Сибирский математический журнал
Сентябрь—октябрь, 2007. Том 48, № 5

УДК 512.544

О МИНИМАЛЬНЫХ НЕГРУППОВЫХ СКРУЧЕННЫХ ПОДМНОЖЕСТВАХ, СОДЕРЖАЩИХ ИНВОЛЮЦИИ

А. Л. Мыльников

Аннотация: Подмножество K группы G называется *скрученным*, если $1 \in K$ и для любых $x, y \in K$ элемент $xy^{-1}x$ принадлежит K. Исследуются конечные скрученные подмножества с инволюцией, которые сами не являются подгруппами, но любое собственное скрученное подмножество в них — подгруппа. Исследуются группы, порожденные такими скрученными подмножествами.

Ключевые слова: скрученное подмножество, скрученная подгруппа.

Определение 1 [1]. Подмножество K из группы G называется *скрученным*, если $1 \in K$ и $xy^{-1}x \in K$ для любых элементов $x, y \in K$.

Интерес к скрученным подмножествам вызван прежде всего тем, что они связаны с инволютивными автоморфизмами группы (подробно эта связь изложена в работах Ашбахера [2] и автора [3]).

Понятно, что любая подгруппа в группе является скрученным подмножеством, но обратное не всегда верно (примером такого скрученного подмножества служит подмножество в группе диэдра D_{2n}, $n > 2$, состоящее из всех инволюций и единицы). Поскольку вокруг понятия группы имеется достаточно хорошо разработанная теория, а понятие скрученного подмножества новое, естественно начинать изучение нового объекта с исследования скрученных подмножеств, которые «близки» по своим свойствам к подгруппам. Также напрашивается вопрос о том, какое строение имеют группы, порожденные такими «почти групповыми» скрученными подмножествами.

Ранее, в работах [1, 4], изучались конечные группы, содержащие только скрученные подмножества, являющиеся подгруппами. Естественным продолжением этих исследований будет изучение «наименьших негрупповых» скрученных подмножеств и групп, порожденных такими подмножествами. Более точно, мы определим эти подмножества следующим образом.

Определение 2. Подмножество K группы G называется *минимальным негрупповым скрученным подмножеством* (MNG-*подмножеством*), если выполняются следующие условия:

(1) $K \neq \langle K \rangle$;

(2) для любого собственного скрученного подмножества S из K справедливо $S = \langle S \rangle$.

В настоящей работе изучаются MNG-подмножества, содержащие инволюции. Получены следующие результаты.

Теорема 1. *Пусть G — конечная группа и K — скрученное подмножество из G такое, что $G = \langle K \rangle$. Тогда следующие условия эквивалентны:*

(I) *K — MNG-подмножество, содержащее более одной инволюции;*

(II) *$G \cong D_{2p}$ — группа диэдра порядка $2p$, где p — простое число, причем справедлив один из следующих случаев:*

(a) *$K = \{1, u, v\}$ при $p = 2$, где u, v — различные инволюции из G;*

(b) *$K = E \cup \{1\}$ при $p \neq 2$, где E — множество инволюций из G.*

Теорема 2. *Пусть G — конечная группа и K — скрученное подмножество из G такое, что $G = \langle K \rangle$. Тогда следующие условия эквивалентны:*

(I) *K — MNG-подмножество, содержащее только одну инволюцию, но более чем одну максимальную циклическую 2-подгруппу;*

(II) *G и K удовлетворяют одному из случаев:*

(1) *$G \cong Q_8$ — группа кватернионов и $K = \langle a \rangle \cup \langle b \rangle$, где a, b — элементы из G такие, что $G = \langle a, b \rangle$.*

(2) *$G = \langle z \rangle \leftthreetimes \langle t \rangle$, где $|t| = 2^n$, $n > 1$, $|z| = p$, p — простое число, $\langle t^2 \rangle \leq Z(G)$, $z^t = z^{-1}$ и справедлив один из вариантов:*

(a) *$K = \langle a \rangle \cup \langle b \rangle$ при $p = 2$ для некоторых различных элементов a, b таких, что $|a| = |b| = 2^n$;*

(b) *$K = \bigcup\limits_{c \in \langle z \rangle} \langle t \rangle^c$ при $p \neq 2$.*

В силу этих результатов общий вопрос о строении MNG-подмножеств, содержащих инволюцию, редуцируется к вопросу о строении MNG-подмножеств, содержащих ровно одну максимальную циклическую 2-подгруппу.

1. Вспомогательные результаты. Следуя [1], подгруппоид, порожденный некоторым подмножеством $M \cup 1$ группы G, с помощью бинарной операции $x \circ y := xy^{-1}x$ будем обозначать через $Tw(M)$.

Лемма 1. *Пусть G — группа и u, v — две различные инволюции из G. Тогда скрученное подмножество $Tw(u, v)$ не является подгруппой.*

Доказательство. Введем обозначение $K := Tw(u, v)$. Допустим противное, т. е. что K — подгруппа.

Заметим, что если a, b — инволюции, то элемент aba также является инволюцией. В силу этого нетрудно видеть, что $x^2 = 1$ для любого $x \in K$.

Так как по предположению K — подгруппа, то $xy \in K$ для любых $x, y \in K$ и, следовательно, $(xy)^2 = 1$, откуда ввиду соотношений $x^2 = 1$, $y^2 = 1$ получаем, что $xy = yx$. Таким образом, K — абелева подгруппа в G, и, значит, $uv = vu$. Легко видеть, что подмножество $N := \{1, u, v\}$ является скрученным. Следовательно, $K = \{1, u, v\}$. Очевидно, K не является подгруппой, что противоречит исходному предположению. Лемма 1 доказана. $\square$

Следующая лемма является объединением двух общеизвестных утверждений о группе диэдра.

Лемма 2. *Пусть $G = \langle u, v \rangle$, где u, v — различные инволюции из G. Тогда*

(*a*) *$G = \langle uv \rangle \leftthreetimes \langle v \rangle$, причем $x^v = x^{-1}$ для любого элемента x из $\langle uv \rangle$;*

(*b*) *если $|uv|$ — нечетное число, то все инволюции из группы G сопряжены с инволюцией v при помощи элементов из $\langle uv \rangle$.*

Непосредственно из определения множества $Tw(M)$ вытекает

Лемма 3. *Пусть G — группа, a, b — элементы из G и $K := Tw(a, b)$.*

Тогда для любого элемента x из K либо $x = a^{n_1}b^{m_1}\dots a^{n_k}b^m a^{n_k}\dots b^{m_1}a^{n_1}$, либо $x = a^{n_1}b^{m_1}\dots a^{n_k}b^{m_k}a^n b^{m_k}a^{n_k}\dots b^{m_1}a^{n_1}$, где n_i, m_i, n, m — некоторые целые числа, $i = 1, \dots, k$.

Лемма 4. *Пусть G — группа, H — нормальная подгруппа в G и K — MNG-подмножество группы G. Допустим, что $xH \subseteq K$ для любого $x \in K$. Пусть $\overline{G} := G/H$ и $\overline{K}$ — образ подмножества K в $\overline{G}$.*

Тогда $\overline{K}$ — MNG-подмножество.

Доказательство. Допустим противное, т. е. пусть $\overline{K}$ не является MNG-подмножеством. Тогда в $\overline{K}$ существует собственное скрученное подмножество $\overline{S}$, которое не является подгруппой. Пусть S — полный прообраз $\overline{S}$ в G. В силу условия K — полный прообраз множества $\overline{K}$, значит, $S \subseteq K$. Понятно, что S — скрученное подмножество и S не подгруппа. Следовательно, $S = K$, откуда $\overline{S} = \overline{K}$, что противоречит выбору $\overline{S}$. □

Лемма 5 [1, лемма 2.1]. *Пусть G — группа и K — скрученное подмножество из G. Тогда $\langle x\rangle$ содержится в K для любого $x \in K$.*

2. Доказательство теоремы 1. Покажем, что из (I) вытекает (II). Пусть u, v — различные инволюции из K. Тогда из леммы 1 следует, что $K = Tw(u, v)$. Так как $G = \langle K\rangle$, то G — группа диэдра. По лемме 2 $G = \langle uv\rangle \leftthreetimes \langle v\rangle$, причем $x^v = x^{-1}$ для любого элемента x из $\langle uv\rangle$.

Далее, пусть z — элемент из $\langle uv\rangle$ такой, что $|z| = p$, где p — простое число из $\pi(\langle uv\rangle)$. Рассмотрим множество $N^* := \langle z\rangle \cup v$. Поскольку $z^v = z^{-1}$, то $vN^*v = N*$. Для любого числа t имеем $z^t v z^t = z^t v z^t v v = z^t z^{-t} v = v$, откуда следует, что $z^t N^* z^t \subseteq N^*$. Таким образом, N^* — скрученное подмножество.

Очевидно, N^* не является подгруппой.

Рассмотрим множество $K^* := vN^*$. Нетрудно видеть, что K^* — скрученное подмножество, причем K^* не является подгруппой.

Покажем, что $K^* = K$.

Заметим, что для любого числа k справедливо равенство $v(uv)^k = (vu)^k v$.

Так как $z \in \langle uv\rangle$, то существует число m такое, что $z = (uv)^m$, откуда $vz^t = v(uv)^{mt}$. Если mt — четное число, т. е. $mt = 2k$, то

$$v(uv)^{mt} = v(uv)^{2k} = v(uv)^k(uv)^k = (vu)^k v(uv)^k.$$

Если mt — нечетное число, т. е. $mt = 2k + 1$, то

$$v(uv)^{mt} = v(uv)^{2k+1} = v(uv)^k(uv)(uv)^k = (vu)^k(vuv)(uv)^k.$$

Нетрудно видеть, что при любом t элемент vz^t содержится в K. Таким образом, $K^* \subseteq K$. Поскольку K^* не является подгруппой, а K — MNG-подмножество, то $K^* = K$. Тогда $G = \langle K\rangle = \langle N^*\rangle$, откуда вытекает, что $G \cong D_{2p}$ — группа диэдра порядка $2p$, где p — простое число.

Далее, при $p = 2$ имеем $G = \langle u\rangle \times \langle v\rangle$ и $K = \{1, u, v\}$. Таким образом, в этом случае G и K удовлетворяют случаю II(a) теоремы 1.

Рассмотрим случай, когда $p \neq 2$.

Поскольку $G \cong D_{2p}$, p нечетно, то в силу леммы 1.2(b) все инволюции из G сопряжены с инволюцией v при помощи элементов из $\langle uv\rangle$. Таким образом, если f — инволюция из группы G, то $f = (uv)^m u(vu)^m$ для некоторого числа m. Нетрудно видеть, что $f \in K$. Значит, $E \cup 1 \subseteq K$, где E — множество инволюций из G. Легко показать, что $E \cup 1$ — скрученное подмножество и не подгруппа. Следовательно, $E \cup 1 = K$.

Таким образом, при $p \neq 2$ получаем, что G и K удовлетворяют случаю II(b) теоремы 1.

Итак, доказательство того, что в теореме 1 из (I) следует (II), завершено.

Покажем, что из (II) следует (I). Очевидно, что в случае II(a) теоремы 1 $G = \langle K \rangle$ и K является MNG-подмножеством.

Рассмотрим случай II(b). Понятно, что $G = \langle K \rangle$. Таким образом, остается показать, что K — MNG-подмножество.

Очевидно, K не является подгруппой.

Покажем, что любое собственное скрученное подмножество S из K является подгруппой, для чего докажем, что S содержит не более одной инволюции. Допустим противное, т. е. что подмножество S содержит две различные инволюции u, v. Тогда $G = \langle uv \rangle \leftthreetimes \langle v \rangle$ и по лемме 1(b) все инволюции из группы G сопряжены с инволюцией v при помощи элементов из $\langle uv \rangle$. Таким образом, если f — некоторая инволюция из G, то $f = (uv)^k v (vu)^k$ для некоторого числа k. Очевидно, что $f \in Tw(u, v) \subseteq S$. Следовательно, $E \cup 1 \subseteq S \subseteq K$, откуда получаем, что $S = K$; противоречие с выбором S.

Итак, S содержит не более одной инволюции. Следовательно, либо $S = 1$, либо $S = \langle u \rangle$, где u — некоторая инволюция из G. В обоих случаях S — подгруппа, значит, K — MNG-подмножество, и теорема 1 доказана.

3. Доказательство теоремы 2. Покажем, что из (I) следует (II).

Пусть $\langle x \rangle$, $\langle y \rangle$ — две различные максимальные циклические 2-подгруппы из K. Так как в K существует только одна инволюция, то $\langle x \rangle \cap \langle y \rangle \neq 1$. Существуют элементы a из $\langle x \rangle$ и b из $\langle y \rangle$ такие, что $a \neq b$, но $a^2 = b^2 \neq 1$.

Пусть $K^* := Tw(a, b)$, $G^* := \langle K^* \rangle$ и $H := \langle a^2 \rangle$. Понятно, что $H \leq Z(G^*)$. Также ясно, что $K^* \subseteq K$.

Далее анализ разбивается на ряд этапов.

(1) $K = K^* = Tw(a, b)$.

Рассмотрим фактор-группу $\overline{G}^* := G^*/H$. Пусть $\overline{K}^*$ — образ множества K^* в $\overline{G}^*$. Ясно, что $\overline{K}^* = Tw(\bar{a}, \bar{b})$, где $\bar{a}$, $\bar{b}$ — образы соответственно элементов a, b в $\overline{G}^*$, $\overline{G}^* = \langle \overline{K}^* \rangle$ и $\bar{a}^2 = \bar{b}^2 = 1$, $\bar{a} \neq \bar{b}$. По лемме 1 получаем, что $\overline{K}^*$ не подгруппа. Следовательно, K^* не является подгруппой. Поскольку $K^* \subseteq K$, то ввиду того, что K — MNG-подмножество, получаем, что $K = K^*$.

(2) $G = \langle a, b \rangle$, $H \leq Z(G)$.

Очевидное следствие (1).

(3) *Для любого элемента z из K будет $zH \subseteq K$.*

Пусть $z \in K$. Тогда по лемме 3 либо

$$z = a^{n_1} b^{m_1} \dots a^{n_k} b^m a^{n_k} \dots b^{m_1} a^{n_1},$$

либо

$$z = a^{n_1} b^{m_1} \dots a^{n_k} b^{m_k} a^n b^{m_k} a^{n_k} \dots b^{m_1} a^{n_1}$$

для некоторых целых чисел n, m, n_i, m_i, $i = 1, \dots, k$.

Для любого элемента h из подгруппы H существует такое целое число s, что $h = a^{2s} = b^{2s}$. По (2) $H \leq Z(G)$. Тогда либо

$$zh = (a^{n_1} b^{m_1} \dots a^{n_k}) b^m (a^{n_k} \dots b^{m_1} a^{n_1}) b^{2s} = (a^{n_1} b^{m_1} \dots a^{n_k}) b^{m+2s} a^{n_k} \dots b^{m_1} a^{n_1},$$

либо

$$zh = (a^{n_1}b^{m_1}\dots a^{n_k}b^{m_k})a^n(b^{m_k}a^{n_k}\dots b^{m_1}a^{n_1})a^{2s} = (a^{n_1}b^{m_1}\dots a^{n_k}b^{m_k})a^{n+2s}(b^{m_k}a^{n_k}\dots b^{m_1}a^{n_1}).$$

В обоих случаях $zh \in K$. Следовательно, $zH \subseteq K$ для любого элемента z из K, и п. (3) доказан.

(4) *Пусть $\overline{G} := G/H$ и $\overline{K}$ — образ подмножества K в $\overline{G}$. Тогда*
(a) *$\overline{K}$ — MNG-подмножество;*
(b) *$\overline{G} \cong D_{2p}$ — группа диэдра порядка $2p$, где p — простое число.*

Понятно, что $\overline{K}^* = Tw(\bar{a}, \bar{b})$, где $\bar{a}$, $\bar{b}$ — образы соответственно элементов a, b в $\overline{G}^*$, $\overline{G}^* = \langle \overline{K}^* \rangle$ и $\bar{a}^2 = \bar{b}^2 = 1$, $\bar{a} \neq \bar{b}$. В силу п. (2) из леммы 4 следует, что $\overline{K}$ является MNG-подмножеством. Тогда по теореме 1 получаем, что $\overline{G} \cong D_{2p}$ — группа диэдра порядка $2p$, где p — простое число.

(5) *Пусть $p = 2$. Тогда G и K удовлетворяют либо случаю* (1), *либо случаю* (2)(a) *теоремы* 2.

Из (4) получаем, что $\overline{G} = \langle \bar{a} \rangle \times \langle \bar{b} \rangle$, $|\bar{a}| = |\bar{b}| = 2$. Тогда $\langle a \rangle^b = \langle a \rangle$ и $\langle b \rangle^a = \langle b \rangle$. В силу выбора элементов a, b имеем $|a| = |b| = 2^n$ для некоторого натурального числа $n > 1$. Поскольку $a^b = a^m$ для некоторого числа m, то $a^{b^2} = a^{m^2} = a$, откуда вытекает, что $m^2 - 1 \equiv 0 (\operatorname{mod} 2^n)$ и $m \not\equiv 0 (\operatorname{mod} 2)$. Так как $m^2 - 1 = (m-1)(m+1)$, то либо $m \equiv 1 (\operatorname{mod} 2^n)$, либо $m \equiv -1 (\operatorname{mod} 2^n)$.

Если $ab \neq ba$, то $m \equiv -1 (\operatorname{mod} 2^n)$, откуда $a^b = a^{-1}$. Аналогично доказывается, что в этом случае $b^a = b^{-1}$. Следовательно, $n = 2$, т. е. $|a| = |b| = 4$. Значит, $G \cong Q_8$ — группа кватернионов, т. е. группа G удовлетворяет случаю (1) теоремы 2.

Если $ab = ba$, то $m \equiv 1 (\operatorname{mod} 2^n)$. Рассмотрим элемент $c := ab^{-1}$. Поскольку $a^2 = b^2$, имеем $c^2 = 1$. Ясно, что $G = \langle c, b \rangle$. Значит, $G = \langle b \rangle \times \langle c \rangle$. Таким образом, группа G удовлетворяет случаю (2)(a) теоремы 2.

Далее, в обоих случаях рассмотрим множество $N := \langle a \rangle \cup \langle b \rangle$. В силу леммы 5 $N \subseteq K$. Понятно, что N не является подгруппой. Для любого элемента a^t из $\langle a \rangle$ имеем $a^t \langle b \rangle a^t = a^{2t}(a^{-t}\langle b \rangle a^t) = a^{2t}\langle b \rangle = \langle b \rangle$, так как $a^{2t} \in \langle b \rangle$. Значит, $a^t N a^t \subseteq N$ для любого числа t. Аналогично показывается, что для любого числа t справедливо $b^t N b^t \subseteq N$. Следовательно, N является скрученным подмножеством. Поскольку K — MNG-подмножество и $N \subseteq K$, получаем, что $N = K$, и п. (5) доказан.

(6) *Пусть $p \neq 2$. Тогда G и K удовлетворяют случаю* (2)(b) *теоремы* 2.

Доказательство разбивается на ряд этапов.

(6.1) *Группа G удовлетворяет случаю* (2)(b) *теоремы* 2.

Из (4) и леммы 2 следует, что $\overline{G} = \langle \bar{z} \rangle \rtimes \langle \bar{t} \rangle$, где $|\bar{t}| = 2$, $|\bar{z}| = p$, p — простое число, отличное от 2, и $(\bar{z})^{\bar{t}} = (\bar{z})^{-1}$. Поскольку $|H| = 2^s$ для какого-то числа s, то в группе G существует элемент z, который является некоторым прообразом элемента $\bar{z}$ в группе $\overline{G}$ и имеет порядок, равный p.

Пусть t — некоторый прообраз элемента $\bar{t}$ в группе $\overline{G}$. Так как $t^2 \in Z(G)$ и $(\bar{z})^{\bar{t}} = (\bar{z})^{-1}$, то $\langle z \rangle \lhd G$. Понятно, что $\langle z \rangle \cap \langle t \rangle = 1$. Следовательно, $G = \langle z \rangle \rtimes \langle t \rangle$. Нетрудно видеть, что $z^t = z^{-1}$. Таким образом, группа G удовлетворяет случаю (2)(a) теоремы 2.

(6.2) *Множество* $N := \bigcup_{c \in \langle z \rangle} \langle t \rangle^c$ *является скрученным подмножеством, причем* $N \neq \langle N \rangle = G$.

Легко видеть, что N не является подгруппой и $G = \langle N \rangle$. Таким образом, остается показать, что N — скрученное подмножество.

Очевидно, $1 \in N$.

Далее, для любых целых чисел k, m, n, s имеем

$$(z^{-k}t^m z^k)(z^{-s}t^n z^s)(z^{-k}t^m z^k) = z^{-k}t^m z^{k-s}t^n z^{s-k}t^m z^k$$
$$= z^{-k}(t^m z^{k-s}t^{-m})t^{n+2m}(t^{-m}z^{s-k}t^m)z^k,$$

откуда вытекает соотношение

$$(z^{-k}t^m z^k)(z^{-s}t^n z^s)(z^{-k}t^m z^k) = z^{-k}z^{(-1)^m(k-s)}t^{n+2m}z^{(-1)^m(s-k)}z^k.$$

Таким образом,

$$(z^{-k}t^m z^k)(z^{-s}t^n z^s)(z^{-k}t^m z^k) \in \langle t \rangle^c,$$

где $c = z^{(-1)^m(s-k)+k}$. Итак, N — скрученное подмножество, и п. (6.2) доказан.

(6.3) $K = N$.

Рассмотрим фактор-группу $\overline{G} = G/H$ и множество $\overline{K}$ — образ K в $\overline{G}$.

В силу п. (4) $\overline{G} = \langle \bar{z} \rangle \leftthreetimes \langle \bar{t} \rangle$, где $|\bar{z}| = p$, $|\bar{t}| = 2$. Ввиду (1) $\overline{K} = Tw(\bar{a}, \bar{b})$, где $|\bar{a}| = |\bar{b}| = 2$ и $\bar{a} \neq \bar{b}$. Поскольку по (4) $\overline{K}$ — MNG-подмножество, применяя теорему 1, получаем, что $\overline{K} = \overline{E} \cup 1$, где $\overline{E}$ — множество инволюций из $\overline{G}$. Следовательно, для любого элемента $\bar{c}$ из $\langle \bar{z} \rangle$ имеем $\langle \bar{t} \rangle^{\bar{c}} \subseteq \overline{K}$. Тогда ввиду п. (3) получаем, что для любого элемента c из $\langle z \rangle$ справедливо $\langle t \rangle^c \subseteq K$, откуда $N \subseteq K$. В силу (6.2) имеем $N = K$, и п. (6.3), а вместе с ним п. (6) доказаны.

Итак, доказательство того, что в теореме 2 из (I) следует (II), завершено.

Покажем, что из (II) следует (I).

Легко видеть, что в случаях (1) и (2)(a) множество K есть MNG-подмножество и $G = \langle K \rangle$. Покажем, что это справедливо и для случая (2)(b). Легко видеть, что в этом случае $G = \langle K \rangle$. Таким образом, остается только показать, что K — MNG-подмножество.

Сначала покажем, что K — скрученное подмножество.

Пусть $x = z^{-m}t^k z^m$, $y = z^{-s}t^r z^s$ — некоторые элементы из K, где m, k, s, r — целые числа. Тогда

$$xy^{-1}x = (z^{-m}t^k z^m)(z^{-s}t^{-r}z^s)(z^{-m}t^k z^m) = z^{-m}t^k z^{m-s}t^{-r}z^{s-m}t^k z^m$$
$$= z^{-m}(t^k z^{m-s}t^{-k})t^{2k-r}(t^{-k}z^{s-m}t^k)z^m.$$

Если число k нечетное, то

$$t^k z^{m-s}t^{-k} = z^{-(m-s)}, \quad t^{-k}z^{s-m}t^k = z^{-(s-m)},$$

а если k четное, то

$$t^k z^{m-s}t^{-k} = z^{m-s}, \quad t^{-k}z^{s-m}t^k = z^{s-m}.$$

Таким образом, в первом случае $xy^{-1}x = z^{s-2m}t^r z^{-(s-2m)}$, а во втором — $xy^{-1}x = z^{-s}t^{2k-r}z^s$. Очевидно, что в обоих случаях $xy^{-1}x \in K$.

Итак, K — скрученное подмножество.

Теперь покажем, что если S — собственное скрученное подмножество из K, то S является подгруппой.

Допустим противное, т. е. что существует собственное скрученное подмножество S в K, не являющееся подгруппой. Тогда ввиду леммы 5 S содержит подгруппы $\langle t\rangle^{z_1}$, $\langle t\rangle^{z_2}$, где z_1, z_2 — некоторые различные элементы из $\langle z\rangle$. Значит, $\langle t^2\rangle \subseteq S$.

Обозначим $H := \langle t^2\rangle$. Заметим, что для любого элемента x из S справедливо $xH \subseteq S$. Действительно, если $x \in S$, то $x = a^c$, где $a \in \langle t\rangle, c \in \langle z\rangle$. По лемме 5 $\langle a^c\rangle \subseteq S$. Тогда если $x \in H$, то $xH \subseteq H \subseteq S$, а если $x \notin H$, то $xH \subseteq \langle a^c\rangle \subseteq S$. Таким образом, для любого элемента x из S справедливо $xH \subseteq S$.

Аналогично показывается, что $xH \subseteq K$ для любого $x \in K$.

Рассмотрим фактор-группу $\overline{G} := G/H$. Очевидно, что $\overline{G} \cong D_{2p}$ — группа диэдра порядка $2p$, где p — простое число и $p \neq 2$. Пусть $\overline{S}, \overline{K}$ — образы соответственно множеств S, K в $\overline{G}$. Нетрудно видеть, что $\overline{K} = \overline{E} \cup \{1\}$, где $\overline{E}$ — множество инволюций из $\overline{G}$. Множество $\overline{S}$ содержит более одной инволюции. В силу теоремы 1 $\overline{K}$ — MNG-подмножество. Поскольку $\overline{S} \neq \langle \bar{s}\rangle$, имеем $\overline{S} = \overline{K}$. Следовательно, $S = K$, так как множества S и K являются полными прообразами множеств $\overline{S}$ и $\overline{K}$. Получаем противоречие с тем, что S — собственное скрученное подмножество из K и, значит, K — MNG-подмножество. Теорема 2 доказана.

Автор выражает глубокую благодарность профессору В. В. Беляеву, под руководством которого была выполнена эта работа.

ЛИТЕРАТУРА

1. *Мыльников А. Л.* Конечные перекрученные группы // Математические системы. Красноярск: Краснояр. гос. аграр. ун-т, 2005. Вып. 3. С. 53–58.
2. *Aschbacher M.* Near subgroups of finite groups // J. Group Theory. 1998. V. 1, N 2. P. 113–129.
3. *Мыльников А. Л.* Конечные минимальные неперекрученные группы // Вестн. Красноярск. гос. ун-та. 2005. № 1. С. 71–76.
4. *Мыльников А. Л.* Абелевы перекрученные группы // Математические системы. Красноярск: Краснояр. гос. аграр. ун-т, 2005. Вып. 3. С. 59–61.

Статья поступила 10 ноября 2005 г.

Мыльников Андрей Леонидович
Сибирский федеральный университет,
Институт естественных и гуманитарных наук, кафедра высшей математики,
пр. Свободный, 79, Красноярск 660041
mylnand@yandex.ru