Владикавказский математический журнал
2008, Том 10, Выпуск 1, С. 40–52

УДК **512.542**

ОБОБЩЕНИЕ ТЕОРЕМЫ ЦАССЕНХАУЗА[1]

В. Д. Мазуров

Дано новое доказательство теоремы Цассенхауза о строении конечной группы, действующей свободно на абелевой группе.

Ключевые слова: свободное действие, элемент порядка 3, группа Фробениуса.

Введение

Пусть группа A действует на нетривиальной группе B. Это действие называется *свободным* (а сама группа A действующей *свободно*, если $b^a \neq b$ для всех $A \ni a \neq 1 \neq b \in B$. Характерным примером свободного действия является действие дополнительного множителя конечной группы Фробениуса на ее ядре. Более того, если группа A действует свободно на конечной группе B, то естественное полупрямое произведение $G = AB$ является группой Фробениуса, в которой B — ядро, а A — дополнение. Кроме того, A свободно действует при сопряжении в G на центре некоторой силовской подгруппы из B и, таким образом, изучение строения дополнений конечных групп Фробениуса эквивалентно изучению групп, действующих свободно на нетривиальных конечных абелевых группах. 70 лет назад Цассенхауз [1] классифицировал дополнения конечных групп Фробениуса. Разбор случая неразрешимых дополнений в этой работе был очень сложным и не свободным от пробелов в доказательстве. Позднее Цассенхауз внес исправления в доказательство, но содержащая их рукопись осталась неопубликованной. Впервые исправленное, но столь же длинное и сложное доказательство появилось в [2] в связи с классификацией полных связных римановых многообразий постоянной положительной кривизны, которая целиком основывается на классификации Цассенхауза. Следует добавить, что доказательства в [1, 2] в большой мере используют теорию характеров конечных групп, что делает невозможным их обобщения на бесконечные группы. В настоящей работе мы предлагаем другое доказательство классификации конечных неразрешимых групп, действующих свободно на абелевых группах, которое может быть обобщено на широкий класс бесконечных свободно действующих групп. Мы постарались при этом использовать лишь наиболее простые факты, которые изложены в большинстве учебников по теории групп.

Основным результатом настоящей работы является доказательство следующего результата.

© 2008 Мазуров В. Д.

[1]Работа выполнена при поддержке Российским фондом фундаментальных исследований, проект № 06-01-39001.

Теорема 1. *Пусть группа G действует свободно на нетривиальной абелевой группе. Если G порождена таким непустым инвариантным множеством X элементов порядка* 3, *что $X = X^{-1}$ и для любых $x, y \in X$ порядок xy конечен, то G конечна и изоморфна $SL_2(5)$, $SL_2(3)$ или циклической группе порядка* 3.

Здесь $SL_2(q)$ обозначает группу всех двумерных матриц с определителем, равным единице, над полем порядка q.

Из теоремы 1 вытекает характеризация конечных групп, действующих свободно на абелевых группах, которая в большинстве случаев вполне заменяет исчерпывающую классификацию таких групп.

Теорема 2. *Конечная группа G тогда и только тогда может действовать свободно на нетривиальной абелевой группе, когда ее подгруппа G_0, порожденная всеми элементами простых порядков, является прямым произведением циклической холловой подгруппы Z, порядок которой свободен от квадратов, и группы, изоморфной $SL_2(5)$, $SL_2(3)$ или тривиальной группе.*

Другим следствием теоремы 1 является полученное в свое время Цассенхаузом описание неразрешимых дополнений групп Фробниуса.

Теорема 3. *Пусть конечная неразрешимая группа G действует свободно на нетривиальной абелевой группе. Тогда в G содержится такая нормальная подгруппа G_0 индекса 1 или 2, что $G_0 \simeq M \times SL_2(5)$, где M — метациклическая группа, порядок которой взаимно прост с числом* 30.

1. Обозначения и используемые результаты

Если H — подгруппа группы G, $x, y \in G$, X, Y — подмножества из G, то $x^y = y^{-1}xy$, $X^y = \{y^{-1}xy | x \in X\}$, $[x, y] = x^{-1}x^y$, $x^Y = \{x^y | y \in Y\}$, $X^Y = \{x^y | x \in X,\ y \in Y\}$, $N_H(X) = \{g \in H | X^g = X\}$, $\langle X\rangle$ — подгруппа, порожденная X, $[X, Y] = \langle [x, y] | x \in X,\ y \in Y\rangle$, $C_H(X) = \{h \in H \,\big|\, [h, x] = 1 \text{ для всех } x \in X\}$, $Z(G) = C_G(G)$.

Группа всех (внешних) автоморфизмов группы G обозначается через $\mathrm{Aut}(G)$ (соответственно, через $\mathrm{Out}(G)$). Для простого числа p подгруппа $O_p(G)$ определяется как произведение всех нормальных p-подгрупп из G, A_m и S_m означают знакопеременную и, соответственно, симметрическую группу степени m. Если I — множество произвольной мощности, то $A(I)$ обозначает знакопеременную группу множества I, т. е. (локально конечную) группу всех почти тождественных четных подстановок I.

Для группы всех невырожденных линейных преобразований векторного пространства V над полем K (с равным единице определителем) будет использоваться обозначение $GL(V)$ (соответственно, $SL(V)$). Если размерность V равна n, то с помощью выбора базиса в V группа $GL(V)$ ($SL(V)$) отождествляется с группой $GL_n(K)$ (соответственно, с группой $SL_n(K)$) всех невырожденных n-мерных матриц над K (с равным единице определителем). Если K — конечное поле порядка q, то вместо $G(S)L_n(K)$ будем писать $G(S)L_n(q)$.

Символами $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$ и $\mathbb{C}$ обозначаются соответственно множество натуральных чисел, кольцо целых чисел и поля рациональных и комплексных чисел. Кольцо эндоморфизмов абелевой группы A обозначается через $\mathrm{End}(A)$.

Если M — конечное подмножество аддитивной коммутативной полугруппы, то через $\sum M$ будем обозначать сумму всех элементов из M, т. е. $\sum M = \sum\limits_{m \in M} m$.

Через $\varphi(n)$ обозначается значение функции Эйлера на натуральном числе n. По определению, $\varphi(1) = 1$, а если $n > 1$, то $\varphi(n)$ равно количеству натуральных чисел, меньших

n и взаимно простых с n. Хорошо известно, что

$$\varphi(n) = p_1^{\alpha_1-1}(p_1-1)\cdots p_s^{\alpha_s-1}(p_s-1),$$

если $n = p_1^{\alpha_1}\cdots p^{\alpha_s}$, где $p_1, \ldots, p_s$ — различные простые делители числа n.

Если m и n — целые числа, то (m, n) означает их наибольший общий делитель.

Лемма 1. *Пусть P — силовская p-подгруппа конечной группы G.*

1) (*Гёльдер* [4, *теорема* 9.4.3]). *Если P является циклической группой для каждого простого числа p, делящего $|G|$, то G — метациклическая.*

2) (*Бернсайд* [4, *теорема* 14.3.1]). *Если P содержится в центре $N_G(P)$, то G обладает нормальным p-дополнением.*

3) (*Известное следствие теоремы Фробениуса* [4, *теорема* 14.4.7]). *Если $p = 2$, P — метациклическая группа и порядок G взаимно прост с 3, то G обладает нормальным p-дополнением.*

4) (*Бернсайд* [4, *теорема* 12.5.2]). *Если каждая абелева подгруппа из P циклическая, то при $p > 2$ группа P является циклической, а при $p = 2$ — либо циклической, либо обобщенной группой кватернионов.*

Элементарное доказательство следующего результата (не использующее теорию когомологий) можно найти, например, в [5, гл. 7, § 2, теорема Шура].

Лемма 2. *Пусть N — нормальная p-подгруппа конечной группы H, индекс которой не делится на p. Тогда в G существует такая подгруппа C, что $H = NC$ и $N \cap C = 1$.*

Лемма 3 (формула обращения Мёбиуса [6, параграф 1, глава 9]**).** *Пусть f и g — комплекснозначные функции натурального аргумента. Если $f(n) = \sum \big\{ g(d) \big|\, d$ — натуральный делитель числа $n \big\}$, то $g(n) = \sum \big\{ \mu(n/d) f(d) \big|\, d$ — натуральный делитель числа $n \big\}$, где μ — функция Мёбиуса, т. е. $\mu(1) = 1$, $\mu(p_1 p_2 \cdots p_k) = (-1)^k$, если $p_1, \ldots, p_k$ — различные простые числа, $\mu(n) = 0$, если n делится на квадрат простого числа.*

2. Предварительные леммы

Лемма 4. 1) *Пусть x, y — элементы порядка 3, порождающие A_4. Тогда $(xy)^2 = 1$ или $(xy^{-1})^2 = 1$.*

2) *Пусть I — непустое множество, не содержащее 1 и 2, и $K = \{1, 2\} \cup I$. Тогда отображение $x_i \to (1, 2, i)$, $i \in I$, можно продолжить до изоморфизма группы $G = \big\langle x_i,\ i \in I \big|\, x_i^3 = (x_i x_j)^2 = 1,\ i, j \in I,\ i \neq j \big\rangle$ на $A(K)$.*

3) *Пусть x, y — элементы порядка 3, порождающие A_5. Тогда $(xy)^5 = (xx^y)^2 = (yy^x)^2 = 1$.*

4) $A_5 \simeq \big\langle x,\ y \big|\, x^3 = y^3 = (yy^x)^2 = (xx^y)^2 = 1 \big\rangle \simeq \big\langle x,\ y \big|\, x^3 = y^3 = (xy)^5 = (xx^y)^2 = 1 \big\rangle$.

5) *Если x, y — такие элементы порядка 3 из A_5, что $\langle x \rangle \neq \langle y \rangle$ и $(xy)^2 = 1$, то существует $z \in A_5$ порядка 3, для которого $(xz)^2 = (yz)^2 = 1$.*

$\lhd$ 1) Два 3-цикла (i_1, i_2, i_3) и (j_1, j_2, j_3) тогда и только тогда порождают A_4, когда $\big|\{i_1, i_2, i_3, j_1, j_2, j_3\}\big| = 4$, поэтому без потери общности можно считать, что $x = (1, 2, 3)$, $y = (1, 2, 4)^{\pm 1}$, после чего все соотношения проверяются непосредственными вычислениями.

2) Предположим вначале, что I конечно, т. е. $K = \{1, 2, \ldots, n\}$ для некоторого натурального числа $n \geqslant 3$. В этой части наши рассуждения повторяют доказательство Кармайкла [7, с. 172]. Если $n = 3$, то, очевидно, $G \simeq A_3$, поэтому предположим, что $n > 3$, и используем индукцию по n. Положим $H = \langle x_1, \ldots, x_{n-1} \rangle$, $C_1 = H$, $C_2 = Hx_n$,

$C_i = Hx_nx_i^{-1}$, $i = 3, \ldots, n-1$, $C_n = Hx_n^{-1}$ и покажем, что $C_1, \ldots, C_n$ исчерпывают все смежные классы по H в G. Отметим, что

$$x_i^2 = x_i^{-1}, \quad x_ix_j = x_j^{-1}x_i^{-1} = x_j^2x_i^2, \quad i, j = 3, \ldots, n, \ i \neq j. \tag{1}$$

Далее, очевидно, что

$$C_1x_i^{-1} = C_1, \quad i = 3, \ldots, n-1;$$
$$C_1x_n = C_2;$$
$$C_2x_i^{-1} = C_i, \quad i = 3, \ldots, n-1;$$
$$C_2x_n = C_n.$$

Теперь по (1) для $i, j = 3, \ldots, n-1$, $i \neq j$ справедливы равенства

$$C_ix_i^{-1} = Hx_nx_i = Hx_i^{-1}x_n^{-1} = C_n;$$
$$C_nx_i^{-1} = Hx_n^{-1}x_i^{-1} = Hx_ix_n = Hx_n = C_2;$$
$$C_ix_j^{-1} = Hx_nx_i^{-1}x_j^{-1} = Hx_nx_jx_i = Hx_j^{-1}x_n^{-1}x_i = Hx_n^{-1}x_i =$$
$$= C_nx_i = C_nx_i^{-1}x_i^{-1} = C_2x_i^{-1} = C_i.$$

Таким образом, множество $D = C_1 \cup \ldots \cup C_n$ инвариантно относительно умножения справа на $x_3^{-1}, \ldots, x_{n-1}^{-1}, x_n$. Поскольку порядки этих элементов конечны, $D = G$ и $|G : H| \leqslant n$. По индуктивному предположению H — гомоморфный образ группы A_{n-1}, поэтому $|G| \leqslant |A_n|$. С другой стороны, A_n порождается подстановками $y_i = (1, 2, i)$, $i = 3, \ldots, n$, удовлетворяющими соотношениям $y_i^3 = (y_iy_j)^2$ для $j \neq i$, поэтому отображение $\varphi : x_i \to y_i$, $i = 3, \ldots, n$, можно продолжить до гомоморфизма G на A_n. Поэтому $|G| \geqslant |A_n|$ и следовательно $G \simeq A_n$.

В общем случае отображение $\varphi : x_i \to (1, 2, i)$, $i \in I$, можно продолжить до гомоморфизма $G = \langle x_i, \ i \in I \,|\, x_i^3 = (x_ix_j)^2 = 1, \ i, j \in I, \ i \neq j \rangle$ на $A(K)$. Предположим, что ядро этого гомоморфизма содержит нетривиальный элемент y. Тогда y — некоторое слово от порождающих x_i. Пусть $x_{i_1}, \ldots, x_{i_t}$ — все порождающие из записи этого слова. По предыдущим рассуждениям ограничение φ на $\langle x_{i_1}, \ldots, x_{i_t} \rangle$ является изоморфизмом на $A(\{1, 2, i_1, \ldots, i_t\})$ и поэтому $y = 1$.

3) Подобно рассуждениям в доказательстве 1) можно считать, что $x = (1, 2, 3)$, $y = (3, 4, 5)$, после чего все соотношения проверяются непосредственно.

4) Дополнительное соотношение $[x, y] = 1$ превращает G в тривиальную группу, поэтому $G = [G, G]$. Пусть $H = \langle x, x^y, x^{y^2} \rangle$. Так как $\langle y \rangle$ переставляет при сопряжении порождающие H, то H является $\langle y \rangle$-инвариантной. Так как H содержит x, то H и $\langle x \rangle$-инвариантна. Поэтому $H \trianglelefteq G$. Очевидно, что G/H абелева, следовательно $H = G$. Поскольку $(x^yx^{y^2})^2 = ((xx^y)^2)^y = 1$ и $(x^{y^2}x)^2 = ((xx^y)^2)^{y^2} = 1$, из 2) вытекает, что H — гомоморфный образ A_5. По 1) $H \simeq A_5$.

5) Без потери общности можно предполагать, что $x = (1, 2, 3)$, $y = (1, 2, 4)$. Теперь подстановку $(1, 2, 5)$ можно взять в качестве z. $\triangleright$

Лемма 5. (1) $SL_2(5) \simeq X = \langle x, y \,|\, x^3 = y^3 = (xx^y)^4 = (yy^x)^4 = (xx^y)^2(yy^x)^2 = [x, (xx^y)^2] = [y, (xx^y)^2] = 1 \rangle$.

(2) $SL_2(3) \simeq Y = \langle x, y \,|\, x^3 = y^3 = (xy)^4 = [x, (xy)^2] = [y, (xy)^2] = 1 \rangle$.

$\triangleleft$ Если к соотношениям группы добавить равенство $(xx^y)^2 = 1$, то получившаяся группа будет удовлетворять соотношениям для X из леммы 4, 4). Кроме того, порядок элемента $(xx^y)^2$ в X не превосходит числа 2 и этот элемент лежит в центре X. Таким образом, $|X| \leqslant 120$. В группе $H = SL_2(5)$ (ее порядок равен 120) положим $x = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$,

$y = \begin{pmatrix} 1 & 1 \\ 2 & -2 \end{pmatrix}$. Тогда порядки элементов x, y, xy равны, соответственно, 3, 3 и 10. Следовательно, порядок группы $X = \langle x, y \rangle$ делится на 30, т. е. ее индекс в H делит 4. Отсюда $X = H$. Непосредственно проверяется, что для x и y выполняются все соотношения группы X. Поэтому $H \simeq X$.

Аналогично, порядок центрального элемента $(xy)^2$ из группы Y не превосходит числа два, а тривиализация этого элемента превращает соотношения для Y в соотношения для $SL_2(3)$ из леммы 4, 2). Взяв $x = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in SL_2(3)$, получим пункт (2) леммы. $\triangleright$

Лемма 6. *Пусть V — двумерное векторное пространство над $\mathbb{C}$. Пусть $x, y \in SL(V)$ такие элементы порядка 3, что $xy \neq yx$ и порядок xy равен n. Тогда в V существует база, в которой x, y представимы матрицами*

$$x = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad y = \begin{pmatrix} -1 & -\lambda^{-1} \\ \lambda & 0 \end{pmatrix}, \tag{1}$$

где λ — примитивный корень n-ой степени из единицы. Если $n = 4$, то $H = \langle x, y \rangle \simeq SL_2(3)$; если $n = 10$, то $H \simeq SL_2(5)$.

$\triangleleft$ Пусть $v \in V$ собственный вектор для xy. Поскольку xy подобна диагональной матрице, характеристические корни которой взаимно обратны, $vxy = \lambda v$, где λ — примитивный корень n-ой степени из единицы. Отметим также, что x, y подобны диагональной матрице с диагональными элементами ε, $1/\varepsilon$, где $\varepsilon = (-1 + i\sqrt{3})/2$ и поэтому $x^2 + x + 1 = y^2 + y + 1 = 0$, т. е. $x^{-1} = x^2 = -1 - x$, $y^{-1} = -1 - y$. Если v является собственным вектором и для x, то $H = \langle x, y \rangle$ диагонализируема и поэтому $xy = yx$ вопреки предположению. Следовательно, $v_1 = v$, $v_2 = vx$ образуют базу в V и

$$v_1 x = v_2, \quad v_2 x = vx^2 = -v - vx = -v_1 - v_2. \tag{2}$$

Далее, $vxy = \lambda v$, так что $vx = \lambda v y^{-1} = -\lambda(vy + v)$, $vy = -v - \lambda^{-1} vx$ и поэтому

$$v_1 y = -v_1 - \lambda^{-1} v_2, \quad v_2 y = \lambda v_1. \tag{3}$$

Равенства (2), (3) показывают, что v_1, v_2 — искомая база в V.

Непосредственно проверяется, что при $n = 10$, 4 элементы x, y удовлетворяют соотношениям леммы 5. $\triangleright$

Лемма 7. *Пусть A — прямая сумма аддитивных циклических групп $\langle a_i \rangle$, $i = 1, \ldots, n$, одного и того же порядка p^r, где p — простое число, $r \in \mathbb{N}$, и F — группа автоморфизов подгруппы $B = \{a \in A \,|\, pa = 0\}$, порядок которой не делится на p. Тогда в $\mathrm{Aut}(A)$ существует подгруппа, изоморфная F, действие которой на B совпадает с действием F.*

$\triangleleft$ Очевидно, элементы $b_i = p^{r-1} a_i$, $i = 1, \ldots, n$ составляют базис элементарной абелевой подгруппы B и для любого $f \in F$ в интервале $[1, p-1]$ существуют однозначно определенные целые числа $t_{ij}(f)$, $i, j = 1, \ldots, n$, для которых

$$b_i f = \sum_{j=1}^{n} t_{ij}(f) b_j$$

и поэтому существует единственный эндоморфизм $\hat{f}$ группы A, для которого

$$a_i \hat{f} = \sum_{j=1}^{n} t_{ij}(f) a_j.$$

Поскольку $\hat{f}$ индуцирует автоморфизм группы A/pA, где $pA = \{px \mid x \in A\}$, эндоморфизм $\hat{f}$ является автоморфизмом. Пусть $\hat{F} = \langle \hat{f} \mid f \in F \rangle$. Если U — подгруппа из $\hat{F}$, состоящая из тех автоморфизмов, которые индуцируют тождественный автоморфизм в A/pA, то $U \trianglelefteq \hat{F}$ и $\hat{F}/U \simeq F$. Так как U является p-группой, то по лемме 2 $\hat{F} = UF_0$, где $F_0 \cap U = 1$.

Для каждого $f \in F$ существует ровно один элемент f_0 из F_0 такой, что $f_0 = u\hat{f}$ для подходящего $u \in U$. Очевидно, что отображение $\phi : F_0 \to F$, определенное правилом $f_0\phi = f$, является изоморфизмом F_0 на F. Более того, если $f_0\phi = f$, то для $\overline{a_i} = a_i + pA$, $i = 1, \ldots, n$, имеет место равенство

$$\overline{a_i} f_0 = \sum_{j=1}^{n} t_{ij}(f)\overline{a_j}.$$

Так как для каждого элемента $a_i + a$ из смежного класса $a_i + pA$ выполнено равенство $p^{r-1}(a_i + a) = b_i$, то

$$b_i f_0 = \sum_{j=1}^{n} t_{ij}(f) b_j. \triangleright$$

Следующая лемма хорошо известна. Мы дадим ее элементарное доказательство, использующее только самые начальные результаты теории групп.

Лемма 8. *Пусть F — конечная группа, действующая свободно на нетривиальной абелевой группе A. Тогда F изоморфна такой подгруппе $F_1 \leqslant GL(V)$ для некоторого конечномерного векторного пространства V над полем комплексных чисел, что F_1 действует свободно на V, иными словами, любой характеристический корень любого нетривиального элемента из F_1 не равен единице.*

$\triangleleft$ Будем использовать аддитивную запись в A и записывать результат действия элемента $f \in F$ на $a \in A$ как af. Пусть a — ненулевой элемент из A. Группа $B = \langle af \mid f \in F \rangle$ является конечно порожденной абелевой группой, содержащей a.

Пусть вначале a — элемент бесконечного порядка и C — множество всех элементов конечного порядка из B. Тогда B является F-инвариантной подгруппой, и $D = B/C$ — нетривиальная конечно порожденная группа без кручения, на которой F действует свободно. Другими словами, F содержится в $GL_n(\mathbb{Z}) \leqslant GL_n(\mathbb{Q})$, где n — число свободных порождающих группы D, и $df \neq d$ для любой ненулевой целочисленной n-ки d и любого нетривиального элемента f из F. Но тогда $df \neq d$ и для любой рациональнозначной n-ки d. Таким образом, 1 не является собственным значением для f. Вкладывая $GL_n(\mathbb{Q})$ в $GL_n(\mathbb{C})$, получим для этого случая справедливость заключения.

Можно, следовательно, считать, что A — конечная группа. Заметим, что в качестве a можно взять теперь элемент некоторого простого порядка p. В этом случае B — элементарная абелева p-группа. Очевидно можно считать, что $A = B$. Пусть $|A| = p^n$ и A_r — прямая сумма n циклических групп порядка p^r. Отождествим A с подгруппой $\{a \in A_r \mid pa = 0\}$ из A_r. По лемме 7 действие F можно продолжить на A_r и, следовательно, на прямую сумму S всех A_r, $r \in \mathbb{N}$. Очевидно, это действие F на S является свободным. Пусть $E = \mathrm{End}(S)$. Группа F действует свободно на аддитивной группе кольца E и поскольку период S не ограничен, аддитивный порядок тождественного автоморфизма S (единицы кольца E) бесконечен. В частности, аддитивная группа E содержит элемент бесконечного порядка, и мы возвращаемся к уже рассмотренному случаю. $\triangleright$

Лемма 9. *Пусть F — группа, действующая свободно на нетривиальной* (*аддитивной*) *абелевой группе A.*

(1) *Если f — инволюция из F, то $af = -a$ для любого $a \in A$. В частности, f — единственная инволюция в F и $f \in Z(F)$.*

(2) *Если C — периодическая коммутативная подгруппа из F, то F — локально циклическая.*

(3) *Если C — конечная подгруппа из F, порядок которой свободен от квадратов, то C — цклическая.*

(4) *Если P — конечная примарная подгруппа из F, то P — либо циклическая, либо обобщенная группа кватернионов.*

$\lhd$ Пусть f — инволюция из F. Тогда $(a+af)f = a+af$ для любого $a \in A$ и пункт (1) доказан.

Для доказательства (2) достаточно показать, что подгруппа $D = \langle x, y\rangle$ является циклической для любых коммутирующих элементов $x, y \in C$. Но в этом случае D — конечная группа, действующая свободно на A, и по лемме 8 можно считать, что A является конечномерным векторным пространством над $\mathbb{C}$. Отсюда следует, что для D существует общий собственный вектор a. Теперь отображение φ, для которого $\varphi(d) = \lambda(d) \in \mathbb{C}$, где $d \in D$ и $ad = \lambda(d)a$, является гомоморфизмом D в $\mathbb{C}^*$, ядро которого тривиально в силу свободы действия D на A, и поэтому D изоморфна конечной, а следовательно циклической подгруппе из $\mathbb{C}$. Это доказывает (2).

Докажем (3). По лемме 1 C — метациклическая группа, поэтому достаточно рассмотреть случай, когда $|C| = pq$, где p, q — различные простые числа, $p < q$ и значит $C = \langle u, v\rangle$, где $u^v = u^t$, $t \in \mathbb{N}$, $1 \leqslant t < p$, $t^q - 1$ делится на p. По пункту (2) можно считать, что C неабелева и, значит, $t \neq 1$. Лемма 8 позволяет предполагать, что A — конечномерное пространство над $\mathbb{C}$. Пусть $a \in A$ — собственный вектор для u. Тогда $au = \lambda u$, где λ — отличный от единицы корень полинома $x^p - 1$. Так как $u^{v^i} = u^{t^i}$ для $i \in \mathbb{N}$, то $a(v^{-i}uv^i) = au^{t^i} = \lambda^{t^i}a$, откуда $(av^{-i})u = \lambda^{t^i}(av^{-i})$. Поскольку все числа λ^{t^i}, $i = 1, 2, \ldots, q-1$, различны, векторы $(av^{-i}$, $i = 0, 1, \ldots, q-1$ линейно независимы и, следовательно, $b = \sum\{a, av^{-1}, \ldots, av^{-q+1}\} \neq 0$. Но теперь $bv^{-1} = b$, что противоречит свободе действия F на A.

Пункт (4) следует из (2) и леммы 1 1). $\rhd$

Лемма 10. *Пусть n — натуральное число и α — примитивный корень степени n из единицы в $\mathbb{C}$. Тогда для любого целого $r \in \{0, 1, \ldots, n-1\}$*

$$\sum \left\{\alpha^{rk} \middle| 1 \leqslant k < n,\ (k, n) = 1\right\} = \mu(n/d)\varphi(n)/\varphi(n/d),$$

где $d = (r, n)$.

$\lhd$ Пусть вначале $r = 1$. Для каждого натурального t обозначим через $g(t)$ сумму примитивных корней степени t из единицы. Очевидно,

$$f(n) = \sum \left\{\alpha^i \middle| i = 0, 1, \ldots, n-1\right\} = \sum\{g(t) | t \text{ — натуральный делитель } n\}.$$

С другой стороны, $f(n)$ — сумма всех корней полинома $x^n - 1$, поэтому $f(1) = 1$ и $f(n) = 0$, если $n > 1$. По формуле обращения Мёбиуса (лемма 3) $g(n) = \mu(n)$.

Пусть r любое. Тогда α^r — примитивный корень степени n/d из единицы, $\alpha^{rk} = \alpha^{rl}$, где l — остаток от деления k на d, и если $(k, n) = 1$, то $(l, n) = 1$. По предыдущему абзацу

$$\sum \left\{\alpha^{rk} \middle| 1 \leqslant k < 1,\ (k, n) = 1\right\}$$
$$= \left(\sum \left\{\alpha^{rk} \middle| 1 \leqslant k < n/d,\ (k, n/d) = 1\right\}\right) \varphi(n)/\varphi(n/d) = \mu(n/d)\varphi(n)/\varphi(n/d). \rhd$$

Лемма 11. *Пусть β — примитивный корень степени u из единицы, γ — примитивный корень степени v из единицы в $\mathbb{C}$, $\lambda + \lambda^{-1} + \gamma + \gamma^{-1} = 1$ и $1 < u \leqslant v$. Тогда либо $u = 4$, $v = 6$, либо $u = v = 10$.*

$\lhd$ Пусть n — наименьшее общее кратное чисел u и v, α — примитивный корень степени n из единицы. Тогда $\beta = \alpha^r$, $\gamma = \alpha^s$ для некоторых натуральных r и s, и

$$\alpha^r + \alpha^{-r} + \alpha^s + \alpha^{-s} = 1.$$

Отображение $\alpha \to \alpha^k$, где $(n, k) = 1$, продолжается до автоморфизма поля $\mathbb{C}$, поэтому для таких k

$$\alpha^{rk} + \alpha^{-rk} + \alpha^{sk} + \alpha^{-sk} = 1.$$

Суммируя эти равенства по k, меньшим n, получим с учетом леммы 10

$$2\varphi(n)\mu(u)/\varphi(u) + 2\varphi(n)\mu(v)/\varphi(v) = \varphi(n),$$

откуда

$$\mu(u)/\varphi(u) + \mu(v)/\varphi(v) = 1/2.$$

Так как $|\mu(u)| \leqslant 1$, то $\varphi(u) \leqslant 4$, поэтому $u \in \{2, 3, 4, 5, 6, 8, 10, 12\}$.

Если $u = 2$, то $\varphi(u) = 1$, $\mu(u) = -1$ и $\mu(v)/\varphi(v) = 3/2$, что невозможно. Аналогично исключаются остальные возможности для u, кроме 4 и 10, для которых v равно 6 и 10, соответственно. $\rhd$

Лемма 12. *Пусть K — конечная группа, H — ее нетривиальная нормальная подгруппа и $x \in K$ — такой элемент порядка 3, что $C_H(x) = 1$. Если $h \in H$, то подгруппа $H_0 = \langle h, h^x\rangle$ является x-инвариантной и $H_0 = \langle h\rangle \times \langle h^x\rangle$. Кроме того, $\langle H_0, x\rangle = \langle h, x\rangle = \langle x, x^h\rangle$*

$\lhd$ Централизатор x в $H\langle x\rangle$ равен $\langle x\rangle$, и все подгруппы порядка 3 сопряжены в $H\langle x\rangle$. Если $h \in H$, то $\langle xh\rangle$ — абелева подгруппа, порядок которой делится на 3. Поэтому $(xh)^3 = 1$. Отсюда следует, что $1 = (xh)^3 = xhx^{-1}x^{-1}hxh$, т. е.

$$(h^{-1})^{x^2} = hh^x. \tag{1}$$

Аналогично, $1 = (hx^{-1})^3 = hh^xh^{x^2}$, т. е.

$$(h^{-1})^{x^2} = h^xh. \tag{2}$$

Теперь из (1) и (2) вытекает, что $\langle h, h^x\rangle$ — абелева подгруппа, инвариантная относительно x. $\rhd$

Лемма 13. *Пусть H — конечная группа, x — элемент порядка 3 в H. Предположим, что $H = \langle x^H\rangle$ и для любого $h \in H$ подгруппа $\langle x, x^h\rangle$ либо циклическая, либо изоморфна одной из групп A_4, A_5.*

1) *Если $|H/O_2(H)| = 3$, то $O_2(H)$ — элементарная абелева группа и $C_{O_2(H)}(x) = 1$.*

2) *Если $H/O_2(H) \simeq A_5$, то $O_2(H) = 1$.*

$\lhd$ Предположим противное. Пусть H — противоречащий пример наименьшего порядка и N — минимальная нормальная подгруппа группы H, содержащаяся в $O_2(H)$. Предположим вначале, что неверен пункт 1. По предположению $E = O_2(H)/N$ — элементарная абелева группа и $C_E(x) = 1$. Пусть h — элемент порядка 4 в $O_2(H)$. Если $C_{O_2(H)}(x) = 1$, то по лемме 12 h принадлежит подгруппе $\langle x, x^h\rangle$, которая по условию не содержит элементов порядка 4. Итак, $N \leqslant C(x)$ и поэтому $N = \langle t\rangle$, где $t^2 = 1$. По лемме 12 элемент Nh фактор-группы H/N содержится в подгруппе $\langle Nx, Nx^h\rangle$ порядка 4 и значит $h \in \langle x, x^h, N\rangle = \langle x, x^h\rangle$. Это по условию невозможно.

Теперь предположим, что неверен пункт 2. Тогда $N = O_2(H)$ и $H = NA$, где $A \simeq A_5 \simeq SL_2(4)$. Поскольку N — неприводимый A_5-модуль над полем порядка 2, $|N| = 16$ и N либо естественный $SL_2(4)$-модуль, либо N можно получить из естественного 5-мерного подстановочного модуля группы A_5 над полем порядка 2 факторизацией по одномерному подмодулю. Так как в первом случае x действует при сопряжении без неподвижных точек на некоторой силовской 2-подгруппе из H, которая по пункту 1 должна быть элементарной абелевой, то этот случай невозможен и, следовательно, N — фактормодуль подстановочного модуля. В этом случае порождающие элементы $v_1, \ldots, v_4$ группы N могут быть выбраны так, что для каждого элемента a из группы A, которую мы отождествляем с A_5, выполнено равенство $v_i^a = v_{ia}$, $i = 1, \ldots, 5$, где $v_5 = v_1v_2v_3v_4$. Без ограничения общности можно считать, что $x = (1,2,3) \in A$. Положим $y = (1,2,4) \in A$, $v = v_1v_3$. Тогда $\langle x, y\rangle \simeq A_4$. Далее, $(vx)^3 = vxvxvx = vv^{x^2}v^x = v_1v_3v_3v_2v_2v_1 = 1$ и $v^{xy} = v_3v_4 \neq v$, поэтому $(vxy)^2 = vv^{xy} \neq 1$ и, следовательно, vxy — элемент порядка 4. С другой стороны, все элементы порядка 3 сопряжены с x и поэтому в силу предположения $\langle vx,\ y\rangle$ не может содержать элементов порядка 4. Это противоречие доказывает лемму. $\triangleright$

Лемма 14. *Если группа G с некоммутирующими порождающими x, y порядка 3 действует свободно на нетривиальной (аддитивной) абелевой группе и порядки n, m элементов xy, xy^{-1} конечны, то G конечна и изоморфна $SL_2(5)$ или $SL_2(3)$.*

$\triangleleft$ Заменив при необходимости y на y^{-1} можно считать, что $n \leqslant m$. Понятно, что G действует свободно, а следовательно и точно, на каждой нетривиальной G-инвариантной подгруппе из V. Пусть u — элемент из V. Поскольку $(ux^2 + ux + u)x = ux^2 + ux + u$ и G действует свободно на V, $ux^2 + ux + u = 0$ и

$$ux^{-1} = ux^2 = -u - ux \text{ для любого } u \in V. \tag{4}$$

Точно так же,

$$uy^{-1} = -u - uy \text{ для любого } u \in V. \tag{5}$$

Пусть теперь $v \in V$ — нетривиальный элемент. Определим $u_i = v(xy)^i$, $v_i = v(xy)^ix$, $i = 0, 1, \ldots, n-1$. Тогда, очевидно,

$$u_ix = v_i, \quad i = 0, 1, \ldots, n-1 \tag{6}$$

и по (4), (6)

$$v_ix = u_ix^2 = -u_i - u_ix = -u_i - v_i, \quad i = 0, 1, \ldots, n-1. \tag{7}$$

С другой стороны, по (6),

$$v_iy = u_ixy = u_{i+1} \text{ для } i < n-1, \quad v_{n-1}y = v(xy)^n = v = u_0. \tag{8}$$

Теперь (5) и (8) дают $v_i = u_{i+1}y^{-1} = -u_{i+1} - u_{i+1}y$ для $i < n-1$ и $v_{n-1} = u_0y^{-1} = -u_0 - u_0y$, поэтому

$$u_0y = -u_0 - v_{n-1}, \quad u_jy = -u_j - v_{j-1}, \quad j = 1, \ldots, n-1. \tag{9}$$

По (6)–(9) подгруппа $U = \langle u_i, v_i \big| \, i = 0, 1, \ldots, n-1\rangle$ является G-инвариантной. Если порядок элемента v конечен, то U и, следовательно, G конечны. В этом случае по лемме 8 U можно заменить на векторное пространство над полем комплексных чисел. Поэтому можно считать, что V без кручения, откуда следует, что U — конечномерный $\mathbb{Z}G$-модуль.

Очевидно, G действует свободно на $U \bigotimes_{\mathbb{Z}} \mathbb{C}$, и без потери общности можно предполагать, что этот $\mathbb{C}G$-модуль совпадает с V. Пусть $u \in V$ — собственный вектор для xy, т. е.

$$u(xy) = \lambda u, \tag{10}$$

где $\lambda \in \mathbb{C}$. По (5) и (10),

$$ux = \lambda u y^{-1} = \lambda(-u - uy). \tag{11}$$

Положим $w_1 = u$, $w_2 = ux$. Тогда (4), (5) и (11) показывают, что

$$w_1 x = w_2, \quad w_2 x = -w_1 - w_2, \quad w_1 y = -w_1 - \lambda^{-1} w_2, \quad w_2 y = \lambda w_1. \tag{12}$$

Отсюда следует, что подпространство W, порожденное элементами w_1, w_2, является G-инвариантным. Если W одномерно, то G абелева вопреки предположению. Если W двумерно, то w_1, w_2 составляют базу в W и (12) показывает, что G изоморфна подгруппе в $SL_2(\mathbb{C})$, порожденной матрицами

$$x = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad y = \begin{pmatrix} -1 & -\lambda^{-1} \\ \lambda & 0 \end{pmatrix}, \tag{13}$$

где λ — примитивный корень n-ой степени из единицы. Тогда $xy = \begin{pmatrix} \lambda & 0 \\ 1-\lambda & \lambda^{-1} \end{pmatrix}$, $xy^{-1} = \begin{pmatrix} -\lambda & -1 \\ \lambda & 1-\lambda^{-1} \end{pmatrix}$, где λ — примитивный корень n-ой степени из единицы. Если γ, $1/\gamma$ — характеристические корни элемента xy^{-1}, то след xy^{-1} равен $\gamma + \gamma^{-1} = 1 - \lambda - \lambda^{-1}$, т. е. $\gamma + \gamma^{-1} + \lambda + \lambda^{-1} = 1$. По лемме 11 число n равно 4 или 10, и лемма следует из леммы 6. $\triangleright$

3. Доказательство основных результатов

Доказательство теоремы 1. Если все элементы их X перестановочны, то $|G| = 3$ по лемме 9 и в этом случае заключение теоремы 1 верно. Поэтому в дальнейшем будем считать, что в X есть пара некоммутирующих элементов и значит в G по лемме 14 есть элемент z порядка 2. По лемме 9 z является единственной инволюцией в G. По леммам 1, 9, 14 для $\overline{G} = G/\langle z \rangle$ и образа $\overline{X}$ множества X в группе $\overline{G}$ выполнены следующие условия: любые два неперестановочных элемента из $\overline{X}$ порождают подгруппу, изоморфную $PSL_2(3) \simeq A_4$ или $PSL_2(5) \simeq A_5$, и любая конечная p-подгруппа из $\overline{G}$ является циклической группой или 2-группой диэдра. Таким образом, теорема 1 вытекает из следующего утверждения.

Предложение. *Пусть G — некоммутативная группа, порожденная таким инвариантным множеством X элементов порядка 3, что любые два неперестановочных элемента из X порождают подгруппу, изоморфную A_4 или A_5, и любая конечная 3-подгруппа из G является циклической, а любая конечная 2-подгруппа — двупорожденной. Тогда G изоморфна A_4 или A_5.*

$\triangleleft$ Скажем, что упорядоченная тройка (x, y, z) элементов $x, y, z \in G$ удовлетворяет условию T, если $x, y, z \in X$, $x \neq y \neq z \neq x$ и $(xy)^2 = (xz)^2 = 1$.

Лемма 15. *Пусть $H = \langle x, y, z \rangle$, где (x, y, z) удовлетворяет условию T.*
1) $(y^{-1}z)^x = yz^{-1}$ *и* $[y, z] \neq 1$.
2.1) *Если* $(xz^y)^2 = 1$, *то* $(yzy)^x = z^{-1}y$.
2.2) *Если* $(x^{-1}z^y)^2 = 1$, *то* $(y^{-1}zy^{-1})^x = y^{-1}z^{-1}$.

2.3) *Если* $(z^y z^{yx})^2 = 1$, *то* $(zy^{-1}z^{-1})^x \in \langle y, z\rangle$.

3) *Если* $x \notin B = \langle y, z\rangle$, *то* $B \simeq A_4$, $(yz)^2 = 1$ *и* $H \simeq A_5$.

$\lhd$ По предположению $yx = x^{-1}y^{-1}$, $zx = x^{-1}z^{-1}$ и поэтому $(y^{-1}z)^x = (x^{-1}y^{-1})(zx) = (yx)(x^{-1}z^{-1}) = yz^{-1}$. Если $[y, z] = 1$, то $(y^{-1}z)^x = (y^{-1}z)^{-1}$. Поскольку порядок x равен 3, $y^{-1}z = (y^{-1}z)^{-1}$ и поэтому $y^2 = z^2$, т. е. $y = z$, что противоречит предположению. Это доказывает 1).

Пусть $(xz^y)^2 = 1$. Тогда $1 = (z^y x)^2 = y^{-1}z(yx)y^{-1}zyx = y^{-1}zx^{-1})y^{-1}y^{-1}zyx = y^{-1}z(yzy)^x$, что доказывает 2.1). Доказательство 2.2) подобным же образом вытекает из равенств $1 = (z^y x^{-1})^2 = y^{-1}zyx^{-1}y^{-1}zyx^{-1} = y^{-1}zy^{-1}xzyx^{-1}$.

Если $(z^y z^{yx})^2 = 1$, то использование 1) дает $z^y z^{yx} = y^{-1}zyx^{-1}y^{-1}zyx = y^{-1}zy(y^{-1}z)^x x^{-1}yx = y^{-1}zyyz^{-1}x^{-1}(yx) = y^{-1}zy^2z^{-1}xy^{-1}$, и поэтому $1 = (z^y z^{yx})^2 = y^{-1}zy^2z^{-1}x(y^{-1}y^{-1})zy^2z^{-1}xy^{-1} = y^{-1}zy^2z^{-1}(xy)zy^2z^{-1}xy^{-1} = y^{-1}zy^2z^{-1}y^{-1}(x^{-1}zy^2z^{-1}x)y^{-1}$, откуда вытекает, что $(zy^{-1}z^{-1})^x = x^{-1}(zy^2z^{-1})x \in \langle y, z\rangle$. Это доказывает 2.3).

Пусть $x \notin B$. Докажем вначале, что $x \notin N_H(B)$. Предположим противное. Тогда B нормальна в H и поэтому $y^H \subseteq B$. Так как $(xy)^2 = x^3 = 1$, то $xy^{-1} = y^x \in B$, т. е. $x \in B$.

По 1) $[y, z] \neq 1$. Если $(yz)^2 = 1$, то по пункту 2) леммы 4 $B \simeq A_4$ и $H \simeq A_5$. Таким образом, по пунктам 1) и 3) леммы 4 можно считать, что либо $(y^{-1}z)^2 = 1$ и $B \simeq A_4$, либо $B \simeq A_5$ и $(y^{-1}z)^5 = 1$. Кроме того, либо $[x, z^y] = 1$, либо $(xz^y)^2 = 1$, либо $(x^{-1}z^y)^2 = 1$, либо $(z^y z^{yx})^2 = 1$.

Если $[x, z^y] = 1$, то по 1) $\langle z^y, y^{-1}z\rangle^x \leqslant B$. Однако $\langle z^y, y^{-1}z\rangle = \langle y^{-1}zy, y^{-1}z\rangle = B$, поэтому $x \in N_H(B)$, что противоречит условию.

Если $(x^{-1}z^y)^2 = 1$, то по 1) и 2.2) $B^x = \langle y^{-1}z, y^{-1}zy^{-1}\rangle^x \leqslant B$, что невозможно.

Если $(z^y z^{yx})^2 = 1$, то по 1) и 2.3) $W^x \leqslant B$, где $W = \langle y^{-1}z, zy^{-1}z^{-1}\rangle$ и поэтому $W \neq B$. В случае, когда $(y^{-1}z)^2 = 1$, это невозможно, поскольку порядок элемента $zy^{-1}z^{-1}$ равен 3 и $\langle y, z\rangle \simeq A_4$. В случае, когда $\langle y, z\rangle \simeq A_5$, это также невозможно, поскольку при таких обстоятельствах порядок первого порождающего элемента группы W равен пяти, а второго — трем.

Итак, $(xz^y)^2 = 1$, и по 1) и 2.1) $\langle y^{-1}z, yzy\rangle^x \leqslant B$. Следовательно $W = \langle y^{-1}z, yzy\rangle = \langle y^{-1}z, (y^{-1}z)^y\rangle \neq B$. Если $B \simeq A_5$, то порядок $y^{-1}z$ равен 5 и, поскольку $\langle y^{-1}z\rangle \neq \langle (y^{-1}z)^y\rangle$, подгруппа W совпадает с B. Отсюда $B \simeq A_4$ и неравенство $W \neq B$ возможно только если $y^{-1}z$ порядка 2. В этом случае $W = O_2(B)$ и поэтому W нормальна в H. Поскольку образы элементов y и z в H/W совпадают, H/W изоморфна фактору $\langle x, y\rangle \simeq A_4$. Таким образом, H содержит нормальную 2-подгруппу индекса 3, и теперь 3) следует из леммы 13. $\rhd$

Рассмотрим вначале случай, когда любые два неперестановочных элемента из X порождают подгруппу, изоморфную A_4. Пусть $x, y \in X$ такие, что $A = \langle x, y\rangle \simeq A_4$. Если $A \neq G$, то существует такой элемент $z \in X$, что $z \notin A$ и $[x, z] \neq 1$. Тогда $\langle x, z\rangle \simeq A_4$ и без потери общности $(xy)^2 = (xz)^2 = 1$. По пункту 2) леммы 15 $D \simeq A_5$. Однако все элементы порядка 3 в A_5 сопряжены и два из них порождают A_5. Это противоречит условию. Таким образом, X содержит пару элементов, порождающих подгруппу H, изоморфную A_5. Поскольку все элементы порядка 3 в A_5 сопряжены, любой элемент из X сопряжен в G со своим обратным элементом. Кроме того, H содержит такие различные элементы b, c, d из X, что $(bc)^2 = (bd)^2 = (cd)^2 = 1$. Наша цель — показать, что $H = G$. В противном случае существует такой элемент x из X, что с точностью до переобозначений выполнены условия следующей леммы, доказательство которой завершает доказательство предложения и теоремы 1, поскольку в A_6 силовская 3-подгруппа не является циклической. $\rhd$

Лемма 16. *Пусть x, b, c, d — различные элементы из X, для которых $(xb)^2 = (bc)^2 = (bd)^2 = (cd)^2 = 1$ и $x \notin A = \langle b, c, d\rangle$.*

1) *Если $(xc)^2 = 1$, то $(xd)^2 = 1$.*

2) *Существует такой элемент $a \in X$, что $(ab)^2 = 1$ и либо $a \in \langle x, b, c\rangle$ и $(ac)^2 = 1$, либо $a \in \langle x, b, d\rangle$ и $(ad)^2 = 1$. В частности, $\langle x, b, c, d\rangle = \langle a, b, c, d\rangle \simeq A_6$.*

$\lhd$ По пункту 2) леммы 4 $A \simeq A_5$.

1) Отметим, что (b, x, c) и (b, x, d) satisfy the condition T. Если $\langle x, d\rangle \simeq A_5$, то по п. 3) леммы 15 $b, c \in \langle x, d\rangle$. Отсюда $\langle x, b, c, d\rangle = \langle x, d\rangle \simeq A_5 \simeq A$ и поэтому $x \in A$, что противоречит условию. Следовательно, $\langle x, d\rangle \not\simeq A_5$ и по п. 1) леммы 15 $\langle x, d\rangle \simeq A_4$. Если $(xd)^3 = 1$, то по п. 3) леммы 15 b, c нормализуют $B = O_2(\langle b, d\rangle)$ и поэтому $A \simeq A_5$ нормализует B. Отсюда A централизует B, что неверно. Таким образом, $(xd)^2 = 1$.

2) Если x, b, c порождают подгруппу, изоморфную A_5, то по п. 5) леммы 4 существует такой элемент $a \in \langle x, b, c\rangle \cap X$, что $\langle a, b, c\rangle = \langle x, b, c\rangle$ и $(ab)^2 = (ac)^2 = 1$. По п. 1) $(ad)^2 = 1$, и лемма в этом случае верна.

Итак, можно считать, что $\langle x, b, c\rangle \not\simeq A_5$, а из-за симметрии между c и d, что также $\langle x, b, d\rangle \not\simeq A_5$. По п. 3) леммы 15 b, c нормализуют $O_2(\langle x, d\rangle)$, и противоречие получается так же, как в доказательстве п. 1).

Доказательство теоремы 2. Пусть G — конечная группа, порожденная элементами простых порядков и действующая свободно на абелевой группе.

Пусть вначале $C = \langle x \in G \,\big|\, x^3 = 1\rangle$ — циклическая группа.

Лемма 17. *G — циклическая группа, порядок которой свободен от квадратов.*

$\lhd$ Индукция по порядку группы. Покажем вначале, что G обладает нормальным 2-дополнением. В противном случае по лемме 1. 3) в G силовская 3-подгруппа нетривиальна и $|C| = 3$. Если $N_G(C) = C_G(C)$, то по лемме 1, 2) G обладает нормальным 3-дополнением и, следовательно, силовская 3-подгруппа имеет порядок 3 и лежит в центре G. Но тогда G обладает нормальным 2-дополнением. Если же $N_G(C) \neq C_G(C)$, то в $N_G(C) \setminus C_G(C)$ все элементы имеют непростые порядки, что невозможно. Понятно теперь, что порядок силовской 2-подгруппы не превосходит числа 2, поэтому все силовские подгруппы из G являются циклическими и G — метациклическая группа по лемме 1, 1). Если p — наименьшее простое число, делящее $|G|$, то по лемме 1, 2) G обладает нормальным p-дополнением Q. Понятно, что индекс этого дополнения равен p и элемент x порядка p по лемме 9 централизует любую силовскую подгруппу из G, которую он нормализует. Поэтому x лежит в центре G и $G = Q \times \langle x\rangle$. Теперь утверждение леммы вытекает из индукционного предположения. $\rhd$

Пусть C — нециклическая группа. По теореме 1 G изоморфна $SL_2(3)$ или $SL_2(5)$. В любом случае $|G : C_G(C)C| \leqslant 2$. Если $|G : C_G(C)C| = 2$, то G не может быть порождена элементами простых порядков, поэтому $G = C_G(C)C$ и по лемме 9 $(|C|, |C_G(C)|) \leqslant 2$. Понятно теперь, что порядок $C_G(C)$ свободен от квадратов и что строение G соответствует заключению теоремы.

Пусть теперь подгруппа G_0 нетривиальной группы G, порожденная всеми элементами простых порядков, является прямым произведением циклической холловой подгруппы $Z = \langle z\rangle$, порядок которой свободен от квадратов, и группы, изоморфной $SL_2(5), SL_2(3)$ или тривиальной группе. Пусть $\zeta \in \mathbb{C}$— примитивный корень степени $|Z|$ из единицы. Если $Z \neq 1$, то она действует свободно на двумерном векторном пространстве V на $\mathbb{C}$ умножением каждого $v \in V$ на соответствующую степень ζ. Легко проверить, что действие $S = SL_2(p)$, $p = 2, 3$, на V, описанное в доказательстве леммы 14, является свободным. Кроме того, оно продолжается до свободного действия группы $Z \times S$, если

$(|S|, |Z|) = 1$. Очевидно, действие группы G на V^G, индуцированное описанным действием G_0 на V, является свободным.

Доказательство теоремы 3. По теореме 1 $C = \langle x \in G \big| \, x^3 = 1 \rangle$ изоморфна $SL_2(5)$. Так как $|\operatorname{Out}(C)| = 2$ и $C_G(C)$ по леммам 9 и 1, п. 1) — метациклическая группа, порядок которой взаимно прост с числом 15, а силовская 2-подгруппа имеет порядок 2, то заключение теоремы справедливо.

Литература

1. *Zassenhaus H.* Über endliche Fastkörper // Abh. Math. Semin. Univ. Hambburg.—1935.—V. 11.—P. 187–220.
2. *Wolf J. A.* Spaces of constant curvature.—Berkley: Univ. of California press, 1972.—408 p.—(Пер. на рус. яз: Вольф Дж. Пространства постоянной кривизны.—М.: Наука, 1982.—480 с.)
3. *Мазуров В. Д.* Характеризация знакопеременных групп // Алгебра и логика.—2005.—Т. 44, № 1.—С. 54–69.
4. *Холл М.* Теория групп.—М.: ИЛ, 1962.—468 с.
5. *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп.—М.: Наука, 1972.—240 с.
6. *Кострикин А. И.* Введение в алгебру.—М.: Наука, 1977.—495 с.
7. *Carmichael R. D.* Introduction to the theory of groups of finite order.—Boston, 1937.—447 p.

Статья поступила 24 января 2008 г.

Мазуров Виктор Данилович
Институт математики СО РАН
Новосибирск, 630090, РОССИЯ
E-mail: mazurov@math.nsc.ru