}(q^i-(-1)^i)\right)$	$\frac{q^p+1}{(q+1)(p,q+1)}$
${}^2A_p(q)$	$(q+1)\vert(p+1)$, $(p,q) \neq (3,3), (5,2)$	$\pi\left(q(q^{p+1}-1)\prod_{i=1}^{p-1}(q^i-(-1)^i)\right)$	$\frac{q^p+1}{q+1}$
${}^2A_3(2)$		$\{2,3\}$	5
$B_n(q)$	$n = 2^m \geq 4$, q нечетно	$\pi\left(q\prod_{i=1}^{n-1}(q^{2i}-1)\right)$	$(q^n+1)/2$
$B_p(3)$		$\pi\left(3(3^p+1)\prod_{i=1}^{p-1}(3^{2i}-1)\right)$	$(3^p-1)/2$
$C_n(q)$	$n = 2^m \geq 2$	$\pi\left(q\prod_{i=1}^{n-1}(q^{2i}-1)\right)$	$\frac{q^n+1}{(2,q-1)}$
$C_p(q)$	$q = 2, 3$	$\pi\left(q(q^p+1)\prod_{i=1}^{p-1}(q^{2i}-1)\right)$	$\frac{q^p-1}{(2,q-1)}$
$D_p(q)$	$p \geq 5, q = 2, 3, 5$	$\pi\left(q\prod_{i=1}^{p-1}(q^{2i}-1)\right)$	$\frac{q^p-1}{q-1}$
$D_{p+1}(q)$	$q = 2, 3$	$\pi\left(q(q^p+1)\prod_{i=1}^{p-1}(q^{2i}-1)\right)$	$\frac{q^p-1}{(2,q-1)}$
${}^2D_n(q)$	$n = 2^m \geq 4$	$\pi\left(q\prod_{i=1}^{n-1}(q^{2i}-1)\right)$	$\frac{q^n+1}{(2,q+1)}$
${}^2D_n(2)$	$n = 2^m+1, m \geq 2$	$\pi\left(2(2^n+1)\prod_{i=1}^{n-2}(2^{2i}-1)\right)$	$2^{n-1}+1$
${}^2D_p(3)$	$5 \leq p \neq 2^m+1$	$\pi\left(3\prod_{i=1}^{p-1}(3^{2i}-1)\right)$	$\frac{3^p+1}{4}$
${}^2D_n(3)$	$n = 2^m+1 \neq p, m \geq 2$	$\pi\left(3(3^n+1)\prod_{i=1}^{n-2}(3^{2i}-1)\right)$	$\frac{3^{n-1}+1}{2}$
$G_2(q)$	$2 < q \equiv \epsilon(3)$, $\epsilon = \pm 1$	$\pi(q(q^2-1)(q^3-\epsilon))$	$q^2-\epsilon q+1$
${}^3D_4(q)$		$\pi(q(q^6-1))$	q^4-q^2+1
$F_4(q)$	q нечетно	$\pi(q(q^6-1)(q^8-1))$	q^4-q^2+1
${}^2F_4(2)'$		$\{2,3,5\}$	13
$E_6(q)$		$\pi(q(q^5-1)(q^8-1)(q^{12}-1))$	$\frac{q^6+q^3+1}{(3,q-1)}$
${}^2E_6(q)$	$q > 2$	$\pi(q(q^5+1)(q^8-1)(q^{12}-1))$	$\frac{q^6-q^3+1}{(3,q+1)}$
M_{12}		$\{2,3,5\}$	11

Окончание таблицы 1.

P	Ограничения на P	$\pi_1(P)$	n_2
J_2		$\{2,3,5\}$	7
Ru		$\{2,3,5,7,13\}$	29
He		$\{2,3,5,7\}$	17
McL		$\{2,3,5,7\}$	11
Co_1		$\{2,3,5,7,11,13\}$	23
Co_3		$\{2,3,5,7,11\}$	23
Fi_{22}		$\{2,3,5,7,11\}$	13
F_5		$\{2,3,5,7,11\}$	19

подгруппа индекса 2 в стабилизаторе в $GL^-_{n-1}(q)$ разложения $(n-1)$-мерного унитарного пространства над полем порядка q^2 в прямую сумму двух вполне сингулярных подпространств одинаковой размерности). Цикл Зингера Z в этой подгруппе есть циклическая группа порядка $q^{n-1}-1$. Рассматривая образ подгруппы Z при естественном гомоморфизме группы $SL^-_n(q)$ на $L^-_n(q)$, получим первое утверждение п. (б).

Пусть теперь n четно. Рассуждая, как в предыдущем абзаце, получим, что подгруппа $H_1 \cong SL^-_{n-1}(q)$ содержит циклическую подгруппу Z порядка $q^{n-2}-1$. Так как $H_1 \cap Z(SL^\epsilon_n(q)) = 1$, то образ подгруппы Z при естественном гомоморфизме группы $SL^-_n(q)$ на $L^-_n(q)$ изоморфен Z, откуда следует второе утверждение п. (б).

(в) Ввиду утверждений 4.2.3 и 4.2.5 из [19] стабилизатор в $Sp_{2n}(q)$ разложения $2n$-мерного симплектического пространства над полем порядка q в прямую сумму двух ортогональных вполне сингулярных подпространств одинаковой размерности содержит подгруппу, изоморфную группе $GL_n(q)$. Цикл Зингера Z в этой подгруппе есть циклическая группа порядка q^n-1. Рассматривая образ подгруппы Z при естественном гомоморфизме группы $Sp_{2n}(q)$ в ее фактор-группу по центру, получим циклическую подгруппу порядка $(q^n-1)/(2,q-1)$.

Ввиду утверждения 4.1.3 из [19] группа $PSp_{2n}(q)$ содержит подгруппу, изоморфную $Sp_{2(n-1)}(q)$, которая, как мы видели в предыдущем абзаце, содержит циклическую подгруппу порядка $q^{n-1}-1$.

(г) Ввиду утверждения 4.1.20 из [19] группа $P\Omega_{2n+1}(q)$ при нечетном q содержит подгруппу, изоморфную единственной подгруппе $\frac{1}{2}GL_n(q)$ индекса 2 в $GL_n(q)$. Пересечение цикла Зингера из $GL_n(q)$ с подгруппой $\frac{1}{2}GL_n(q)$ дает циклическую подгруппу порядка $(q^n-1)/2$.

Так как $GL_{n-1}(q) < SL_n(q) \leq \frac{1}{2}GL_n(q)$, то цикл Зингера из $GL_{n-1}(q)$ дает циклическую подгруппу порядка $q^{n-1}-1$.

(д) Ввиду утверждения 4.1.20 из [19] группа $P\Omega^+_{2n}(q)$ содержит подгруппу, изоморфную группе $GL_n(q)$ при четном q, группе $\frac{1}{2}GL_n(q)$ при нечетных q и $qn(q-1)/2$ и фактор-группе J группы $\frac{1}{2}GL_n(q)$ по ее единственной центральной подгруппе порядка 2 при нечетном q и четном $n(q-1)/2$. Теперь если Z — цикл Зингера в $GL_n(q)$, то циклической подгруппой порядка $(q^n-1)/f$ в $P\Omega^+_{2n}(q)$ будет Z при четном q, пересечение Z с $\frac{1}{2}GL_n(q)$ при нечетных q и $qn(q-1)/2$, и образ этого пересечения в J при нечетном q и четном $n(q-1)/2$.

Таблица 2. Конечные простые группы P с $t(P) = 3$

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

Ввиду утверждения 4.1.6 из [19] группа $P\Omega^+_{2n}(q)$ содержит подгруппу H, изоморфную $\Omega^+_{2(n-1)}(q)$. Из доказательства утверждения 4.1.20 в [19] видно, что H содержит подгруппу H_1, изоморфную группе $GL_{n-1}(q)$ при четном q и группе $\frac{1}{2}GL_{n-1}(q)$ при нечетном q. Как мы видели выше, подгруппа H_1 содержит циклические подгруппы порядков $(q^{n-1}-1)/(2,q-1)$ и $q^{n-2}-1$.

(е) Ввиду утверждения 4.1.20 из [19] группа $P\Omega^-_{2n}(q)$ содержит подгруппу H, изоморфную группе $GL_{n-1}(q)$ при четном q, группе $\frac{1}{2}GL_{n-1}(q)$ при нечетных q и $q(n-1)(q-1)/2$ и фактор-группе J группы $\frac{1}{2}GL_{n-1}(q)$ по ее единственной центральной подгруппе порядка 2 при нечетном q и четном $(n-1)(q-1)/2$. Далее, рассуждая как при доказательстве п. (д), получаем первое утверждение

Таблица 3. Конечные простые группы P с $t(P) > 3$

$t(P)$	P	Ограничения на P	$\pi_1(P)$	n_2	n_3	n_4	n_5	n_6
4	$A_2(4)$		$\{2\}$	3	5	7		
	${}^2B_2(q)$	$q = 2^{2m+1} > 2$	$\{2\}$	$q-1$	$q-\sqrt{2q}+1$	$q+\sqrt{2q}+1$		
	${}^2E_6(2)$		$\{2,3,5,7,11\}$	13	17	19		
	$E_8(q)$	$q \equiv 2,3(5)$	$\pi(q(q^8-1)(q^{12}-1)(q^{14}-1)(q^{18}-1)(q^{20}-1))$	$\frac{q^{10}+q^5+1}{q^2+q+1}$	q^8-q^4+1	$\frac{q^{10}-q^5+1}{q^2-q+1}$		
	M_{22}		$\{2,3\}$	5	7	11		
	J_1		$\{2,3,5\}$	7	11	19		
	$O'N$		$\{2,3,5,7\}$	11	19	31		
	LyS		$\{2,3,5,7,11\}$	31	37	67		
	Fi'_{24}		$\{2,3,5,7,11,13\}$	17	23	29		
	F_1		$\{2,3,5,7,11,13,17,19,23,29,31,47\}$	41	59	71		
5	$E_8(q)$	$q \equiv 0,1,4(5)$	$\pi(q(q^8-1)(q^{10}-1)(q^{12}-1)(q^{14}-1)(q^{18}-1))$	$\frac{q^{10}+q^5+1}{q^2+q+1}$	$\frac{q^{10}-q^5+1}{q^2-q+1}$	q^8-q^4+1	$\frac{q^{10}+1}{q^2+1}$	
6	J_4		$\{2,3,5,7,11\}$	23	29	31	37	43

п. (e).

Если $n = 2^m \geq 4$, то ввиду утверждений 4.3.16 и 2.9.1 из [19] группа $P\Omega^-_{2n}(q)$ содержит подгруппу, изоморфную $P\Omega^-_4(q^{n/2}) \cong L_2(q^n)$. Цикл Зингера из этой подгруппы есть искомая циклическая подгруппа для второго утверждения п. (e).

Лемма доказана.

Доказательство теоремы. Пусть $L = E^\delta_6(q)$, $d = (3, q-\delta 1)$ и G — конечная группа с условием $\omega(G) = \omega(L)$. Распознаваемость группы ${}^2E_6(2)$ доказана (см. [3]), поэтому мы будем считать, что $q > 2$ при $\delta = -$. Ввиду теоремы Грюнберга — Кегеля, результата М. Р. Зиновьевой (Алеевой) [20] и лемм 1 и 2 имеем $\mathrm{Inn}(P) \trianglelefteq \overline{G} = G/F(G) \leq \mathrm{Aut}(P)$, где P — конечная простая группа с $t(P) \geq t(L) = 2$, $\pi(F(G)) \cup \pi(\overline{G}/\mathrm{Inn}(P)) \subseteq \pi_1(G) = \pi(q(q^5-\delta 1)(q^8-1)(q^{12}-1))$ и $n_2(L) = (q^6+\delta q^3+1)/d \in \{n_i(P) \mid 2 \leq i \leq t(P)\}$. Далее рассматриваются все возможности для P, описываемые в лемме 1.

Если P изоморфна одной из спорадических групп или одной из групп ${}^2A_3(2)$, ${}^2F_4(2)'$, ${}^2A_5(2)$, $E_7(2)$, $E_7(3)$, $A_2(4)$, ${}^2E_6(2)$, то непосредственными вычислениями показываем, что включения $(q^6+\delta q^2+1)/d \in \{n_i(P) \mid 2 \leq i \leq t(P)\}$ и $\pi_1(P) \subseteq \pi_1(L)$ приводят к противоречию.

1. Пусть $P \cong E^\epsilon_6(r)$, где $r > 2$ при $\epsilon = -$. Следовательно, $t(P) = 2$ и

$$(q^6+\delta q^3+1)/d = (r^6+\epsilon r^3+1)/(3, r-\epsilon 1).$$

Предположим, что $d = (3, r - \epsilon 1)$. Тогда $q^6 + \delta q^2 + 1 = r^6 + \epsilon r^3 + 1$, откуда $q^3(q^3 + \delta 1) = r^3(r^3 + \epsilon 1)$. Если $(q, r) \neq 1$, то $r = q$ и $\epsilon = \delta$, что не противоречит теореме. Пусть $(q, r) = 1$. Тогда $(q^3 + \delta 1) = ar^3$ для некоторого $a \in \mathbb{N}$ и, следовательно, $r^3(r^3 + \epsilon 1) = ar^3(ar^3 - \delta 1)$, откуда $(a^2 - 1)r^3 = \delta a + \epsilon 1$. Если $a = 1$, то $r^3 - q^3 = \delta 1$; противоречие с леммой 4. Поэтому $a > 1$ и, следовательно, $\delta a + \epsilon 1 > 0$. Но тогда $\delta = +$ и $8 \leq r^3 = (a + \epsilon 1)/(a^2 - 1) \leq (a + \epsilon 1)/(a - 1) = 1 + (1 + \epsilon 1)/(a - 1) \leq 3$; противоречие.

Итак, без ограничения общности можно считать, что $d = 3$ и $(3, r - \epsilon 1) = 1$. Положим $q_1 = q^3$ и $r_1 = r^3$. Тогда $q_1^2 + \delta q_1 + 1 = 3\bigl(r_1^2 + \epsilon r_1 + 1\bigr)$ и, следовательно, $(q_1 - \delta 1)(q_1 + \delta 2) = 3r_1(r_1 + \epsilon 1)$. Так как $(q_1 - \delta 1, q_1 + \delta 2) = 3$, то r_1 делит либо $q_1 - \delta 1$, либо $q_1 + \delta 2$.

Предположим, что r_1 делит $q_1 - \delta 1$, т. е. $q_1 - \delta 1 = ar_1$ для некоторого $a \in \mathbb{N}$. Тогда $a(ar_1 + \delta 3) = 3(r_1 + \epsilon 1)$ и, следовательно, $(a^2 - 3)r_1 = 3(\epsilon 1 - \delta a)$. Если $a = 1$, то $r_1 = 3(\delta 1 - \epsilon 1)/2 \leq 3$; противоречие. Поэтому $a > 1$ и, следовательно, $\epsilon 1 - \delta a > 0$. Но тогда $\delta = -$ и либо $a = 2$, $\epsilon = +$ и $r_1 = r^3 = 9$, либо $8 \leq r_1 = 3(a + \epsilon 1)/(a^2 - 3) \leq 6$; противоречие.

Аналогично приходим к противоречию и в случае, когда r_1 делит $q_1 + 2\delta 1$.

2. Пусть $P \cong A_n$. По лемме 1 либо $n \in \{p, p+1, p+2\}$, одно из $n, n-2$ не простое и $n_2(L) = p$, либо числа $n = p, p-2$ простые и $n_2(L) \in \{p, p-2\}$. Ясно, что $1 < n_2(L) - 2 \leq n - 2$ и $n_2(L) - 2$ нечетно. Поэтому в P существует элемент (цикл) порядка $n_2(L) - 2$.

Предположим, что $d = 1$. Тогда $n_2(L) - 2 = q^6 + \delta q^3 - 1$. Положим $f = q^6 + \delta q^3 - 1$. Тогда в L существует полупростой элемент порядка f. Этот элемент принадлежит некоторому максимальному тору T группы L. Поэтому f делит $|T|$. Легко проверить, что $(f, q^6 - 1) = (f, q^6 + \delta q^3 + 1) = (f, q^4 + 1) = 1$, $(f, q^2 + 1) = (5, q + \delta 2)$, $(f, q^5 - \delta 1) = (11, q + \delta 2)$ и $(f, q^6 + 1) = (5, q^6 + 1)$. Если $q = 2$ и $\delta = +$, то $f = 71$. Если $q \geq 3$, то $f \geq 3^6 - 3^3 - 1 = 701$. В каждом из этих случаев ввиду леммы 5 число f не может делить порядок никакого максимального тора из L; противоречие.

Итак, $d = 3$, и $n_2(L) - 2 = (q^6 + \delta q^3 - 5)/3$. Положим $f = q^6 + \delta q^3 - 5$. Если 5 делит q, то $f_5 = 5$. Поэтому число $f/(5, q)$ взаимно просто с q. Следовательно, в L существует полупростой элемент порядка $\frac{f}{3(5,q)}$. Этот элемент принадлежит некоторому максимальному тору T группы L, поэтому $\frac{f}{3(5,q)}$ делит $|T|$. Легко проверить, что $(f, q - 1) = (4 - \delta 1, q - 1)$, $(f, q + 1) = (4 + \delta 1, q + 1)$, $(f, q^2 + 1) = (37, q + \delta 6)$, $(f, q^2 + q + 1) = (4 - \delta 1, q^2 + q + 1)$, $(f, q^2 - q + 1) = (4 + \delta 1, q^2 - q + 1)$, $(f, q^4 + 1) = (697, q - \delta 202)$, $(f, (q^5 - \delta 1)/(q - \delta 1)) = (991, q - \delta 197)$, $(f, q^6 + 1) = (37, q^6 + 1)$ и $(f, q^6 + \delta q^3 + 1) = (3, q^6 + \delta q^3 + 1)$. Ввиду леммы 5 отсюда, в частности, получается, что $\pi(f) \subseteq \{3, 5, 17, 37, 41, 991\}$. Если $q = 4$ и $\delta = +$, то $f = 4155 = 15 \cdot 277$; противоречие. Если $q = 5$ и $\delta = -$, то $f = 15495 = 3 \cdot 5 \cdot 1033$; противоречие. Поэтому $q \geq 7$ и, следовательно, $f \geq 7^6 - 7^3 - 5 = 117301$.

Пусть $(f, (q^5 - \delta 1)/(q - \delta 1)) \neq 1$. Тогда по доказанному выше $(f, (q^5 - \delta 1)/(q - \delta 1)) = (991, q - \delta 197) = 991$ и, в частности, $q \geq 991 + \delta 197 \geq 991 - 197 = 794$. Ввиду леммы 5 число $\frac{f}{3(5,q)}$ делит $991(q - \delta 1)(q \pm 1)/3$ и, следовательно, f делит $(5, q)991(q - \delta 1)(q \pm 1)$. Если $(5, q) = 5$, то f делит $3^2 \cdot 5 \cdot 991$ или $3 \cdot 5^2 \cdot 991$. Если $(5, q) = 1$, то f делит $3^2 \cdot 991$ или $3 \cdot 5 \cdot 991$. В любом случае имеем $f \leq 75 \cdot 991$. С другой стороны, $f \geq 794^6 - 794^3 - 5 > 75 \cdot 991$; противоречие.

Пусть $(f, q^4 + 1) \neq 1$. Так как $697 = 17 \cdot 41$, по доказанному выше $(f, q^4 + 1) = (697, q - \delta 202) \in \{17, 41, 697\}$. Ввиду леммы 5 число $\frac{f}{3(5,q)}$ делит $697(f, q^2 - 1)/3$ и, следовательно, f делит число $(5,q)(f,697)15$, не превосходящее $75\cdot 697 < 117301$; противоречие с тем, что $f \geq 117301$.

Пусть $(f, q^2+1) \neq 1$. По доказанному выше $(f, q^2+1) = 37$. Ввиду леммы 5 число $\frac{f}{3(5,q)}$ делит одно из чисел $37(q^2-1)(q\pm 1)^2/3$, $37(q^2-1)^2/3$, $37(q^2-1)(q^2-\delta q+1)^2/3$, $37^2(q-\delta 1)^2/3$. Если $(5,q)=5$, то f делит одно из чисел $37\cdot 5^2\cdot 3^3$, $37\cdot 5^4\cdot 3$, $37\cdot 5^3\cdot 3^2$ или $37^2\cdot 5\cdot 3^2$. Если $(5,q)=1$, то f делит одно из чисел $37\cdot 5\cdot 3^3$, $37\cdot 5^3\cdot 3$, $37\cdot 5^2\cdot 3^2$ или $37^2\cdot 3^2$. В любом случае имеем $f \leq 37\cdot 5^4\cdot 3 = 69375$. С другой стороны, $f \geq 117301$; противоречие.

Итак, $\pi(f) \subseteq \{3,5\}$, и ввиду леммы 5 получаем $f \leq 3\cdot 5^6 = 46875$. Вместе с тем $f \geq 117301$; противоречие.

3. Пусть $P \cong {}^3D_4(r)$ или $F_4(r)$. Тогда $(q^6+\delta q^3+1)/d \in \{r^4+1, r^4-r^2+1\}$.

Пусть $(q^6+\delta q^3+1)/d = r^4+1$. Тогда по лемме 1 число r четно. Если $d=1$, то $q^3(q^3+\delta 1) = r^4$; противоречие. Поэтому $d=3$ и $q^6+\delta q^3-2 = 3r^4$, откуда $(q^3-\delta 1)(q^3+\delta 2) = 3r^4$. Так как 3 делит $q^3-\delta 1$ и $q^3+\delta 2 = (q^3-\delta 1)+\delta 3$, то r есть степень числа 3; противоречие с четностью r.

Итак, $(q^6+\delta q^3+1)/d = r^4-r^2+1$. Полагая $q_1 = q^3$ и $r_1 = r^2$, получим $\big(q_1^2+\delta q_1+1\big)/d = r_1^2-r_1+1$.

Пусть $d=1$. Тогда $q_1(q_1+\delta 1) = r_1(r_1-1)$. Предположим, что $(q,r)\neq 1$. Тогда $r_1 = q_1$ и $\delta = -$. Поэтому $\pi(q^9-1) \subseteq \pi_1(P) \subseteq \pi_1(L) = \pi((q^5+1)(q^8-1)(q^{12}-1))$. Так как $(q^9-1, q^5+1) = (q-1,2)$, $(q^9-1, q^8-1) = q-1$ и $(q^9-1, q^{12}-1) = q^3-1$, то по теореме Жигмонди найдется простой делитель числа q^9-1, который не делит $|L|$; противоречие. Таким образом, $(q_1, r_1) = 1$. Поэтому $q_1+\delta 1 = ar_1$ и $r_1 - 1 = bq_1$ для некоторых $a,b\in\mathbb{N}$ и, следовательно, $q_1+\delta 1 = a(bq_1+1)$. Отсюда $ab=1$ и $\delta=+$. В частности, $r_1-q_1=1$, и ввиду леммы 4 получаем $r=3$ и $q=2$. Если $P\cong F_4(3)$, то

$$\pi_1(F_4(3)) = \{2,3,5,7,13,41\} \subseteq \pi_1(E_6(2)) = \{2,3,5,7,13,17,31\};$$

противоречие. Следовательно, $P\cong {}^3D_4(3)$ и $\pi_1({}^3D_4(3)) = \{2,3,7,13\}$. Так как $|\operatorname{Out}({}^3D_4(3))| = 3$, то $\pi(F(G))$ содержит $\{5,17,31\}$. Поскольку подгруппа $F(G)$ нильпотентна, в ней найдется элемент порядка $5\cdot 17\cdot 31$. Значит, и в L найдется полупростой элемент порядка $5\cdot 17\cdot 31$. Этот элемент содержится в некотором максимальном торе T группы L, и, следовательно, $5\cdot 17\cdot 31$ делит $|T|$. Но это по лемме 5 противоречит всем возможностям для $|T|$.

Итак, $d=3$ и $q_1^2+\delta q_1-2 = 3r_1(r_1-1)$. Отсюда $(q_1-\delta 1)(q_1+\delta 2) = 3r_1(r_1-1)$. Ясно, что $(q_1-\delta 1, q_1+\delta 2) = 3$, поэтому r_1 делит $q_1-\delta 1$ или $q_1+\delta 2$.

Пусть $q_1-\delta 1 = ar_1$ для некоторого $a\in\mathbb{N}$ и, следовательно, $ar_1(ar_1+\delta 3) = 3r_1(r_1-1)$. Отсюда $(a^2-3)r_1 = -3(\delta a+1)$. Если $a>1$, то $\delta = -$ и $4 \leq r_1 = 3(a-1)/(a^2-3) \leq 3$; противоречие. Поэтому $a=1$ и $\delta=+$, откуда $r_1 = r^2 = 3$; противоречие.

Аналогично приходим к противоречию и в случае, когда r_1 делит $q_1+\delta 2$.

4. Пусть $P \cong B_n(r)$ (r нечетно), $C_n(r)$, ${}^2D_n(r)$ ($n\geq 4$), ${}^2D_{n+1}(2)$ или ${}^2D_{n+1}(3)$, где $n = 2^m \geq 2$.

Пусть $P\cong C_n(r)$ и $n = 2^m\geq 2$. По лемме 1 имеем

$$\frac{r^n+1}{(2,r-1)} = \frac{q^6+\delta q^3+1}{d}.$$

Если $(2,r-1) = d = 1$, то $r^n+1 = q^6+\delta q^3+1$, откуда $r^n = q^3(q^3+\delta 1)$; противоречие.

Пусть $(2, r-1) = 2$ и $d = 1$. Тогда $r^n - 1 = 2q^3(q^3 + \delta 1)$. Положим $r_1 = r^{n/2}$. Тогда $(r_1 - 1)(r_1 + 1) = 2q^3(q^3 + \delta 1)$. Ясно, что $(r_1 - 1, r_1 + 1) = 2$. Поэтому q^3 делит либо $r_1 - 1$, либо $r_1 + 1$. Отсюда $r_1 + \varepsilon 1 = aq^3$ для некоторого $a \in \mathbb{N}$. Если $\varepsilon = -$, то $aq^3(aq^3 + 2) = 2q^3(q^3 + \delta 1)$, откуда $(a^2 - 2)q^3 = 2(\delta 1 - a)$ и, следовательно, $a = 1$ и $8 \leq q^3 = 2(1 - \delta 1) \leq 4$; противоречие. Если $\varepsilon = +$, то $aq^3(aq^3 - 2) = 2q^3(q^3 + \delta 1)$, откуда $(a^2 - 2)q^3 = 2(\delta 1 + a)$ и, следовательно, $a > 1$ и $8 \leq q^3 \leq 2(a+1)/(a^2 - 2) \leq 3$; противоречие.

Пусть $(2, r-1) = 1$ и $d = 3$. Тогда $3r^n = q^6 + \delta q^3 - 2$, откуда $3r^n = (q^3 - \delta 1)(q^3 + \delta 2)$. Так как $(q^3 - \delta 1, q^3 + \delta 2) = 3$, то r есть степень числа 3; противоречие.

Итак, $(2, r-1) = 2$ и $d = 3$. Поэтому $(r^n + 1)/2 = (q^6 + \delta q^3 + 1)/3$ и, следовательно, $(r^n - 1)/2 = (q^6 + \delta q^3 - 2)/3 = (q^3 - \delta 1)(q^3 + \delta 2)/3$. Ввиду леммы 6 в P существует элемент порядка $(r^n - 1)/2$. Значит, в L существует полупростой элемент порядка $(q^3 - \delta 1)(q^3 + \delta 2)/3$. Этот элемент принадлежит некоторому максимальному тору T группы L, поэтому $(q^3 - \delta 1)(q^3 + \delta 2)/3$ делит $|T|$. Но это по лемме 5 противоречит всем возможностям для $|T|$, так как $(q^3 + \delta 2, q^3 - \delta 1) = 3, (q^3 + \delta 2, q^3 + \delta 1) = (q^3 + \delta 2, q^4 - q^2 + 1) = 1, (q^3 + \delta 2, q^2 + 1) = (5, q - \delta 2), (q^3 + \delta 2, q^4 + 1) = (17, 2q - \delta 1), (q^3 + \delta 2, q^5 - \delta 1) = (33, q - \delta 4)$.

Аналогично приходим к противоречию и в случае, когда P изоморфна $B_n(r)$ (r нечетно) или ${}^2D_n(r) (n \geq 4)$.

Пусть $P \cong {}^2D_{n+1}(r)$, где $n = 2^m \geq 2$ и $r = 2, 3$. Если $r = 2$, то $2^{n-1} + 1 = (q^6 + \delta q^3 + 1)/d$, откуда $2^{n-1} = (q^6 + \delta q^3 + 1 - d)/d$ и, следовательно, 2^{n-1} равно $q^3(q^3 + \delta 1)$ при $d = 1$ и $(q^3 - \delta 1)(q^3 + \delta 2)/3$ при $d = 3$; противоречие. Пусть $r = 3$. Тогда $(q^6 + \delta q^3 + 1)/d \in \{(3^n + 1)/2, (3^{n+1} + 1)/4\}$.

Если $d = 1$, то, рассуждая, как в случае $P \cong C_n(r)$, придем к противоречию.

Итак, $d = 3$ и, следовательно,

$$(q^6 + \delta q^3 - 2)/3 = (q^3 - \delta 1)(q^3 + \delta 2)/3 \in \{(3^n - 1)/2, 3(3^n - 1)/4\}.$$

Это противоречит тому, что 27 делит $(q^3 - \delta 1)(q^3 + \delta 2)$.

5. Пусть p — нечетное простое число и $P \cong B_p(3), C_p(r) (r = 2, 3), {}^2D_p(3), D_p(r)$ $(p \geq 5, r = 2, 3, 5)$ или $D_{p+1}(r)$ $(r = 2, 3)$. Мы рассмотрим только случай, когда $P \cong C_p(r)$ и $r = 2, 3$, так как остальные указанные возможности рассматриваются аналогично. По лемме 1 имеем $(r^p - 1)/(2, r-1) = (q^6 + \delta q^3 + 1)/d$.

Пусть $r = 2$. Тогда $2^p - 1 = (q^6 + \delta q^3 + 1)/d$. Вычитая 1 из обеих частей последнего равенства, получим $2(2^{p-1} - 1) = (q^6 + \delta q^3 + 1)/d - 1$. Отсюда, $2(2^{p-1} - 1) = q^3(q^3 + \delta 1)$ при $d = 1$ и $2^{p-1} - 1 = (q^3 - \delta 1)(q^3 + \delta 2)/6$ при $d = 3$. В обоих случаях приходим к противоречию, как в случае 4.

Итак, $r = 3$, и, следовательно, $(3^p - 1)/2 = (q^6 + \delta q^3 + 1)/d$. Вычитая 1 из обеих частей последнего равенства, имеем $3(3^{p-1} - 1)/2 = (q^6 + \delta q^3 + 1)/d - 1$. Отсюда, $3(3^{p-1} - 1) = 2q^3(q^3 + \delta 1)$ при $d = 1$ и $3^{p-1} - 1 = 2(q^3 - \delta 1)(q^3 + \delta 2)/9$ при $d = 3$. В обоих случаях приходим к противоречию, как в случае 4.

6. Пусть $P \cong A_p^{\epsilon}(r)$, где p — нечетное простое число, $(r - \epsilon 1) \mid (p+1)$ и $(p, r) \neq (3, 3), (5, 2)$ при $\epsilon = -$. По лемме 1 имеем $(r^p - \epsilon 1)/(r - \epsilon 1) = (q^6 + \delta q^3 + 1)/d$. Вычитая 1 из обеих частей последнего равенства, получим $(r(r^{p-1} - 1))(r - \epsilon 1) = (q^6 + \delta q^3 + 1)/d - 1$.

Пусть $d = 1$. Тогда $r(r^{p-1} - 1) = q^3(q^3 + \delta 1)(r - \epsilon 1)$.

Пусть $(q, r) \neq 1$. Тогда $r = q^3$ и, значит, $r^{p-1} - 1 = (r + \delta 1)(r - \epsilon 1) \in \{(r \pm 1)^2, r^2 - 1\}$. Если $r^{p-1} - 1 = r^2 - 1$, то $p = 3$ и, следовательно, $q^3 - \epsilon 1$ делит 4, что невозможно. Равенство $r^{p-1} - 1 = (r \pm 1)^2$ невозможно, так как $r = q^3 \geq 8$.

Итак, $(q,r)=1$. Имеем $r(r^k-1)(r^k+1)=q^3(q^3+\delta 1)(r-\epsilon 1)$, где $2k=p-1$. Поскольку (r^k-1,r^k+1) делит 2, то q^3 делит r^k-1 или r^k+1.

Пусть q^3 делит r^k-1. Тогда $r^k-1=q^3a$ для некоторого $a\in\mathbb{N}$ и, следовательно, $(q^3+\delta 1)(r-\epsilon 1)=ra(q^3a+2)$, откуда $q^3(ra^2-r+\epsilon 1)=-r(2a-\delta 1)-\delta 1\cdot\epsilon 1$. Если $a>1$, то левая часть последнего равенства положительна, а правая отрицательна, что невозможно. Поэтому $a=1$ и, следовательно, $r^k-q^3=1$. Ввиду леммы 4 и условия $(r-\epsilon 1)\mid(p+1)$ это возможно лишь при $k=q=2$, $r=3$, $p=5$, что противоречит равенству $r(r^{p-1}-1)=q^3(q^3+\delta 1)(r-\epsilon 1)$.

Итак, q^3 делит r^k+1 . Тогда $r^k+1=q^3a$ для некоторого $a\in\mathbb{N}$ и, следовательно, $(q^3+\delta 1)(r-\epsilon 1)=ra(q^3a-2)$. Если $a>1$, то $r-\epsilon 1\le r+1<2r\le ra$ и $q^3+\delta 1\le q^3+1<2q^3-2\le q^3a-2$, что противоречит предыдущему равенству. Поэтому $a=1$ и, следовательно, $q^3-r^k=1$. Ввиду леммы 4 получаем $k=1$, откуда $p=3$, что противоречит условию $(r-\epsilon 1)\mid(p+1)$.

Таким образом, $d=3$, и, следовательно, $r(r^{p-1}-1)/(r-\epsilon 1)=(q^3-\delta 1)(q^3+\delta 2)/3$. Так как 9 делит $q^3-\delta 1$ и $q^3+\delta 2=(q^3-\delta 1)+3$, то $(q^3+\delta 2)/3=3$ и, следовательно, $(q^3-\delta 1,(q^3+\delta 2)/3)=1$. Поэтому r делит $q^3-\delta 1$ или $(q^3+\delta 2)/3$.

Предположим, что r делит $q^3-\delta 1$. Тогда

$$\frac{r^{p-1}-1}{r-\epsilon 1}=\frac{q^3-\delta 1}{r}\cdot\frac{q^3+\delta 2}{3}.$$

Ввиду леммы 6 в P существует элемент порядка $(q^3+\delta 2)/3$. Значит, в L существует полупростой элемент порядка $(q^3+\delta 2)/3$. Этот элемент принадлежит некоторому максимальному тору T группы L, поэтому $(q^3+\delta 2)/3$ делит $|T|$. Так как $(q^3+\delta 2)/3$ взаимно просто с q^6-1, q^4-q^2+1 и $q^6+\delta q^3+1$, $(q^3+\delta 2,q^2+1)=(5,q-\delta 2)$, $(q^3+\delta 2,q^4+1)=(17,2q-\delta 1)$ и $((q^3+\delta 2)/3,q^5-\delta 1)=(11,q-\delta 4)$, то по лемме 5 число $(q^3+\delta 2)/3$ делит одно из чисел $(5,q-\delta 2)^2$, $(17,2q-\delta 1)$, $(11,q-\delta 4)$, что невозможно.

Итак, r делит $(q^3+\delta 2)/3$. Тогда

$$\frac{r^{p-1}-1}{r-\epsilon 1}=(q^3-\delta 1)\cdot\frac{q^3+\delta 2}{3r}.$$

Ввиду леммы 6 в P существует элемент порядка $(q^3-\delta 1)\cdot\frac{q^3+\delta 2}{3r}$. Значит, в L существует полупростой элемент порядка $(q^3-\delta 1)\cdot\frac{q^3+\delta 2}{3r}$. Этот элемент принадлежит некоторому максимальному тору T группы L, поэтому $(q^3-\delta 1)\cdot\frac{q^3+\delta 2}{3r}$ делит $|T|$. Отсюда по лемме 5 имеем $\frac{q^3+\delta 2}{3r}=1$, т. е. $q^3+\delta 2=3r$. Поэтому $r^{p-1}-1=3(r-\delta 1)(r-\epsilon 1)$, что невозможно.

7. Пусть $P\cong A^{\epsilon}_{p-1}(r)$, где p — нечетное простое число, r — степень некоторого простого числа s и $(p,r)\ne(3,2),(3,4)$ при $\epsilon=+$. Тогда

$$\frac{r^p-\epsilon 1}{(r-\epsilon 1)(p,r-\epsilon 1)}=\frac{q^6+\delta q^3+1}{d},\tag{1}$$

откуда

$$\frac{r^p-\epsilon 1}{r-\epsilon 1}=\frac{(p,r-\epsilon 1)(q^6+\delta q^3+1)}{d}.$$

Вычитая 1 из обеих частей последнего равенства, получим

$$r\frac{r^{p-1}-1}{r-\epsilon 1}=\frac{(p,r-\epsilon 1)(q^6+\delta q^3+1)-d}{d},$$

откуда

$$\frac{r^{p-1}-1}{r-\epsilon 1} = \frac{(p, r-\epsilon 1)q^3(q^3+\delta 1)+(p, r-\epsilon 1)-d}{dr}. \tag{2}$$

Допустим, что $p = 3$. Тогда равенство (1) запишется в виде

$$\frac{r^2+\epsilon r+1}{(3, r-\epsilon 1)} = \frac{q_1^2+\delta q_1+1}{d},$$

где $q_1 = q^3$. Рассуждая, как в случае 1, получим, что $\epsilon = \delta$ и $r = q_1$. Тогда

$$\pi_1(P) = \pi(q(q^6-1)) \subseteq \pi_1(L) = \pi(q(q^5-\delta 1)(q^8-1)(q^{12}-1)).$$

Предположим, что порядок группы $\overline{G}/\operatorname{Inn}(P)$ делится на нечетное простое число $t > 3$. Тогда в $\overline{G}\setminus\operatorname{Inn}(P)$ существует элемент x порядка t, индуцирующий на P полевой автоморфизм, поэтому ввиду [21, (9–1)] имеем $O^{s'}(C_P(x)) \cong A_2^\epsilon(r_0)$, где $r_0^t = r$. В группе $A_2^\epsilon(r_0)$ есть элемент порядка $\frac{r_0^2+\epsilon r_0+1}{(3, r_0-\epsilon 1)}$, поэтому

$$\pi\left(\frac{r_0^2+\epsilon r_0+1}{(3, r_0-\epsilon 1)}\right) \subseteq \pi_1(L).$$

Но $\frac{r_0^2+\epsilon r_0+1}{(3, r_0-\epsilon 1)}$ делит $\frac{r^2+\epsilon r+1}{(3, r-\epsilon 1)}$; противоречие. Таким образом, $\overline{G}/\operatorname{Inn}(P)$ является $\{2,3\}$-группой. По теореме Жигмонди существуют простой делитель f_1 числа q^8-1, не делящий q^i-1 для всех $1 \le i < 8$, и простой делитель f_2 числа $q^{12}-1$, не делящий q^i-1 для всех $1 \le i < 12$. Поэтому $f_1, f_2 \in \pi(F(G))$. Так как подгруппа $F(G)$ нильпотентна, в ней найдется элемент порядка $f_1 f_2$. Значит, в L найдется полупростой элемент порядка $f_1 f_2$. Этот элемент содержится в некотором максимальном торе T группы L, и, значит, $f_1 f_2$ делит $|T|$. Но это по лемме 5 противоречит всем возможностям для $|T|$. Поэтому

$$p \ge 5. \tag{3}$$

Предположим, что $(p, r-\epsilon 1) = 1$. Тогда равенство (2) запишется в виде

$$\frac{r(r^{p-1}-1)}{r-\epsilon 1} = \frac{q^3(q^3+\delta 1)+1-d}{d}.$$

Допустим, что $d = 1$. Тогда $r(r^{p-1}-1) = q^3(q^3+\delta 1)(r-\epsilon 1)$. Если $(r, q) \ne 1$, то $r = q^3$ и, следовательно, $r^{p-1}-1 = (r+\delta 1)(r-\epsilon 1) \in \{(r\pm 1)^2, r^2-1\}$, что противоречит условию (3). Поэтому $(r, q) = 1$. Теперь, рассуждая, как в случае 6, придем к противоречию.

Поэтому $d = 3$ и, следовательно, $3(r^{p-1}-1) = (q^3-\delta 1)(q^3+\delta 2)(r-\epsilon 1)$. Опять, рассуждая, как в случае 6, придем к противоречию. Таким образом,

$$(p, r-\epsilon 1) = p. \tag{4}$$

Оценим число r сверху некоторой функцией от q. Если $\epsilon = +$, то из (1) и (4) следует, что

$$\frac{2q^6}{d} > \frac{q^6+\delta q^3+1}{d} = \frac{r^p-1}{(r-1)p} > \frac{r^p-1}{(r-1)r} > r^{p-2}.$$

Пусть $\epsilon = -$. Тогда из (1) и (4) вытекает, что

$$\frac{2q^6}{d} > \frac{q^6+\delta q^3+1}{d} - \frac{1}{p} = \frac{r(r-1)}{p(r+1)} \cdot \frac{r^{p-1}-1}{r-1} > \frac{r(r-1)}{p(r+1)} \cdot r^{p-2}.$$

Если $3 \neq r+1 \neq p$, то легко показывается, что $r(r-1)/(p(r+1)) > 1$ и, следовательно, $2q^6/d > r^{p-2}$. Из (3) и (4) получим, что $3 \neq r+1$.

Предположим, что $r+1 = p$. Тогда

$$\frac{r(r-1)}{p(r+1)} = \frac{p^2-3p+2}{p^2}.$$

Число $\frac{10}{9}q^6 - (q^6+\delta q^3+1) = \frac{q^3(q^3-\delta 9)-9}{9}$ положительно, если $q \geq 3$ или $\delta = -$. Если $q = 2$ и $\delta = +$, то из (1) следует, что $\frac{r^p+1}{(r+1)^2} = 73$, а это невозможно. Поэтому

$$\frac{10q^6}{9d} > \frac{p^2-3p+2}{p^2} \cdot r^{p-2}, \quad \text{откуда} \quad \frac{2q^6}{d} > \frac{9(p^2-3p+2)}{5p^2} \cdot r^{p-2}.$$

Если $p \geq 7$, то $9(p^2-3p+2)/5p^2 > 1$ и, следовательно, $2q^6/d > r^{p-2}$. В случае $p = 5$ получаем $r = 4$, что противоречит равенству (2). Итак, в любом случае имеем

$$r^{p-2} < 2q^6/d. \tag{5}$$

Допустим, что $(r,q) \neq 1$. Тогда ввиду (2) и (4) число r делит $pq^3(q^3+\delta 1) + p-d$. Если $r \geq q^3$, то в силу (5) получаем $p = 3$, что противоречит (3). Поэтому $r < q^3$ и, следовательно, r делит $p-d$, что противоречит (4). Таким образом,

$$(r,q) = 1. \tag{6}$$

Положим $f = pq^3(q^3+\delta 1)+p-d$ и $q_1 = f_u$, где u — простой делитель числа q. Тогда ввиду (2), (4) и (6) имеем

$$\frac{r^{p-1}-1}{r-\epsilon 1} = \frac{f}{dr}, \quad q_1 = \left(\frac{f}{dr}\right)_u = (p-d)_u.$$

По лемме 6 в L есть полупростой элемент порядка $\frac{f}{rq_1 d}$. Этот элемент содержится в некотором максимальном торе T группы L, поэтому $\frac{f}{drq_1}$ делит $(f/d, |T|)$. Сначала оценим сверху наибольший общий делитель числа f с возможными ввиду леммы 5 делителями $q^3 \pm 1, q^2+1, q^4+1, q^4-q^2+1$ и $(q^5-\delta 1)/(q-\delta 1)$ числа $d|T|$ (заметим, что по (1) и (2) число f/d взаимно просто с $(q^6+\delta q^3+1)/d$). Согласно (3) число p не делит f. Теперь непосредственными вычислениями с применением алгоритма Евклида получаем, что

$(f, q^3+\delta 1)$ делит $(p-d)/q_1$;

$(f, q^3-\delta 1)$ делит $3p-d$;

(f, q^2+1) и (f, q^4-q^2+1) делят p^2+d^2;

(f, q^4+1) делит $p^4-4p^3+8p^2-4p+1$ при $d=1$ и $p^4-12p^3+72p^2-108p+81$ при $d=3$;

$(f, (q^5-\delta 1)/(q-\delta 1))$ делит $p^4-3p^3+4p^2-2p+1$ при $\delta = +$ и $d=1$, p^4-3p^3+81 при $\delta = +$ и $d = 3$, $p^4-3p^3+4p^2-4p+1$ при $\delta = -$ и $d=1$ и $p^4-6p^3+9p^2-54p+243$ при $\delta = -$ и $d = 3$.

Отсюда, применяя лемму 5 и учитывая, что в случае $|T| = (q-\delta 1)^6/d$ экспонента подгруппы T не превосходит $q-\delta 1$, получим, что

$$\text{число } \frac{f}{rq_1} \text{ не превосходит } \frac{(3p-d)^5(p-d)}{q_1} \text{ или } (3p-d)^2(p^2+d^2)^2. \tag{7}$$

Предположим, что $p \geq 17$. Тогда по (4) имеем $p \leq r+1$ и, следовательно, $r \geq 16$. Если $\frac{f}{rq_1} \leq \frac{(3p-d)^5(p-d)}{q_1}$, то

$$f \leq 3^5 r(p-d)(p-d/3)^5 \leq 3^5 r(p-1)(r+1)^5 < 3^5 r^8 < r^{10},$$

так как $(r+1)^5 < r^6$ и $3^5 < 16^2 \leq r^2$. Если $\frac{f}{rq_1} \leq (3p-d)^2(p^2+d^2)^2$, то

$$f \leq 9r(p-d)(p-d/3)^2(p^2+d^2)^2 \leq 9r^2(r+1)^2((r+1)^2+9)^2 < 9r^{10} < r^{11},$$

поскольку $(r+1)^2+9 < r^3$ и $(r+1)^2 < r^3$. В любом случае получаем $f < r^{11}$. Но ввиду (5) имеем $r^{11} < 2^{11/(p-2)}q^{66/(p-2)} \leq 2^{11/15}q^{66/15} < 2q^5$, что противоречит неравенству $f - 2q^5 > 0$.

Таким образом, $p < 17$, откуда ввиду (3) имеем $p \in \{5, 7, 11, 13\}$.

Пусть $p = 13$. Тогда $r - \epsilon 1 \neq p$ и, следовательно, по (4) имеем $r - \epsilon 1 \geq 2p$, откуда $p \leq (r+1)/2$ и $r \geq 25$. Если $\frac{f}{rq_1} \leq \frac{(p-d)(3p-d)^5}{q_1}$, то

$$\begin{aligned} f \leq r(p-d)(3p-d)^5 &\leq 3^5 r((r+1)/2-d)((r+1)/2-d/3)^5 \\ &< 243r(r-1)(r+1)^5/64 < 243r^8/64 < r^9/6, \end{aligned}$$

так как $(r+1)^5 < r^6$ и $r \geq 25$. Но в силу (5) имеем $r^9/6 < 2^{9/11}q^{54/11}/6 < q^5/3$, что противоречит неравенству $f - q^5/3 > 0$. Если $\frac{f}{rq_1} \leq (3p-d)^2(p^2+d^2)^2$, то

$$\begin{aligned} f \leq 9r(p-d)(p-d/3)^2(p^2+d^2)^2 &\leq 9r((r+1)/2-d)((r+1)/2-d/3)^2(((r+1)/2)^2+d^2)^2 \\ &< 9r(r-1)(r+1)^2((r+1)^2+36)^2 < 9r^{11}/128, \end{aligned}$$

поскольку $(r+1)^2 < r^3$ и $(r+1)^2+36 < r^3$, поэтому ввиду (5) имеем $f < 9q^{66/11}/64 < q^6/6$, что противоречит неравенству $f - q^6/6 > 0$.

Пусть $p = 11$. Тогда в силу (4) имеем $p \leq (r-1)/2$ и $r \geq 23$. Если $\frac{f}{rq_1} \leq \frac{(p-d)(3p-d)^5}{q_1}$, то

$$\begin{aligned} f \leq r(p-d)(3p-d)^5 &\leq 3^5 r((r-1)/2-d)((r-1)/2-d/3)^5 \\ &< 243r(r-1)^6/64 < 243r^7/64 < r^8/5, \end{aligned}$$

так как $r \geq 23$, поэтому ввиду (5) имеем $f < r^8/5 < 2^{8/9}q^{48/9}/5 < 2q^6/5$, что противоречит неравенству $f - 2q^6/5 > 0$. Таким образом, $\frac{f}{rq_1} \leq (33-d)^2(121+d^2)^2$. Если $d = 3$, то $q_1 \in \{1, 8\}$ и $f/r \leq 8 \cdot 30^2 \cdot 130^2 = 121680000$. Если $d = 1$, то $q_1 \in \{1, 2, 5\}$ и $f/r \leq 5 \cdot 32^2 \cdot 122^2 < 121680000$. Поэтому $f/r \leq 121680000$. Но $121680000 < 23^6 = 148036089 \leq r^6$, следовательно, $f < r^7$. С учетом (5) имеем $f < r^7 < 2^{7/9}q^{42/9} < 2q^5$, что противоречит неравенству $f - 2q^5 > 0$.

Пусть $p = 7$. Тогда ввиду (7) число $\frac{f}{rq_1}$ не превосходит $\frac{(7-d)(21-d)^5}{q_1}$ или $(21-d)^2(49+d^2)^2$. Если $d = 3$, то $q_1 \in \{1, 4\}$ и $f/r \leq \max\{4 \cdot 18^5, 4 \cdot 58^2 \cdot 18^2\} = 7558272 < 76 \cdot 10^5$. Если $d = 1$, то $q_1 \in \{1, 2, 3\}$ и $f/r \leq \max\{6 \cdot 20^5, 3 \cdot 50^2 \cdot 20^2\} = 192 \cdot 10^5$. Так как в силу (2) имеем $f/dr = (r^6-1)/(r-\epsilon 1)$, отсюда следует, что $(r^6-1)/(r-\epsilon 1) \leq 192 \cdot 10^5$, поэтому $r^5/2 < (r^6-1)/(r-\epsilon 1) \leq 192 \cdot 10^5$, т. е. $r < 40$. В силу того, что r — степень простого числа и $r - \epsilon 1$ делится на 7, пара (r, ϵ) — одна из следующих: $(8, +)$, $(13, -)$, $(27, -)$, $(29, +)$. Поскольку $r(r+\epsilon 1)$ делит f/d и делится на 3, имеем $d = 3$ и, значит,

$$7q^3(q^3+\delta 1) = 3r(r^6-1)/(r-\epsilon 1) - 4 \in \{898772, 13446104, 1120752122, 1827318416\}.$$

Кроме того, как мы видели выше, $f/r < 76 \cdot 10^5$, и, значит, $f < r \cdot 76 \cdot 10^5 \leq 29 \cdot 76 \cdot 10^5 = 2204 \cdot 10^5 < 221 \cdot 10^6$. Но $13q^6/3 < f$, поэтому $q^6 < 663 \cdot 10^6/13 = 51 \cdot 10^6$ и, следовательно, $q < 20$. Так как 898772 не делится на 7, $13446104 = 2^3 \cdot 7 \cdot 240109$, $1120752122 = 2^2 \cdot 7 \cdot 19 \cdot 2106677$, $1827318416 = 2^4 \cdot 7 \cdot 11 \cdot 1483213$ и числа 240109, 2106677, 1483213 не имеют простых делителей, меньших 20, то $q = 2$; противоречие с неравенством (5).

Итак, $p = 5$. Тогда ввиду (7) число $\frac{f}{rq_1}$ не превосходит $\frac{(5-d)(15-d)^5}{q_1}$ или $(15-d)^2(25+d^2)^2$. Если $d = 3$, то $q_1 \in \{1, 2\}$ и $f/r \leq \max\{2 \cdot 12^5, 2 \cdot 34^2 \cdot 12^2\} = 497664$. Если $d = 1$, то $q_1 \in \{1, 2, 4\}$ и $f/r \leq \max\{4 \cdot 14^5, 4 \cdot 26^2 \cdot 14^2\} = 2151296$. Так как в силу (2) имеем $f/dr = (r^4-1)/(r-\epsilon 1) = (r^2+1)(r+\epsilon 1)$, отсюда следует, что $(r^2+1)(r-1) \leq 2151296$, поэтому $r < 129$. Поскольку r — степень простого числа и $r-\epsilon 1$ делится на 5, пара (r, ϵ) — одна из следующих: $(4, -)$, $(9, -)$, $(11, +)$, $(16, +)$, $(19, -)$, $(29, -)$, $(31, +)$, $(41, +)$, $(49, -)$, $(61, +)$, $(64, -)$, $(71, +)$, $(79, -)$, $(81, +)$, $(89, -)$, $(101, -)$, $(109, -)$, $(121, +)$. В частности, $r \leq 121$. Из полученной выше информации о наибольших общих делителях числа f с числами $q^3 \pm 1, q^2 + 1, q^4 + 1, q^4 - q^2 + 1$, $(q^5 - \delta 1)/(q - \delta 1)$ и $(q^6 + \delta q^3 + 1)$ непосредственно получаем, что $\pi(f) \subseteq \{2, 3, 7, 11, 31\}$. Поэтому пара (r, ϵ) — одна из следующих: $(4, -)$, $(9, -)$, $(11, +)$, $(16, +)$, $(31, +)$, $(49, -)$, $(59, -)$, $(64, -)$, $(81, +)$. С использованием элементарной теории сравнений легко видеть, что 9 не делит f. Поэтому $9 \neq r \neq 81$. Так как $(r^2 + 1)(r + \epsilon 1)$ делит f, то f делится на простые числа 17, 61, 17, 13, 1201 и 17, когда пара (r, ϵ) равна $(4, -), (11, +), (16, +), (31, +), (49, -)$ и $(64, -)$ соответственно, что невозможно.

8. Пусть $P \cong A_1(r)$, $r > 3$.

Допустим, что $r = 2^b$ для некоторого $b \in \mathbb{N}$. Тогда $(q^6 + \delta q^3 + 1)/d \in \{2^b - 1, 2^b + 1\}$.

Предположим, что $(q^6 + \delta q^3 + 1)/d = 2^b + 1$. Если $d = 1$, то $q^3(q^3 + \delta 1) = 2^b$, что невозможно. Поэтому $d = 3$ и $(q^3 - \delta 1)(q^3 + \delta 2) = 3 \cdot 2^b$, а это противоречит тому, что 27 делит левую часть последнего равенства.

Таким образом, $(q^6 + \delta q^3 + 1)/d = 2^b - 1$.

Пусть $d = 1$. Тогда из предыдущего равенства следует, что $q^3(q^3 + \delta 1) = 2(2^{b-1} - 1)$ и, в частности, q нечетно.

Предположим, что b нечетно. Тогда $b - 1 = 2k$ для некоторого $k \in \mathbb{N}$ и, следовательно, q^3 делит $2^k - \epsilon 1$ для некоторого $\epsilon \in \{+, -\}$, т. е. $2^k - \epsilon 1 = q^3 a$ для некоторого $a \in \mathbb{N}$. Тогда $q^3(q^3 + \delta 1) = 2q^3 a(q^3 a + \epsilon 2)$, откуда $(2a^2 - 1)q^3 = \delta 1 - \epsilon 4a$. Левая часть последнего равенства больше 1, следовательно, $\epsilon = -$ и $27 \leq q^3 = (\delta 1 + 4a)/(2a^2 - 1) \leq 5$; противоречие.

Поэтому b четно, т. е. $b = 2k$ для некоторого $k \in \mathbb{N}$. Но тогда, вычитая 3 из обеих частей исходного равенства, получим $(q^3 - \delta 1)(q^3 + \delta 2) = 4(4^{k-1} - 1)$. Так как 3 не делит левую часть последнего равенства, но делит его правую часть, получаем противоречие.

Таким образом, $d = 3$, и, следовательно, $(q^6 + \delta q^3 + 1)/3 = 2^b - 1$. Прибавив 2 к обеим частям последнего равенства, получим $(q^6 + \delta q^3 + 7)/3 = 2^b + 1$. В P есть элемент порядка $2^b + 1$. Значит, и в L есть полупростой элемент порядка $(q^6 + \delta q^3 + 7)/3$. Поэтому $(q^6 + \delta q^3 + 7)/3$ делит порядок некоторого максимального тора группы L, что противоречит лемме 5.

Таким образом, $r \equiv \epsilon 1(4)$ и $r = s^b$, где s — простое число и $b \in \mathbb{N}$. Тогда $(q^6 + \delta q^3 + 1)/d \in \{s, (r + \epsilon 1)/2\}$.

Предположим, что $(q^6 + \delta q^3 + 1)/d = s$.

Пусть $d = 1$. Тогда $(q^6 + \delta q^3 + 2)/2 = (s + 1)/2$. Если b четно, то $(s^2 - 1)/2$

делит $(r-1)/2$. Если b нечетно, то $(s+1)/2$ делит $(r+1)/2$. В любом случае в P, а значит, и в L есть элемент порядка $(s+1)/2=(q^6+\delta q^3+2)/2$. Так как q взаимно просто с $(q^6+\delta q^3+2)/2$, то $f:=(q^6+\delta q^3+2)/2$ делит порядок некоторого максимального тора группы L. Это противоречит лемме 5, ибо число f взаимно просто с числами q^4-q^2+1 и $q^6+\delta q^3+1$, (f,q^6-1) делит 8, $(f,q^2+1)=(2,q^2+1)$, $(f,q^4+1)=(2,q^4+1)$ и $(f,(q^5-\delta 1)/(q-\delta 1))=(11,q+\delta 6)$.

Таким образом, $d=3$, и, следовательно, $(q^6+\delta q^3+1)/3=s$. Отсюда $(q^6+\delta q^3-2)/6=(s-1)/2$ и тем самым $(q^3-\delta 1)(q^3+\delta 2)/6=(s-1)/2$. Так как $(s-1)/2$ делит $(r-1)/2\in\omega(P)$, то в L есть полупростой элемент порядка $(q^3-\delta 1)(q^3+\delta 2)/6$. Рассуждая, как в п. 4, придем к противоречию.

Итак, $(q^6+\delta q^3+1)/d=(r+\epsilon 1)/2$. Пусть $d=1$. Тогда $q^6+\delta q^3+1=(r+\epsilon 1)/2$. Если $\epsilon=-$, то $q^6+\delta q^3+2=(r+1)/2\in\omega(P)$, и, рассуждая, как в предыдущем абзаце, придем к противоречию. Поэтому $\epsilon=+$ и $q^6+\delta q^3+1=(r+1)/2$. Отсюда $q^3(q^3+\delta 1)=(r-1)/2$ и $r=2q^3(q^3+\delta 1)+1$. По лемме 1 имеем $\pi(P)=\pi(r(r^2-1))$ и $\pi_1(G)=\pi(q(q^5-\delta 1)(q^8-1)(q^{12}-1))$. Предположим, что порядок группы $\overline{G}/\operatorname{Inn}(P)$ делится на нечетное простое число t. Тогда в $\overline{G}\setminus\operatorname{Inn}(P)$ существует элемент x порядка t и в силу [21, (9–1)] имеем $O^{s'}(C_P(x))\cong L_2(r_0)$, где $r_0^t=r$. В группе $L_2(r_0)$ есть элемент порядка $(r_0+1)/2$. Но $t\in\pi_1(G)$ и $(r_0+1)/2$ делит $(r+1)/2=q^6+\delta q^3+1$; противоречие. Таким образом, $\overline{G}/\operatorname{Inn}(P)$ является 2-группой. Легко показывается, что

$$\pi((q^2+1)(q^4+1)/(2,q-1)^2)\cap\pi(q(q^6-1))=\varnothing.$$

Так как (q^4+1,q^2+1) делит 2, $(r,q^4+1)=1$, а (r,q^2+1) делит 5, то $\pi((q^2+1)(q^4+1)/(2,q-1)^2)\setminus\{5\}\subseteq\pi(F(G))$. Предположим, что $q^2+1=5^t$ для некоторого $t\in\mathbb{N}$. Тогда ввиду леммы 4 получаем, что $t=1$ и $q=2$, откуда $r=2q^3(q^3+\delta 1)+1\in\{113,145\}$ и, следовательно, $r=113$ и $\delta=-$. Но тогда $d=3$; противоречие с предположением. Аналогично ввиду леммы 4 число q^4+1 не может быть степенью 5. Так как подгруппа $F(G)$ нильпотентна, то в ней найдется элемент порядка s_1s_2, где $s_1\in\pi((q^2+1)/(2,q-1))\setminus\{5\}$, $s_2\in\pi((q^4+1)/(2,q-1))\setminus\{5\}$. Значит, и в L найдется полупростой элемент порядка s_1s_2. Этот элемент содержится в некотором максимальном торе T группы L и, значит, s_1s_2 делит $|T|$. Но это по лемме 5 противоречит всем возможностям для $|T|$.

Итак, $d=3$. Тогда $(q^6+\delta q^3+1)/3=(r+\epsilon 1)/2$. Вычитая $\epsilon 1$ из обеих частей последнего равенства, получим $(q^6+\delta q^3+1-\epsilon 3)/3=(r-\epsilon 1)/2$. Так как $(r-\epsilon 1)/2\in\omega(P)$, то в L есть полупростой элемент порядка $(q^6+\delta q^3+1-\epsilon 3)/3$. Рассуждая, как в п. 4, придем к противоречию.

9. Пусть $P\cong {}^2F_4(r)$, $r=2^{2m+1}>2$. Тогда

$$(q^6+\delta q^3+1)/d=r^2+\epsilon\sqrt{2r^3}+r+\epsilon\sqrt{2r}+1.$$

Пусть $d=1$. Тогда

$$q^3(q^3+\delta 1)=r^2+\epsilon\sqrt{2r^3}+r+\epsilon\sqrt{2r}=2^{m+1}(2^{3m+1}+\epsilon 2^{2m+1}+2^m+\epsilon 1).$$

Если q четно, то $q^3=2^{m+1}$, откуда $2^{m+1}+\delta 1=2^{3m+1}+\epsilon 2^{2m+1}+2^m+\epsilon 1$, что невозможно. Поэтому q нечетно и 2^{m+1} делит $q^3+\delta 1=(q+\delta 1)(q^2-\delta q+1)$. Ясно, что 2^{m+1} делит $q+\delta 1$, т. е. $q+\delta 1=2^{m+1}b$ для некоторого $b\in\mathbb{N}$. Поэтому

$$(2^{m+1}b-\delta 1)^3((2^{m+1}b-\delta 1)^3+\delta 1)=2^{m+1}(2^{3m+1}+\epsilon 2^{2m+1}+2^m+\epsilon 1).$$

Если $b>1$, то

$$\begin{aligned}(2^{m+1}b-\delta 1)^3((2^{m+1}b-\delta 1)^3+\delta 1)&\geq(2^{m+2}-1)^3((2^{m+2}-1)^3-1)\\&=(2^{m+1}+(2^{m+1}-1))^3((2^{m+1}+(2^{m+1}-1))^3-1)>2^{6m+6}.\end{aligned}$$

Отсюда $2^{m+1}(2^{3m+1}+\epsilon 2^{2m+1}+2^m+\epsilon 1) > 2^{6m+6}$ и, следовательно, $2^{3m+1}+\epsilon 2^{2m+1}+2^m+\epsilon 1 > 2^{5m+5}$. Но

$$\begin{aligned}2^{5m+5}-(2^{3m+1}+\epsilon 2^{2m+1}+2^m+\epsilon 1) &\geq 2^{5m+5}-(2^{3m+1}+2^{2m+1}+2^m+1)\\ &= (2^{5m+4}-2^{3m+1})+(2^{5m+3}-2^{2m+1})+(2^{5m+3}-2^m)-1\\ &= 2^{3m+1}(2^{2m+3}-1)+2^{2m+1}(2^{3m+2}-1)+2^m(2^{4m+3}-1)-1>0;\end{aligned}$$

противоречие. Поэтому $b=1$. Имеем

$$(2^{m+1}-\delta 1)^3((2^{m+1}-\delta 1)^3+\delta 1) \geq (2^m+(2^m-1))^3(2^m+(2^m-1))^3-1 > 2^{6m-1}.$$

Отсюда $2^{m+1}(2^{3m+1}+\epsilon 2^{2m+1}+2^m+\epsilon 1) > 2^{6m-1}$ и, следовательно,

$$2^{3m+1}+\epsilon 2^{2m+1}+2^m+\epsilon 1 > 2^{5m-2}.$$

Если $m>1$, то

$$\begin{aligned}&2^{5m-2}-(2^{3m+1}+\epsilon 2^{2m+1}+2^m+\epsilon 1)\\ &\quad\geq (2^{5m-3}-2^{3m+1})+(2^{5m-4}-2^{2m+1})+(2^{5m-4}-2^m)-1\\ &\quad= 2^{3m+1}(2^{2m-4}-1)+2^{2m+1}(2^{3m-5}-1)+2^m(2^{4m-4}-1)>0;\end{aligned}$$

противоречие. Поэтому $m=1$ и, следовательно, $(q,\delta)\in\{(3,+),(5,-)\}$. Если $(q,\delta)=(5,-)$, то $q-\delta 1=6$ делится на 3, что противоречит предположению. Поэтому $q=3$ и $\delta=+$, что противоречит равенству

$$(2^{m+1}-\delta 1)^3((2^{m+1}-\delta 1)^3+\delta 1)=2^{m+1}(2^{3m+1}+\epsilon 2^{2m+1}+2^m+\epsilon 1).$$

Итак, $d=3$. Тогда $(q^6+\delta q^3+1)/3=r^2+\epsilon\sqrt{2r^3}+r+\epsilon\sqrt{2r}+1$. Вычитая 1 из обеих частей последнего равенства, получим

$$(q^3-\delta 1)(q^3+\delta 2)/3=2^{m+1}(2^{3m+1}+\epsilon 2^{2m+1}+2^m+\epsilon 1).$$

Рассуждая, как в случае $d=1$, приходим к противоречию.

10. Пусть $P\cong E_8(r)$, где $r=s^b$, s — простое число и $b\in\mathbb{N}$. Тогда

$$\frac{q^6+\delta q^3+1}{d}\in\left\{\frac{r^{10}+r^5+1}{r^2+r+1},\frac{r^{10}+1}{r^2+1},r^8-r^4+1,\frac{r^{10}-r^5+1}{r^2-r+1}\right\}.$$

Пусть сначала $(q^6+\delta q^3+1)/d=r^8-r^4+1$.

Предположим, что $d=1$. Тогда $q^3(q^3+\delta 1)=r^4(r^4-1)$. Если $(q,r)\neq 1$, то $q^3=r^4$, но это противоречит тому, что

$$\pi(q^9-1)\subseteq\pi_1(P)\subseteq\pi_1(L)=\pi(q(q^5-\delta 1)(q^8-1)(q^{12}-1)),$$

так как q^9-1 взаимно просто с $(q^5-\delta 1)(q^8-1)$ и $(q^9-1,q^{12}-1)=q^3-1$, а по теореме Жигмонди существует простой делитель числа q^9-1, не делящий q^i-1 при $1\leq i<9$. Поэтому $(q,r)=1$ и, следовательно, q^3 делит r^4-1 и r^4 делит $q^3+\delta 1$, т. е. $r^4-1=q^3a$ и $q^3+\delta 1=r^4b$ для некоторых $a,b\in\mathbb{N}$. Но тогда $q^3+\delta 1=(q^3a+1)b$, откуда $a=b=1$ и $\delta=+$, т. е. $q^3+1=r^4$, что противоречит лемме 4.

Таким образом, $d=3$. Тогда $(q^3-\delta 1)(q^3+\delta 2)=3r^4(r^4-1)$. Так как 9 делит $q^3-\delta 1$ и $(q^3-\delta 1,q^3+\delta 2)=3$, то r^4 делит либо $q^3-\delta 1$, либо $q^3+\delta 2$. В первом случае $q^3-\delta 1=r^4a$ для некоторого $a\in\mathbb{N}$, откуда $r^4a(r^4a+\delta 3)=3r^4(r^4-1)$ и, следовательно, $(a^2-3)r^4=-3(\delta a+1)$. Но тогда $a=1$ и $\delta=+$, т. е. $q^3-1=r^4$, что противоречит лемме 4. Во втором случае $q^3 + \delta 2 = r^4 a$ для некоторого $a \in \mathbb{N}$, откуда $r^4 a(r^4 a - \delta 3) = 3r^4(r^4 - 1)$ и, следовательно, $(a^2 - 3)r^4 = 3(\delta a - 1)$. Но тогда $a = 1$ и $\delta = -$, т. е. $r^4 = 3$; противоречие.

Пусть теперь $(q^6 + \delta q^3 + 1)/d = (r^{10} + 1)/(r^2 + 1)$.

Предположим, что $d = 1$. Тогда $q^3(q^3 + \delta 1) = r^2(r^4 + 1)(r^2 - 1)$. Если $(q, r) \neq 1$, то $q^3 = r^2$ и, следовательно, $r^2 + \delta 1 = (r^4 + 1)(r^2 - 1)$; противоречие. Поэтому $(q, r) = 1$. Допустим, что q четно. Тогда r нечетно и $(r^4 + 1, r^2 - 1) = (r^4 + 1, 2) = 2$, откуда q^3 делит $2(r^2 - 1)$, т. е. $2(r^2 - 1) = q^3 a$ для некоторого $a \in \mathbb{N}$. Следовательно, $r^2 = (q^3 a + 2)/2$ и $q^3(q^3 + \delta 1) = (q^3 a + 2)/2(((q^3 a + 2)/2)^2 + 1)q^3 a/2$; противоречие. Поэтому q нечетно и тем самым q^3 делит либо $r^4 + 1$, либо $r^2 - 1$. Если q^3 делит $r^2 - 1$, то $q^3 + \delta 1 \leq r^2$ и, значит, $q^3(q^3 + \delta 1) < r^2(r^4 + 1)(r^2 - 1)$; противоречие. Поэтому q^3 делит $r^4 + 1$, т. е. $r^4 + 1 = q^3 a$ для некоторого $a \in \mathbb{N}$. Имеем $(r^4 + 1)(r^4 + 1 + \delta a) = a^2 r^2 (r^4 + 1)(r^2 - 1)$, откуда $(a^2 - 1)r^4 - a^2 r^2 = 1 + \delta a$. Если $a = 1$, то $-r^2 = 1 + \delta 1 \geq 0$; противоречие. Поэтому $a > 1$ и $r^2((a^2 - 1)r^2 - a^2) = 1 + \delta a$, откуда

$$8 < 4\left(4 - 1 + \frac{1}{a^2 - 1}\right) \leq r^2\left(r^2 - \frac{a^2}{a^2 - 1}\right) = \frac{1 + \delta a}{a^2 - 1} \leq \frac{1}{a - 1} \leq 1;$$

противоречие.

Таким образом, $d = 3$. Тогда $(q^3 - \delta 1)(q^3 + \delta 2) = 3r^2(r^4 + 1)(r^2 - 1)$. Число q нечетно, так как в противном случае 2-часть числа $(q^3 - \delta 1)(q^3 + \delta 2)$ равна 2, откуда r нечетно и, следовательно, 8 делит $r^2 - 1$; противоречие. Известно, что $A_8(r) < E_8(r)$ (см., например, [22]). По лемме 6(а) в $A_8(r)$ есть элемент порядка $(r^8 - 1)/(9, r - 1)$, а значит, есть элемент порядка $(r^4 + 1)(r^2 - 1)/(9, r - 1)$. Пусть n — наибольший общий делитель чисел $(q^3 + \delta 2)/3$ и $(r^4 + 1)(r^2 - 1)/(9, r - 1)$. Тогда L содержит полупростой элемент порядка n, поэтому n делит порядок некоторого максимального тора в L. Легко проверить, что $((q^3 + \delta 2)/3, q^6 - 1) = ((q^3 + \delta 2)/3, q^6 + \delta q^3 + 1) = 1$, $(q^3 + \delta 2, q^2 + 1)$ и $(q^3 + \delta 2, q^4 - q^2 + 1)$ делят 5, $(q^3 + \delta 2, q^4 + 1)$ делит 17 и $(q^3 + \delta 2, (q^5 - \delta 1)/(q - \delta 1))$ делит 11. Поэтому ввиду леммы 5 получаем $n \in \{1, 5, 11, 17, 25\}$. Легко проверить, что $r^4 + 1$ не делится на 5 и 11.

Предположим, что $(q^3 + \delta 2, r^4 + 1) = 1$. Тогда $r^4 + 1$ делит $q^3 - \delta 1$, т. е. $q^3 - \delta 1 = (r^4 + 1)a$ для некоторого $a \in \mathbb{N}$. Отсюда $(r^4 + 1)a((r^4 + 1)a + \delta 3) = 3r^2(r^4 + 1)(r^2 - 1)$ и, следовательно, $(a^2 - 3)r^4 = -3r^2 - \delta 3a - a^2$. Если $a = 1$, то $-2r^4 = -3r^2 - \delta 3 - 1$; противоречие. Поэтому $a > 1$ и, значит,

$$4 \leq r^2 = \frac{-3r^2 - \delta 3a - a^2}{r^2(a^2 - 3)} \leq \frac{-3}{a^2 - 3} + \frac{3a}{r^2(a^2 - 3)} - \frac{a^2}{r^2(a^2 - 3)} < \frac{3a}{r^2(a^2 - 3)} < 2;$$

противоречие.

Таким образом, $n = (q^3 + \delta 2, r^4 + 1) = 17$. Отсюда $((q^3 + \delta 2)/3, (r^4 + 1)(r^2 - 1)) = 17$ и, следовательно, $q^3 - \delta 1 = (r^4 + 1)(r^2 - 1)a/17$ для некоторого $a \in \mathbb{N}$. Имеем $(r^4 + 1)(r^2 - 1)a((r^4 + 1)(r^2 - 1)a + \delta 51) = 3 \cdot 17^2 r^2 (r^4 + 1)(r^2 - 1)$, поэтому $a((r^4 + 1)(r^2 - 1)a + \delta 51) = 3 \cdot 17^2 r^2$. Отсюда легко видеть, что $a = 1$ и $r \leq 5$. Теперь из делимости на 17 числа $r^4 + 1$ получаем $r = 2$. Но тогда $q^3 - \delta 1 = 3$, что невозможно.

Итак, $(q^6 + \delta q^3 + 1)/d = (r^{10} + \epsilon r^5 + 1)/(r^2 + \epsilon r + 1)$.

Предположим, что $d = 1$. Тогда $q^3(q^3 + \delta 1) = r(r^4 - 1)(r^3 - \epsilon r^2 + \epsilon 1)$. Если $(q, r) \neq 1$, то $q^3 = r$ и, следовательно, $r + \delta 1 = (r^4 - 1)(r^3 - \epsilon r^2 + \epsilon 1)$, что невозможно. Поэтому $(q, r) = 1$. Так как $(r^3 - \epsilon r^2 + \epsilon 1, r^4 - 1)$ делит 5, то q^3 делит либо $(5, q)(r^4 - 1)$, либо $(5, q)(r^3 - \epsilon r^2 + \epsilon 1)$. Предположим, что q^3

делит $(5,q)(r^4-1)$. Тогда либо q четно и q^3 делит $2(r^2-1)$, либо q нечетно и q^3 делит $5(r^2\pm 1)$. В первом случае $r(r^2+1)(r^3-\epsilon r^2+\epsilon 1)/2$ делит число $q^3+\delta 1$, не превосходящее $2(r^2-1)+1$, что невозможно. Поэтому q^3 делит $(5,q)(r^3-\epsilon r^2+\epsilon 1)$. Отсюда $r(r^4-1)/(5,q)$ делит число $q^3+\delta 1$, не превосходящее $(5,q)(r^3-\epsilon r^2+\epsilon 1)+1$. Имеем $r(r^4-1)/(5,q)\leq (5,q)(r^3-\epsilon r^2+\epsilon 1)+1$. Если $(5,q)=1$, то $r(r^4-1)\leq r^3-\epsilon r^2+\epsilon 1+1$, что невозможно. Поэтому $(5,q)=5$ и $r(r^4-1)\leq 25(r^3-\epsilon r^2+\epsilon 1)+1$. Легко проверяется, что $r\leq 5$. Так как $(q,r)=1$, получаем, что $r\leq 4$. Последнее условие противоречит равенству $q^3(q^3+\delta 1)=r(r^4-1)(r^3-\epsilon r^2+\epsilon 1)$.

Таким образом, $d=3$. Тогда $(q^3-\delta 1)(q^3+\delta 2)=3r(r^4-1)(r^3-\epsilon r^2+\epsilon 1)$. Если $r\leq 5$, то $3r(r^4-1)(r^3-\epsilon r^2+\epsilon 1)$ не делится на 27, что противоречит делимости на 27 числа $(q^3-\delta 1)(q^3+\delta 2)$. Поэтому $r>5$. Так как $A_1(r)\circ A_5(r)<A_8(r)<E_8(r)$, где $\circ$ — знак центрального произведения групп, то по лемме 6(а) группа P содержит элемент порядка $s(r^4-1)$. Пусть n — наибольший общий делитель чисел $(q^3+\delta 2)/3$ и $s(r^4-1)$. Тогда L содержит полупростой элемент порядка n, поэтому n делит порядок некоторого максимального тора в L. Как и выше, имеем $n\in\{1,5,11,17,25\}$.

Предположим, что s делит n. Тогда $s\in\{5,11,17\}$, r делит $q^3+\delta 2$ и $q^3-\delta 1=(r^4-1)a$ для некоторого $a\in\mathbb{N}$. Имеем $(r^4-1)a((r^4-1)a+\delta 3)=3r(r^4-1)(r^3-\epsilon r^2+\epsilon 1)$, откуда $(a^2-3)r^4=a^2-\delta 3a-\epsilon 3r^3+\epsilon 3r$. Если $a=1$, то

$$5\leq r=\frac{\delta 3-1+\epsilon 3r^3-\epsilon 3r}{2r^3}\leq\frac{3-1+3r(r^2-1)}{2r^3}=\frac{1}{r^3}+\frac{3(r^2-1)}{2r^2}<4;$$

противоречие. Поэтому $a>1$ и, следовательно,

$$r=\frac{a^2-\delta 3a}{a^2-3}+\frac{-\epsilon 3r(r^2-1)}{(a^2-3)r^3}\leq\frac{a^2+3a}{a^2-3}+\frac{3(r^2-1)}{(a^2-3)r^2}<1+\frac{3(a+1)}{a^2-3}+\frac{3}{a^2-3}.$$

Так как $1+\frac{3(a+1)}{a^2-3}+\frac{3}{a^2-3}$ равно 13 при $a=2$ и не превосходит 10 при $a\geq 3$, то $r=11$ и $a=2$. Но тогда $q^3-\delta 1=29280$ не делится на 9; противоречие.

Итак, s не делит n, и, следовательно, r делит $q^3-\delta 1$, т. е. $q^3-\delta 1=r(r^4-1)a/n$ для некоторого $a\in\mathbb{N}$. Имеем

$$\frac{r(r^4-1)a}{n}\cdot\left(\frac{r(r^4-1)a}{n}+\delta 3\right)=3r(r^4-1)(r^3-\epsilon r^2+\epsilon 1),$$

откуда $a^2r^5=3n^2r^3-\epsilon 3n^2r^2+a^2r-3n(\delta a-\epsilon n)$, в частности, r делит $3n(\delta a-\epsilon n)$.

Предположим, что $a\geq n/2$. Тогда

$$r^2=\frac{3n^2}{a^2}-\frac{\epsilon 3n^2}{a^2r}+\frac{1}{r^2}-\frac{\delta 3n^2}{ar^3}+\frac{\epsilon 3n^2}{a^2r^3}\leq 25,$$

что противоречит неравенству $r>5$. Поэтому $a<n/2$ и, следовательно, $n\neq 1$. Так как s делит $\delta a-\epsilon n$, то $\delta=-\epsilon$ и, значит, r делит $3(a+n)$, причем $a+n\leq 37$. Заметим, что $a+n$ четно, поскольку a и n нечетны. Поэтому $a+n\leq 36$.

Так как $r>5$, $r/(r,3)$ делит $a+n$, $a+n$ четно и $a+n\leq 36$, то $r\in\{7,8,9,11,16,13,17,32\}$. Но тогда либо $n=5$, либо $n=11$ и $r=32$, либо $n=17$ и $r=16$, либо $n=25$ и $r\in\{7,32\}$. В первом случае из неравенства $a+n\leq 7$ получаем $r=9$ и $a=1$, откуда $q^3-\delta 1=11808$, т. е. $q^3=11808+\delta 1$; противоречие. Второй случай невозможен ввиду неравенства $a+n\leq 15$. Третий случай невозможен в силу неравенства $a+n\leq 25$. Итак, $n=25$ и $r\in\{7,32\}$. Если $r=7$, то из неравенства $a+n\leq 15$ получаем $a=3$, т. е. $q^3=672+\delta 1$; противоречие.

Поэтому $r = 32$ и из неравенства $a+n \leq 36$ получаем $a = 7$, т. е. $q^3 = 293601+\delta 1$; противоречие.

11. Пусть $P \cong G_2(r)$, где $r > 2$. Тогда

$$(q^6 + \delta q^3 + 1)/d = r^2 + \epsilon r + 1$$

для некоторого $\epsilon \in \{+, -\}$.

Предположим, что $d = 1$. Тогда $q^3(q^3 + \delta 1) = r(r + \epsilon 1)$.

Пусть $(q, r) \neq 1$. Тогда $r = q^3$ и $\epsilon = \delta$. В P есть циклический максимальный тор порядка $r^2 - \epsilon r + 1$ (см. [13, с. 209]). Отсюда в L есть полупростой элемент порядка $q^6 - \delta q^3 + 1$, который содержится в некотором максимальном торе группы L. Значит, $q^6 - \delta q^3 + 1$ делит порядок этого максимального тора. Заметим, что $\frac{q^{18}-1}{(q^9-\delta 1)(q^3+\delta 1)} = q^6 - \delta q^3 + 1$. По теореме Жигмонди существует простое число $f \in \pi(q^6 - \delta q^3 + 1)$ такое, что f делит $q^{18} - 1$, но не делит $q^i - 1$ для $1 \leq i < 6$. Это противоречит лемме 5.

Поэтому $(q, r) = 1$ и, следовательно, q^3 делит $r + \epsilon 1$, т. е. $r + \epsilon 1 = q^3 a$ для некоторого $a \in \mathbb{N}$. Отсюда $q^3(q^3+\delta 1) = q^3 a(q^3 a-\epsilon 1)$, поэтому $(a^2-1)q^3 = \epsilon a+\delta 1$. Если $a > 1$, то

$$8 \leq q^3 = \frac{\epsilon a + \delta 1}{a^2 - 1} \leq \frac{a + 1}{a^2 - 1} = \frac{1}{a - 1} \leq 1;$$

противоречие. Поэтому $a = 1$ и $\epsilon = -\delta$. Получаем равенство $r + \epsilon 1 = q^3$. По лемме 4 это возможно только при $(q, r, \epsilon) = (2, 7, +)$ или $(2, 9, -)$. Первый случай противоречит предположению $(q, \delta) \neq (2, -)$. Во втором случае $L = E_6(2)$ и $P \cong G_2(9)$, откуда

$$\pi(P) = \{2, 3, 5, 7, 13, 73\} \subseteq \pi(L) = \{2, 3, 5, 7, 13, 17, 31, 73\}.$$

Так как $|\operatorname{Out}(P)| = 4$, то $\pi(F(G))$ содержит $\{17, 31\}$. Поскольку подгруппа $F(G)$ нильпотентна, в ней найдется элемент порядка $17 \cdot 31$. Значит, и в L найдется полупростой элемент порядка $17 \cdot 31$. Этот элемент содержится в некотором максимальном торе T группы L, и, следовательно, $17 \cdot 31$ делит $|T|$. Но это по лемме 5 противоречит всем возможностям для $|T|$.

Таким образом, $d = 3$ и $(q^3 - \delta 1)(q^3 + \delta 2) = 3r(r + \epsilon 1)$. Рассуждая, как в п. 1, придем к противоречию.

12. Пусть $P \cong {}^2B_2(r)$, $r = 2^{2m+1} > 2$. Тогда $(q^6 + \delta q^3 + 1)/d \in \{r - 1, r - \sqrt{2r} + 1, r + \sqrt{2r} + 1\}$.

Пусть $(q^6 + \delta q^3 + 1)/d = r - 1$. Предположим, что $d = 1$. Тогда $q^3(q^3 + \delta 1) = 2(2^{2m} - 1)$ и, в частности, q нечетно. Теперь ясно, что q^3 делит $2^m - \epsilon 1$ для некоторого $\epsilon \in \{+, -\}$, т. е. $2^m - \epsilon 1 = aq^3$ для некоторого $a \in \mathbb{N}$. Отсюда $q^3(q^3 + \delta 1) = 2aq^3(aq^3 + \epsilon 2)$, $q^3 + \delta 1 = 2a(aq^3 + \epsilon 2)$, $(2a^2 - 1)q^3 = \epsilon 4a - \delta 1$, $27 \leq q^3 = (\epsilon 4a - \delta 1)/(2a^2 - 1) \leq (4a + 1)/(2a^2 - 1) \leq 5$; противоречие.

Поэтому $d = 3$ и, следовательно, $(q^6 + \delta q^3 + 1)/3 = r - 1$. Прибавив 1 к обеим частям последнего равенства, получим $(q^6 + \delta q^3 + 4)/3 = r$. В частности, q нечетно. По лемме 1 имеем $\pi(P) = \pi(r(r-1)(r^2+1))$ и $\pi_1(G) = \pi(q(q^5-\delta 1)(q^8-1)(q^{12}-1))$. Предположим, что порядок группы $\overline{G}/\operatorname{Inn}(P)$ делится на нечетное простое число t. Тогда в $\overline{G}\setminus\operatorname{Inn}(P)$ существует элемент x порядка t и в силу [21, (9-1)] имеем $O^{2'}(C_P(x)) \cong {}^2B_2(r_0)$, где $r_0^t = r$. В группе ${}^2B_2(r_0)$ есть элемент порядка r_0-1. Но $t \in \pi_1(G)$ и r_0-1 делит $r-1 = (q^6+\delta q^3+1)/3$; противоречие. Таким образом, $\overline{G}/\operatorname{Inn}(P)$ является 2-группой. Так как $(q^3 - \delta 1, q^2 + 1) = 2$, а $\delta q(q^2 + \delta q + 1)/2$ взаимно просто с $r(r - 1)(r^2 + 1)$, то $\pi((q^2 + 1)(q^2 + \delta q + 1)/2) \subseteq \pi(F(G))$. В силу того, что подгруппа $F(G)$ нильпотентна, в ней найдется элемент порядка s_1s_2, где $s_1 \in \pi((q^2+1)/2)$ и $s_2 \in \pi(q^2+\delta q+1)$. Значит, и в L найдется полупростой элемент порядка s_1s_2. Этот элемент содержится в некотором максимальном торе T группы L, и, значит, s_1s_2 делит $|T|$. Но это по лемме 5 противоречит всем возможностям для $|T|$.

Итак, $(q^6+\delta q^3+1)/d = r+\epsilon\sqrt{2r}+1$ для некоторого $\epsilon \in \{+,-\}$.

Предположим, что $d=1$. Тогда $q^3(q^3+\delta 1) = r+\epsilon 1\sqrt{2r} = 2^{m+1}(2^m+\epsilon 1)$. Если q четно, то $q^3 = 2^{m+1}$ и, следовательно, $m>1$ и $2^{m+1}+\delta 1 = 2^m+\epsilon 1$, откуда $2^m = -\delta 1+\epsilon 1$, т. е. $m=1$; противоречие. Поэтому q нечетно и, значит, q^3 делит $2^m+\epsilon 1$ и 2^{m+1} делит $q^3+\delta 1$; противоречие.

Таким образом, $d=3$ и $(q^6+\delta q^3+1)/3 = r+\epsilon\sqrt{2r}+1$, откуда $(q^3-\delta 1)(q^3+\delta 2)/3 = 2^{m+1}(2^m+\epsilon 1)$. Если q четно, то $q^3-\delta 1$ нечетно и $(q^3+\delta 2)_2 = 2$; противоречие с тем, что $m>0$. Поэтому q нечетно и, следовательно, $q^3+\delta 2$ нечетно, откуда $9\cdot 2^{m+1}$ делит $q^3-\delta 1$, т. е. $q^3-\delta 1 = 9\cdot 2^{m+1}a$ для некоторого $a \in \mathbb{N}$. Имеем $9\cdot 2^{m+1}a(9\cdot 2^{m+1}a+\delta 3)/3 = 2^{m+1}(2^m+\epsilon 1)$, откуда $9a(3\cdot 2^{m+1}a+\delta 1) = 2^m+\epsilon 1$; противоречие.

13. Пусть $P \cong {}^2G_2(r), r = 3^{2m+1} > 3$. Тогда $(q^6+\delta q^3+1)/d = r+\epsilon\sqrt{3r}+1$ для некоторого $\epsilon \in \{+,-\}$.

Предположим, что $d=1$. Тогда $q^3(q^3+\delta 1) = 3^{m+1}(3^m+\epsilon 1)$. Если 3 делит q, то $q^3 = 3^{m+1}$ и, следовательно, $3^{m+1}+\delta 1 = 3^m+\epsilon 1$, откуда $6 \le 2\cdot 3^m = -\delta 1+\epsilon 1 \le 2$; противоречие. Если 3 не делит q, то 3^{m+1} делит $q^3+\delta 1$, а q^3 делит $3^m+\epsilon 1$, откуда $3^{m+1} \le q^3+\delta 1 \le 3^m+\delta 1+\epsilon 1 \le 3^m+2$ и, следовательно, $3^{m+1} \le 3^m+2$, что противоречит условию $m>0$.

Таким образом, $d=3$ и $(q^6+\delta q^3+1)/3 = r+\epsilon\sqrt{3r}+1$, откуда $(q^3-\delta 1)(q^3+\delta 2) = 3^{m+2}(3^m+\epsilon 1)$. Так как 9 делит $q^3-\delta 1$ и $(q^3-\delta 1, q^3+\delta 2) = 3$, то 3^{m+1} делит $q^3-\delta 1$, т. е. $q^3-\delta 1 = 3^{m+1}a$ для некоторого $a \in \mathbb{N}$. Имеем $3^{m+1}a(3^{m+1}a+\delta 3) = 3^{m+2}(3^m+\epsilon 1)$, откуда $3^m(a^2-1) = -\delta a+\epsilon 1$. Если $a>1$, то

$$3 \le 3^m = \frac{-\delta a+\epsilon 1}{a^2-1} \le \frac{a+1}{a^2-1} = \frac{1}{a-1} \le 1;$$

противоречие. Поэтому $a=1$. Теперь ввиду леммы 4 получаем, что $q=2$, $\delta=-$ и $m=1$; противоречие с предположением.

Итак, мы доказали, что P изоморфна $E_6^\delta(q)$. Наконец, ясно, что $F(G) \le G'$. Применяя результат [23], получим, что G/G' есть циклическая $\{2,3\}$-группа.

Теорема доказана.

Автор благодарит рецензента за замечания, позволившие улучшить первоначальный текст статьи.

ЛИТЕРАТУРА

1. *Williams J. S.* Prime graph components of finite groups // J. Algebra. 1981. V. 69, N 2. P. 487–513.
2. *Кондратьев А. С.* О компонентах графа простых чисел конечных простых групп // Мат. сб. 1989. Т. 180, № 6. С. 787–797.
3. *Мазуров В. Д.* Группы с заданным спектром // Изв. Уральск. гос. ун-та. Математика и механика, вып. 7. 2005. № 36. С. 119–138.
4. *Нерешенные* вопросы теории групп. Коуровская тетрадь. 15-е изд. Новосибирск: Новосиб. гос. ун-т, 2002.
5. *Алексеева О. А., Кондратьев А. С.* О распознаваемости группы $E_8(q)$ по множеству порядков элементов // Укр. мат. журн. 2002. Т. 54, № 7. С. 998–1003.
6. *Алексеева О. А., Кондратьев А. С.* Квазираспознаваемость одного класса конечных простых групп по множеству порядков элементов // Сиб. мат. журн. 2003. Т. 44, № 2. С. 241–255.

7. *Васильев А. В., Гречкосеева М. А.* О распознаваемости конечных простых ортогональных групп размерности 2^m, 2^m+1 и 2^m+2 // Сиб. мат. журн. 2004. Т. 45, № 3. С. 510–526.

8. *Алексеева О. А., Кондратьев А. С.* Квазираспознаваемость по множеству порядков элементов групп ${}^3D_4(q)$ и $F_4(q)$ для нечетного q // Алгебра и логика. 2005. Т. 44, № 5. С. 517–539.

9. *Алексеева О. А.* Квазираспознаваемость по множеству порядков элементов групп ${}^3D_4(q)$, q четно // Алгебра и логика. 2006. Т. 45, № 1. С. 3–19.

10. *Aschbacher M.* Finite group theory. Cambridge: Cambridge Univ. Press, 1986.

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

12. *Huppert B.* Endliche Gruppen I. Berlin a. o.: Springer-Verl., 1967.

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

14. *Стейнберг Р.* Лекции о группах Шевалле. М.: Мир, 1975.

15. *Кондратьев А. С., Мазуров В. Д.* Распознавание знакопеременных групп простой степени по порядкам их элементов // Сиб. мат. журн. 2000. Т. 41, № 2. С. 359–369.

16. *Zsigmondy K.* Zur Theorie der Potenzreste // Monatsh. Math. Phys. 1892. Bd 3. S. 265–284.

17. *Gerono G. C.* Note sur la résolution en nombres entiers et positifs de l'équation $x^m = y^n+1$ // Nouv. Ann. Math. (2). 1870. V. 9. P. 469–471.

18. *Deriziotis D. I.* Conjugacy classes and centralizers of semisimple elements in finite groups of Lie type // Vorlesungen Fachb. Math. Univ. Essen. 1984. Heft 11.

19. *Kleidman P., Liebeck M.* The subgroup structure of the finite classical groups. Cambridge: Cambridge Univ. Press, 1990. (London Math. Soc. Lect. Note Ser.; V. 129).

20. *Алеева М. Р.* О конечных простых группах с множеством порядков элементов как у группы Фробениуса или двойной группы Фробениуса // Мат. заметки. 2003. Т. 73, № 3. С. 323–339.

21. *Gorenstein D., Lyons R.* The local structure of finite groups of characteristic 2 type. Providence, RI: Amer. Math. Soc., 1983. (Mem. Amer. Math. Soc.; V. 42, N 276).

22. *Stensholt E.* Certain embeddings among finite groups of Lie type // J. Algebra. 1978. V. 53, N 1. P. 136–187.

23. *Lucido M. S.* Prime graph components in finite almost simple groups // Rend. Sem. Mat. Univ. Padova. 1999. V. 102. P. 1–22.

Статья поступила 12 мая 2006 г.

Кондратьев Анатолий Семенович
Институт математики и механики УрО РАН,
ул. С. Ковалевской, 16, Екатеринбург, ГСП-384, 620219
a.s.kondratiev@imm.uran.ru