МАТЕМАТИКА

УДК 512.543 MSC 20D99
DOI 10.17223/19988621/55/1

А.И. Забарина, Е.А. Фомина

О МНОЖЕСТВЕ $K_3(G)$ ЭЛЕМЕНТОВ КОНЕЧНЫХ ГРУПП, КОММУТИРУЮЩИХ РОВНО С ТРЕМЯ ЭЛЕМЕНТАМИ ГРУППЫ

Рассмотрены свойства множества $K_3(G)$, состоящего из элементов третьего порядка, каждый из которых перестановочен ровно с тремя элементами группы. В частности, из полученных результатов следует, что все инволюции конечной простой неабелевой группы G с непустым множеством $K_3(G)$ образуют один класс сопряжённых элементов (этот факт был сформулирован в [3] в качестве упражнения)

Ключевые слова: *группа*, *инволюция*, *центр группы*, *нормальный делитель.*

Как известно, при доказательстве классификационной теоремы конечных простых групп важную роль сыграло исследование свойств централизатора инволюций [1, с. 10]

В [2] изучены некоторые свойства конечных групп, каждая инволюция которых обладает двухэлементным централизатором.

В настоящей работе рассматриваются конечные группы, в которых существуют элементы порядка 3, перестановочные ровно с тремя элементами группы. Множество всех таких элементов группы G обозначено $K_3(G)$.

В частности показано, что в каждой конечной простой неабелевой группе с непустым множеством $K_3(G)$ все инволюции образуют один класс сопряженных элементов [3].

1. О мощности множества $K_3(G)$

Пусть G – произвольная конечная мультипликативная группа, $|G| = n$.

Обозначим через $K_3(G)$ множество $\{x \in G \mid x \neq e, |C_G(x)| = 3\}$.

Другими словами, элемент $x \neq e$ принадлежит $K_3(G)$ тогда и только тогда, когда он перестановочен ровно с тремя элементами группы G. Так как централизатор $C_G(g)$ является подгруппой группы G, то

$$K_3(G) = \{x \in G \mid C_G(x) = \{e, x, x^2\}\}.$$

Очевидно, что для абелевой группы G множество $K_3(G)$ не пусто в точности тогда, когда G – циклическая группа третьего порядка. Поэтому, в дальнейшем, будем считать, что группа G неабелева.

Из определения $K_3(G)$ непосредственно вытекает, что:

A) если $x \in K_3(G)$, то порядок этого элемента равен трём: $o(x) = 3$;

B) если $x \in K_3(G)$, то $x^2 \in K_3(G)$.

Рассмотрим некоторые свойства множества $K_3(G)$.

Предложение 1. Если $K_3(G)$ не пусто, то $|G|$ делится на 3 и не делится на 9.

Доказательство. Справедливость утверждения вытекает непосредственно из теоремы Силова [4, с. 99] и свойства коммутативности группы порядка p^2 [5, с. 63]. #

Предложение 2. Множество $K_3(G)$ является инвариантным подмножеством G, то есть если $x \in K_3(G)$, то $x^g \in K_3(G)$ для каждого $g \in G$.

Доказательство. Воспользуемся известным равенством:

$$\forall_G x\ \forall_G g\ C_G(x^g) = (C_G(x))^g.$$

Пусть $x \in K_3(G)$; Тогда $a \in C_G(x^g) \Leftrightarrow a \in \{e, x, x^2\}^g \Leftrightarrow a \in \{e, x^g, (x^g)^2\}$.#

Предложение 3. Пусть $K_3(G) \neq \varnothing$, $x \in G$ и $o(x) = 3$. Тогда $x \in K_3(G)$.

Доказательство. Согласно предложению 1, $\langle x\rangle$ – силовская 3-подгруппа группы G. Из теоремы Силова следует, что для каждого $k \in K_3(G)$ подгруппы $\langle x\rangle$ и $\langle k\rangle$ сопряжены в G. Осталось применить предложение 2. #

Предложение 4. Пусть $|G| = n$; $K_3(G) \neq \varnothing$. Тогда $\left|K_3(G)\right| \in \left\{\frac{n}{3};\ \frac{2n}{3}\right\}$.

Доказательство. Пусть $x \in K_3(G)$. Так как $|G| = |C_G(x)|\cdot|x^G| = 3\cdot|x^G| = n$, то $\left|x^G\right| = \frac{n}{3}$. Заметим, что $e \notin K_3(G)$.

Следовательно, существует не более двух классов сопряжённых друг другу элементов группы G, каждый из которых (в силу предложения 2) является элементом $K_3(G)$. Таким образом, в силу непустоты множества $K_3(G)$, получаем, что $\left|K_3(G)\right| \in \left\{\frac{n}{3};\ \frac{2n}{3}\right\}$. #

Лемма 5. Пусть $a, g \in G$, $o(a) = 3$; $g^{-1}ag = a^2$. Тогда $o(g)\,\vdots\,2$.

Доказательство. Пусть $o(g) = 2k + 1$. Так как по условию $ag = ga^2$, то

$$(ag)^2 = ga^2\cdot ag = g^2.$$

Следовательно,

$$o((ag)^2) = o(g^2) = \frac{2k+1}{(2k+1;\ 2)} = 2k + 1.$$

Отсюда,
$$((ag)^2)^{2k+1} = (ag)^{4k+2} = e. \tag{*}$$

С другой стороны,

$$(ag)^{2k+1} = ((ag)^2)^k\cdot ga^2 = (g^2)^k\cdot ga^2 = a^2.$$

Следовательно,
$$(ag)^{4k+2} = a.$$

Получили противоречие с (*). Значит, $o(g)\,\vdots\,2$. #

Предложение 6. 1) Пусть $o(a) = 3$ и $g^{-1}ag = a^2$. Тогда $|G|\,\vdots\,6$.

2) Если порядок G нечётен, то либо $K_3(G)$ пусто, либо $\left|K_3(G)\right| = \frac{2|G|}{3}$.

Доказательство. Справедливость утверждения 1) непосредственно вытекает из леммы 5.

2) Пусть $|G| = 2m + 1$ и $K_3(G) \neq \varnothing$. Тогда $\forall a \in K_3(G)\ \forall_G g\ (a^g \not\approx a^2)$, то есть в G существует ровно 2 класса сопряжённых элементов множества $K_3(G)$. Согласно предложению 4, $\left|K_3(G)\right| = \frac{2|G|}{3}$. #

Рассмотрим несколько примеров множеств $K_3(G)$ в различных группах.

1) S_n, $n \geq 2$.

Если $n \geq 6$, то $|S_n| \vdots 9$. Согласно предложению 1, для указанных групп $K_3(S_n) = \varnothing$.

Пусть $n = 3$. Так как в S_n каждые две подстановки сопряжены тогда и только тогда, когда они имеют одинаковое циклическое строение [5, с. 66], то

$$[(123)]^{S_3} = \{(123),(132)\}.$$

Следовательно, $$\left|C_{S_3}(123)\right| = \frac{6}{2} = 3.$$

Таким образом, $$K_3(S_3) = \{(123), (132)\},\ \left|K_3(S_3)\right| = \frac{|S_3|}{3}.$$

Рассмотрим группы S_4 и S_5. Очевидно, множество X всех элементов третьего порядка в каждой из них есть множество всех трёхчленных циклов. Для $n = 4$ $\left|X\right| = \frac{4 \cdot 3 \cdot 2}{3} = 8$. Каждые два элемента из множества X сопряжены. Следовательно, $\forall a \in X\ \left|C_{S_4}(a)\right| = 3$. Таким образом, $K_3(S_4) = X$, $\left|K_3(S_4)\right| = \frac{|S_4|}{3}$. Аналогично, в S_5 $\forall a \in X\ \left|C_{S_5}(a)\right| = 6$, то есть $K_3(S_5) = \varnothing$.

2) Покажем, что $K_3(A_n) \neq \varnothing \Leftrightarrow n \in \{3, 4, 5\}$.

Так как при $n > 5$ $|A_n| \vdots 9$, то согласно предложению 1, для соответствующих групп $K_3(A_n) = \varnothing$.

При $n = 3$ имеем

$$K_3(A_3) = K_3(S_3), \text{ так как } A_3 \text{ – абелева; } \left|K_3(A_3)\right| = \frac{2|A_3|}{3}.$$

При $n = 4$ имеем

$$K_3(S_4) \subset A_4 \text{ и, следовательно, } K_3(A_4) = K_3(S_4);\ \left|K_3(A_4)\right| = \frac{2|A_4|}{3}.$$

Рассмотрим, наконец, A_5. Пусть $a = (\alpha\beta\gamma)$ – произвольный трёхчленный цикл. Очевидно, $C_{S_5}(a) = \{e, a, a^2, c, ac, a^2c\}$, где c – двучленный цикл, не пересекающийся с a. Так как c, ac, a^2c – нечётные подстановки, то $C_{A_5}(a) = \{e, a, a^2\}$. Следовательно, $K_3(A_5)$ – множество всех трёхчленных циклов, то есть $\left|K_3(A_5)\right| = 20 = \frac{|A_5|}{3}$.

3) Рассмотрим диэдральную группу D_{2n}, где

$$D_{2n} = \{(a, \varepsilon) \mid a \in C_n, \varepsilon = \pm 1\},\ n \geq 3 \text{ [6, с. 31]}$$

и $$(a_1, \varepsilon_1)\cdot(a_2, \varepsilon_2) = \left(a_1 a_2^{\varepsilon_1},\ \varepsilon_1\varepsilon_2\right).$$

Пусть $X = \{(a, \varepsilon) \mid o((a, \varepsilon)) = 3\}$. Легко видеть, что $(a, \varepsilon) \in X \Leftrightarrow o(a) = 3$ и $\varepsilon = 1$. Однако

$$\forall g \in C_n\ (g, 1)\cdot(a, 1) = (ga, 1) = (ag, 1) = (a, 1)\cdot(g, 1).$$

Отсюда следует, что в каждой группе D_{2n}, $n \geq 4$, множество $K_3(D_{2n})$ пусто. Заметим, что $D_6 \cong S_3$.

4) Пусть G – конечная нильпотентная группа, $|G| = 3^{\alpha_1} p_2^{\alpha_2} ... p_k^{\alpha_k}$, $k > 1$. Тогда согласно теореме Бернсайда – Виланда [4, с. 155],

$$G = H_1 \times H_2 \times \ldots \times H_k,$$

где H_i – соответствующие силовские подгруппы.

а) Если $\alpha_1 > 1$, то согласно предложению 1, $K_3(G) = \varnothing$.

b) Пусть $\alpha_1 = 1$, $x \in G$, $o(x) = 3$. Так как в каждой нильпотентной группе любая нетривиальная нормальная подгруппа имеет нетривиальное пересечение с центром [4, с. 148], то $H_1 \subset Z(G)$. Так как $Z(G) \cap H_2 \neq \{e\}$, то $H_1 \neq Z(G)$. Следовательно, $x \notin K_3(G)$.

Таким образом, в каждой конечной нильпотентной группе G, отличной от циклической группы третьего порядка, множество $K_3(G)$ является пустым.

5) Приведём пример семейства разрешимых групп, в каждой из которых множество $K_3(G)$ не пусто.

Пусть q – простое число, $q \equiv 1 \pmod 3$. Рассмотрим группу $\langle \mathbf{Z}_q^*, \cdot\rangle$. Так как $|\mathbf{Z}_q^*| = q - 1$, то существует элемент $r' \in \mathbf{Z}_q^*$, такой, что $o(r') = 3$. Следовательно, существует элемент $r \in \mathbf{N}$, такой, что

$$r^3 \equiv 1 \pmod q \wedge r \not\equiv 1 \pmod q \tag{1}$$

Пусть $G = \{a^u b^v \mid u \in \{0, 1, 2\},\ v \in \overline{0,\ q-1}\}$. Воспользуемся следующей бинарной алгебраической операцией на G [5, с. 61]:

$$a^{u_1} b^{v_1} a^{u_2} b^{v_2} = a^{u_1+u_2} b^{(v_1 \cdot r^{u_2} + v_2)}. \tag{2}$$

Непосредственно проверяется, что $\langle G, \cdot\rangle$ – неабелева группа порядка $3q$, в которой

$$e = a^0 b^0, \ \left(a^u b^v\right)^{-1} = a^{3-u} b^{-(r^{3-u} v)}.$$

Покажем, что в построенной группе $|K_3(G)| = \dfrac{2 \cdot 3q}{3} = 2q$. Согласно предложению 6, достаточно убедиться, что $a \in K_3(G)$. Пусть

$$a \cdot a^u b^v = a^u b^v \cdot a.$$

Отсюда

$$a^{u+1} b^v = a^{u+1} b^{vr},$$

то есть

$$v(r-1) \ \vdots\ q.$$

Так как $r \not\equiv 1 (\mathrm{mod}\ q)$, то $v = 0$.

Следовательно, $C_G(a) = \{e, a, a^2\}$, то есть $a \in K_3(G)$.

Таким образом, G – разрешимая группа, не являющаяся нильпотентной. Так, например, пусть $q = 7$. Тогда $r = 2$, $|G| = 21$.

$$G = \{a^u b^v \mid u \in \{0, 1, 2\},\ v \in \overline{0;\ 6}\}.$$

$$a^{u_1} b^{v_1} \cdot a^{u_2} b^{v_2} = a^{u_1+u_2} b^{(v_1 \cdot 2^{u_2} + v_2)}.$$

Непосредственные вычисления показывают, что

$$K_3(G) = \{ab^i \mid i \in \overline{0;\ 6}\} \cup \{a^2 b^i \mid i \in \overline{0;\ 6}\}.$$

2. О сопряжённости инволюций в конечных простых группах с непустым множеством $K_3(G)$

Обратимся теперь к простым группам. Нашей целью является доказательство следующего утверждения.

Теорема 7. Пусть G – конечная простая группа, $|G| = n$, $K_3(G) \neq \varnothing$. Тогда все инволюции G образуют один класс сопряжённых элементов.

Постановка задачи взята в [3, с. 81].

Доказательство теоремы опирается на следующее утверждение, доказанное в [3, с. 80]:

Пусть G – конечная простая группа и A – подгруппа нечётного порядка, такая, что:

1) $\forall g \in G \setminus N_G(A)\ (A \cap A^g = \{e\})$;

2) $N_G(A) = (A \leftthreetimes \langle i^* \rangle) \times B$, где $(|A|, |B|) = 1$, i^* – инволюция, инвертирующая каждый элемент из A (говорят, что элемент x группы G *инвертирует* элемент y, если $x^{-1}yx = y^{-1}$).

Тогда каждая инволюция $i \in G$ сопряжена с некоторой инволюцией из множества i^*B.

Приведём также формулировку теоремы Бернсайда [5, с. 227].

Теорема 8 (Бернсайда). Если силовская подгруппа P конечной группы G содержится в центре своего нормализатора, то группа G обладает таким нормальным делителем H, что в качестве представителей смежных классов по H можно выбрать элементы группы P.

Обратимся к доказательству теоремы 7.

Доказательство (теоремы 7). Пусть $k \in K_3(G)$ и $A = \langle k \rangle$. Убедимся, что A удовлетворяет 1) и 2), причём подгруппа B из равенства 2) оказывается единичной.

a) Так как $o(k) = 3$, то

$$\forall_G g\ (g \notin N_G(A) \Rightarrow g^{-1}Ag \cap A = \{e\}),$$

то есть условие 1) выполнено.

b1) Пусть $H = N_G(A)$. Докажем, что $H \neq A$.

Действительно, согласно предложению 1, группа A является силовской подгруппой группы G. Если $H = A$, то A содержится в центре своего нормализатора. Согласно теореме 8, группа G обладает нормальным делителем порядка $\frac{n}{3}$, что противоречит свойству простоты группы G.

b2) Покажем, что $|H| \vdots 2$ и каждая инволюция из H инвертирует все элементы из A.

Пусть $g \in H \setminus A$. Тогда, согласно определению $K_3(G)$,

$$gkg^{-1} = k^{-1},\ g^{-1}k^2g = (k^2)^{-1}. \qquad (3)$$

Согласно лемме 5, $|H| \vdots 2$. Кроме того, согласно (3), каждая инволюция i из H инвертирует все элементы A. Пусть i^* – одна из них.

b3) Пусть $L = A \cdot \langle i^* \rangle$. Покажем, что $L = A \leftthreetimes \langle i^* \rangle$.

Так как $L = A \cdot \langle i^* \rangle = \langle i^* \rangle \cdot A$, то $L < H$. Так как $A \triangleleft L$, $A \cap \langle i^* \rangle = \{e\}$, то $L = A \leftthreetimes \langle i^* \rangle$, $|L| = 6$.

Следовательно, из некоммутативности этой группы получаем $L \cong S_3$. Согласно теореме Гёльдера [7, с. 82], L – совершенная группа.

b4) Убедимся, что $H = L \times C_H(L)$.

Согласно свойству совершенных групп [7, с. 268], достаточно показать, что $L \lhd H$.

Заметим, что множество всех инволюций группы H есть $\{i^*, i^*k, i^*k^2\}$. Действительно, согласно (3) все указанные элементы являются инволюциями группы H.

Пусть $i \in H$, $o(i) = 2$. Тогда из (3)

$$iki = i^*ki^*,$$

то есть

$$(i^*i)k = k(i^*i),$$

отсюда $i^*i \in A$, то есть $i \in \{i^*, i^*k, i^*k^2\}$.

Учитывая, наконец, тот факт, что $A \lhd H$, получаем

$$\forall_H h\ \forall_L l\ (h^{-1}lh = h^{-1}a(i^*)^m h = a_1 i_1),$$

где $a_1 \in A$, $i_1 \in L$. Таким образом, $L \lhd H$.

b5) Покажем, что $C_H(L) = \{e\}$.

Пусть $x \in C_H(L)$. Тогда $xk = kx$ и $xi^* = i^*x$. Следовательно, $x = e$. Таким образом,

$$N_G(A) = (A \rtimes \langle i^* \rangle) \times B, \text{ где } |B| = 1.$$

Тем самым равенство 2) доказано и, следовательно, каждая инволюция i из G сопряжена с инволюцией i^*. #

Так как $K_3(A_5) \neq \varnothing$, то все инволюции A_5 образуют один класс сопряжённых элементов.

Порядки всех спорадических простых групп, за исключением группы Янко J_1, делятся на 3^2 [1, с. 145]. Обратимся к J_1. Согласно её строению [1, с. 93], в ней существует инволюция i, перестановочная с некоторым элементом c, таким что $o(c) = 3$. Следовательно, в J_1 существует элемент порядка 6, то есть $K_3(J_1) = \varnothing$. Таким образом, в каждой спорадической группе G множество $K_3(G)$ пусто.

Авторы благодарят за помощь в написании работы доктора физ.-мат. наук В. А. Белоногова, одного из авторов книг [3, 6].

Авторы искренне благодарны рецензенту за тщательно проделанную работу.

ЛИТЕРАТУРА

1. *Горенстейн Д.* Конечные простые группы: введение в их классификацию. М.: Мир, 1985. 352 с.
2. *Забарина А.И., Гусельникова У.А., Фомина Е.А.* О коммутирующих элементах группы // Вестник Томского государственного университета. Математика и механика. 2015. № 6(38). С. 27–32. DOI 10.17223/19988621/38/3.
3. *Белоногов В.А., Фомин А.Н.* Матричные представления в теории конечных групп. М.: Наука, 1976. 126 с.
4. *Каргаполов М.И., Мерзляков Ю.И.* Основы теории групп. М.: Наука, 1982. 288 с.
5. *Холл М.* Теория групп. М.: ИЛ, 1962. 468 с.
6. *Белоногов В.А.* Задачник по теории групп. М.: Наука, 2000. 240 с.
7. *Курош А.Г.* Теория групп. М.: Физматлит, 1967. 808 с.

Статья поступила 06.03.2018 г.

Zabarina A. I., Fomina E. A. (2018) ON THE SET $K_3(G)$ OF FINITE GROUPS' ELEMENTS COMMUTING EXACTLY WITH THREE ELEMENTS *Vestnik Tomskogo gosudarstvennogo universiteta. Matematika i mekhanika* [Tomsk State University Journal of Mathematics and Mechanics]. 55. pp. 5–11

DOI 10.17223/19988621/55/1

Keywords: group, involution, center of a group, normal subgroup.

Let G be an arbitrary finite multiplicative group, $|G| = n$. We define the set $K_3(G)$ as follows:

$$K_3(G) = \{x \in G \mid |C_G(x)| = 3\} = \{x \in G \mid C_G(x) = \{e, x, x^2\}\}.$$

It follows from the definition of $K_3(G)$ that

A) if $x \in K_3(G)$, then the order of x is 3 ($o(x) = 3$);

B) if $x \in K_3(G)$, then $x^2 \in K_3(G)$.

The following properties of the set $K_3(G)$ have been proved.

Proposition 1. If $K_3(G) \neq \varnothing$, then $|G| \vdots 3$ and $|G| \not\vdots 9$.

Proposition 2. If $x \in K_3(G)$, then $x^g \in K_3(G)$ for each $g \in G$.

Proposition 3. Let $K_3(G) \neq \varnothing$, $x \in G$ and $o(x) = 3$. Then $x \in K_3(G)$.

Proposition 4. Let $|G| = n$; $K_3(G) \neq \varnothing$. Then $\left|K_3(G)\right| \in \left\{\frac{n}{3};\ \frac{2n}{3}\right\}$.

Lemma 5. Let $a, g \in G$, $o(a) = 3$; $g^{-1}ag = a^2$. Then $o(g) \vdots 2$.

Proposition 6. 1) Let $o(a) = 3$ and $g^{-1}ag = a^2$. Then $|G| \vdots 6$.

2) If $|G| = 2k + 1$, then $K_3(G) = \varnothing$ or $\left|K_3(G)\right| = \dfrac{2|G|}{3}$.

Theorem 7. Let G be a finite simple group, $|G| = n$, $K_3(G) \neq \varnothing$. Then all involutions of the group G form a class of conjugate elements.

AMS Mathematical Subject Classification: 20D99

ZABARINA Anna Ivanovna (Candidate of Physics and Mathematics, Tomsk State Pedagogical University, Tomsk, Russian Federation). E-mail: aizabarina@gmail.com

FOMINA Elena Anatolievna (Candidate of Physics and Mathematics, Tomsk State Pedagogical University, Tomsk, Russian Federation). E-mail: ef254@mail.ru

REFERENCES

1. Gorenstein D. (1982) *Finite Simple Groups: An Introduction to Their Classification*. New York: Springer Science & Business Media. 333 p.
2. Zabarina A.I., Guselnikova U.A., Fomina E.A. (2015) O kommutiruyushchikh elementakh gruppy [On commuting elements of a group]. *Vestnik Tomskogo gosudarstvennogo universiteta. Matematika i mekhanika – Tomsk State University Journal of Mathematics and Mechanics*. 6(38). pp. 27–32. DOI: 10.17223/19988621/38/3.
3. Belonogov V.A., Fomin A.N. (1976) *Matrichnye predstavleniya v teorii konechnykh grupp* [Matrix representations in the theory of finite groups]. Moscow: Nauka. 126 p.
4. Kargapolov M.I., Merzlyakov Y.I. (1982) *Osnovy teorii grupp* [Foundations of the group theory]. Moscow: Nauka. 288 p.
5. Hall M. (1959) *The Theory of Groups*. New York: The Macmillan Company. 434 p.
6. Belonogov V.A. (2000) Zadachnik po teorii grupp [Problem book on the group theory]. Moscow: Nauka. 240 p.
7. *Kurosh A.G.* (1960) *The Theory of Groups*. New York: Chelsea Publishing Company. 272 p.