ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИНФОРМАТИКИ

УДК 512.54+512.57

АВТОМОРФИЗМЫ НЕКОТОРЫХ КОНЕЧНЫХ МАГМ С ПОРЯДКОМ СТРОГО МЕНЬШЕ ЧИСЛА N(N+1) И ПОРОЖДАЮЩИМ МНОЖЕСТВОМ ИЗ N ЭЛЕМЕНТОВ[1]

Литаврин А.В.
Сибирский федеральный университет, г. Красноярск

Поступила в редакцию 29.11.2018, после переработки 19.03.2019.

В данной работе исследуются проблемы описания групп автоморфизмов конечных магм, строятся некоторые конечные магмы $\mathfrak{G}$, порожденные n элементами и порядком k, удовлетворяющим неравенствам $n + 1 \leq k < n^2 + n$. Построенные магмы не являются полугруппами или квазигруппами. Для введенных магм указывается общий вид автоморфизма и приводится описание группы всех автоморфизмов. Показано, что группа всех автоморфизмов изоморфна некоторой подгруппе (приводится описание этой группы) симметрической группы подстановок S_n, где n – количество элементов подходящего порождающего множества магмы $\mathfrak{G}$. Доказано, что всякая конечная циклическая группа порядка больше 2 изоморфна группе всех автоморфизмов подходящей магмы $\mathfrak{G}$. Аналогичный результат получен для четвертой группы Клейна. Кроме того, показано, что для любой конечной группы G можно подобрать подходящую магму $\mathfrak{G}$ такую, что G изоморфна некоторой подгруппе группы $Aut\ (\mathfrak{G})$ (приводится алгоритм построения магмы $\mathfrak{G}$ для произвольной конечной группы G).

Ключевые слова: магмы, группоиды, автоморфизмы конечной магмы, автоморфизмы конечного группоида, конечная циклическая группа, группа Диэдра.

Вестник ТвГУ. Серия: Прикладная математика. 2019. № 2. С. 70–87.
https://doi.org/10.26456/vtpmk533

Введение

Алгебраическую систему с одной бинарной алгебраической операцией называем *магмой* (также распространен термин «группоид»). Для всякой алгебраической системы вводится понятие автоморфизма (см. [1]).

Данная работа является продолжением работы [2] и посвящена исследованию автоморфизмов некоторых конечных магм. Основные результаты приведены ниже в виде Теоремы 1, Теоремы 2 и Следствия 1.

[1]Работа выполнена при финансовой поддержке РФФИ (проект №16-01-00707).

Вопросам об автоморфизмах посвящено множество работ, в частности, когда магма является линейной группой (см. работы [3–6] и др.), группой Шевалле (см. работы [7–11]), некоторой матричной полугруппой (см. работы [12–15]) или квазигруппой (см. [16] и др.).

В 1994 году А.П. Ильиных (см. [17]) классифицировал (с точностью до изоморфизма) конечные магмы $\mathfrak{D} = (D, *)$, имеющие 2-транзитивную на множестве-носителе D группу автоморфизмов $Aut\ (\mathfrak{D})$. В работе [18] построены две серии магм $X(\tau)$ и $X(\sigma, k_1, k_2)$ порядков $q(q-1)/2$ и $q(q+1)/2$ соответственно ($q = 2^r$). Магмы $X(\tau)$ и $X(\sigma, k_1, k_2)$ имеют подгруппы автоморфизмов, изоморфные группе $SL(2, q)$ и транзитивные на множестве-носителе.

Как обычно, S_n – симметрическая группа перестановок конечного множества из n элементов. В работе [2] для каждого натурального числа k и кортежа $q \in S_k^{2k}$ вводилась (см. [2, определение 1]) магма $\mathfrak{S} = \mathfrak{S}(k, q) = (V, *)$. При этом в множестве–носителе определялось множество M такое, что выполнялись равенства

$$|V| = k + k^2, \quad |M| = k, \quad V = M \cup (M * M), \quad |M * M| = |M| \cdot |M| = k^2. \qquad (1)$$

Для магмы $\mathfrak{S}$ приводилось описание группы автоморфизмов (см. Теорема 2 в [2]). Кроме того, было установлено, что для всякого натурального числа k существует кортеж $q \in S_k^{2k}$ такой, что $S_k \cong Aut\ (\mathfrak{S}(k, q))$ (см. Теорема 1 из [2]). Отметим, что не всякая магма $\mathfrak{F}$ порядка $k + k^2$ с условиями (1) будет изоморфна подходящей магме $\mathfrak{S}(k, q)$ (см. Определение 1 из [2]).

Известны следующие общие проблемы (см. [1, стр. 108]), связанные с автоморфизмами.

Проблема 1. *Описать группу автоморфизмов $Aut\ (\mathfrak{A})$ некоторой фиксированной алгебраической системы $\mathfrak{A}$.*

Проблема 2. *Для фиксированной группы G и фиксированного класса $\mathfrak{K}$ алгебраических систем определить системы $\mathfrak{A} \in \mathfrak{K}$ (не обязательно все) такие, что $G \cong H \leq Aut\ (\mathfrak{A})$ либо показать, что в классе $\mathfrak{A}$ таких систем $\mathfrak{A}$ нет.*

Приведенные выше Проблемы 1 и 2 изучаются в данной работе для конечных магм $\mathfrak{G}$, которые вводит

Определение 1. *Пусть k и m – натуральные числа такие, что k больше единицы и верно неравенство $2m \leq k^2$. Определим множества*

$$U_{k,m} := \{a_1, ..., a_k, c_1, ..., c_m\} \cup \{b_{ij} \mid i, j = 1, ..., k\}, \quad M := \{a_1, ..., a_k\}.$$

Элементы $a_1, ..., a_k, c_1, ..., c_m, b_{ij}$ $(i, j = 1, ..., k)$ считаем попарно различными.

Полагаем, что X – набор множеств, состоящий из m непересекающихся подмножеств, мощности ≥ 2, множества $M \times M$. Вводим упорядочение множества X. В соответствии с этим упорядочением, каждый элемент из X будет обозначаться символом M_i, где $1 \leq i \leq m$. Таким образом, $X = \{M_1, ..., M_m\}$ и $M_i \cap M_j = \varnothing$ при $i \neq j$. Вводим обозначения:

$$D := (M \times M) \setminus \bigcup_{i=1}^{m} M_i, \quad B := \{b_{ij} \in U_{k,m} \mid (a_i, a_j) \in D\}.$$

Задаем множество $V := M \cup \{c_1, ..., c_m\} \cup B$. *На множестве* V *вводим бинарную алгебраическую операцию «$*$»:*

$$a_i * a_j = c_q, \text{ если } (a_i, a_j) \in M_q; \quad a_i * a_j = b_{ij}, \quad \text{если } (a_i, a_j) \in D; \tag{2}$$

$$a_q * b_{ij} = b_{ij},\ b_{ij} * a_q = b_{ij},\ c_i * a_j = a_j * c_i = c_i;$$

$$b_{ij} * b_{vw} = b_{ij}; \quad c_i * c_j = c_i; \quad b_{ij} * c_w = b_{ij}; \quad c_w * b_{ij} = c_w.$$

Символами

$$\mathfrak{G} = \mathfrak{G}(k, m, M_1, ..., M_m) = (V, *)$$

обозначаем алгебраическую систему с множеством носителем V *и алгебраической операцией* $*$, *которую задают равенства (2).*

Пусть M – множество из определения 1 и $M * M := \{a * b \mid a, b \in M\}$. Тогда равенства (2) показывают, что справедливо равенство $V = M \cup (M * M)$, следовательно, M – *порождающее множество* магмы $\mathfrak{G}$ (определение порождающего множества алгебраической системы можно найти в [19, стр. 55]).

Множества D и B из определения 1 будут пустыми тогда и только тогда, когда $\bigcup_{i=1}^m M_i = M \times M$.

Замечание 1. Пусть заданы две магмы

$$\mathfrak{G} = \mathfrak{G}(k, m, M_1, ..., M_m) = (V, *_1), \qquad \widetilde{\mathfrak{G}} = \mathfrak{G}(k, m, \widetilde{M_1}, ..., \widetilde{M_m}) = (\widetilde{V}, *_2)$$

такие, что $m > 2$, $\widetilde{V} = V$ и $\widetilde{M_1} = M_2$, $\widetilde{M_2} = M_1$, $\widetilde{M_i} = M_i$, при $i \in \{3, ..., m\}$. В этом случае магма $\widetilde{\mathfrak{G}}$ получена из магмы $\mathfrak{G}$ с помощью перенумерации системы множеств $M_1, ..., M_m$. Равенства (2) показывают, что операция умножения в магме $\widetilde{\mathfrak{G}}$ будет отличаться от операции умножения в магме $\mathfrak{G}$. В общем случае магмы $\widetilde{\mathfrak{G}}$ и $\mathfrak{G}$ не изоморфны.

Непосредственно из определения магм $\mathfrak{G}(k, m, M_1, ..., M_m)$ вытекает

Утверждение 1. *Для всякой магмы* $\mathfrak{G}(k, m, M_1, ..., M_m)$ *справедливы следующие условия:*

$$V = M \cup (M * M), \quad M \cap (M * M) = \varnothing, \quad |M| = k, \tag{3}$$

$$|M * M| < |M| \cdot |M| = k^2, \quad 2m \le |\bigcup_{i=1}^{m} M_i| \le k^2, \quad |V| = k + m + k^2 - |\bigcup_{i=1}^{m} M_i|,$$

$$k + 1 \le |V| < k^2 + k.$$

Для формулировки основных результатов статьи нам потребуется

Определение 2. *Полагаем, что задана магма* $\mathfrak{G}(k, m, M_1, ..., M_m)$. *Тогда для всякого номера* $q \in \{1, ..., m\}$ *и всякой перестановки* $\alpha \in S_k$ *введем множество*

$$M_q^\alpha := \{(a_{\alpha(i)}, a_{\alpha(j)}) \mid (a_i, a_j) \in M_q\} \subset M \times M.$$

В множестве S_k *выделим множество* $A(M_1, ..., M_m)$ *подстановок* $\alpha \in S_k$ *таких, что для каждого номера* $q \in \{1, ..., m\}$ *существует номер* $d \in \{1, ..., m\}$ *такой, что справедливо равенство* $M_q^\alpha = M_d$.

Если $\alpha \in A(M_1, ..., M_m)$, *то на множестве* $\{1, ..., m\}$ *можно определить отображение* $r_\alpha : \{1, ..., m\} \to \{1, ..., m\}$ *такое, что* $r_\alpha(i) = j$ *тогда и только тогда, когда* $M_i^\alpha = M_j$. *Отметим, что* r_α *– перестановка из* S_m.

Множество $A(M_1, ..., M_m)$ является подгруппой группы S_k. Этот факт будет установлен ниже (см. лемму 1) независимо от описания группы автоморфизмов магмы $\mathfrak{G}(k, m, M_1, ..., M_m)$.

Замечание 2. Нетрудно увидеть, что для перестановки $\alpha \in A(M_1, ..., M_m)$ и числа $d = r_\alpha(q)$ справедливы равенства: $|M_q^\alpha| = |M_q| = |M_d|$. Кроме того, можно лаконично записать множество $A(M_1, ..., M_m)$ с помощью кванторов:

$$A(M_1, ..., M_m) := \{\alpha \in S_k \mid \forall\ q \in \{1, ..., m\}\ \exists\ d \in \{1, ..., m\}\ :\ M_q^\alpha = M_d\}.$$

К основным результатам статьи относится

Теорема 1. *Для всякой перестановки $\alpha \in A(M_1, ..., M_m)$ отображение ϕ_α, заданное правилом*

$$\phi_\alpha:\ a_i \to a_{\alpha(i)} \quad (1 \le q \le k), \qquad b_{uv} \to b_{\alpha(u),\alpha(v)} \quad ((a_u, a_v) \in D),$$

$$c_q \to c_{q'}, \quad q' = r_\alpha(q) \quad (1 \le q \le m),$$

является автоморфизмом магмы $\mathfrak{G} = \mathfrak{G}(k, m, M_1, ..., M_m)$. При этом

$$Aut\ (\mathfrak{G}) = \{\phi_\alpha \mid \alpha \in A(M_1, ..., M_m)\}, \qquad Aut\ (\mathfrak{G}) \cong A(M_1, ..., M_m).$$

Пусть $k \in \mathbb{N}$, $x \in \{1, ..., k\}$ и F – некоторое подмножество $\{1, ..., k\}$. Тогда *стабилизатором элемента* x и *стабилизатором множества* F под действием S_k называем подгруппы

$$Stab(x) := \{\alpha \in S_k \mid \alpha(x) = x\}, \quad St(F) := \{\alpha \in S_k \mid \alpha(F) = F\}$$

симметрической группы S_k. Как обычно, символом C_n обозначаем *циклическую группу* порядка n. *Группу Диэдра* порядка $2n$ будем обозначать через D_{2n} $(n \ge 2)$; группу D_4 традиционно называем *четвертной группой Клейна*. Группа D_{2n} допускает запись

$$D_{2n} := \left\langle a, b \mid a^n = b^2 = (ab)^2 = 1 \right\rangle, \quad n \ge 2.$$

В работе доказана

Теорема 2. *Пусть k – произвольное натуральное число большее единицы. Тогда справедливы утверждения:*

1. *существует магма $\mathfrak{G}_1 = \mathfrak{G}_1(k, 1, M_1)$ порядка $k^2 + 1$ такая, что имеет место изоморфизм $Aut\ (\mathfrak{G}_1) \cong S_k$ и выполняется равенство $|M_1| = k$;*

2. *для любого не пустого подмножества L множества $\{1, ..., k\}$ существует магма $\mathfrak{G}_2 = \mathfrak{G}_2(k, 1, M_1)$ порядка $k^2 + k + 1 - |L|$ такая, что имеет место изоморфизм $Aut\ (\mathfrak{G}_2) \cong St(L)$ и выполняется равенство $|M_1| = |L|$;*

3. *существует магма $\mathfrak{G}_3 = \mathfrak{G}_3(k, 1, M_1)$ порядка $k^2 + 1$ такая, что имеет место изоморфизм $Aut\ (\mathfrak{G}_3) \cong C_k$ и верно равенство $|M_1| = k$;*

4. *четвертная группа Клейна D_4 изоморфна группе всех автоморфизмов $Aut\ (\mathfrak{G}_4)$ магмы $\mathfrak{G}_4 = \mathfrak{G}_4(4, 1, M_1)$ порядка 19 такой, что $|M_1| = 2$;*

5. *если a и b – пара различных элементов из множества $\{1, ..., k\}$, то существует магма $\mathfrak{G}_5 = \mathfrak{G}_5(k, 1, M_1)$ порядка k^2+k-1 такая, что имеет место изоморфизм $Aut\ (\mathfrak{G}_5) \cong Stab(a) \cap Stab(b)$ и верно равенство $|M_1| = 2$.*

Существование магмы $\mathfrak{G}_1$ из Теоремы 2 и известная Теорема Кэли (о представлении конечной группы G подгруппой перестановок симметрической группы $S_{|G|}$) дают

Следствие 1. *Всякая конечная группа G изоморфна подходящей подгруппе H группы $Aut\ (\mathfrak{G})$ некоторой магмы $\mathfrak{G} = \mathfrak{G}(k, 1, M_1)$. Если $|G| \neq 1$, то магму $\mathfrak{G}$ можно выбрать так, что $k = |M_1| = |G|$.*

Следствие 1 показывает, что Проблема 2 имеет решения для любой конечной группы G, когда $\mathfrak{K}$ – класс всевозможных магм $\mathfrak{G}(k, m, M_1, ..., M_m)$.

Теорема 2 доказывается конструктивно (строятся магмы $\mathfrak{G}_i$ при $i = 1, 2, 3, 4, 5$).

Существуют другие способы представить произвольную конечную группу G автоморфизмами некоторой подходящей магмы $\mathfrak{G}(k, 1, M_1)$.

Во втором разделе приводится пример 6, в котором для каждой группы Диэдра D_{2n} $(n \geq 2)$ строится магма $\mathfrak{G} = \mathfrak{G}(2n, 1, M_1)$ такая, что $|M_1| = 2n$ и группа D_{2n} изоморфна некоторой подгруппе группы $Aut\ (\mathfrak{G})$. Пример 6 иллюстрирует простой способ, позволяющий для каждой конечной группы перестановок G построить магму $\mathfrak{G} = \mathfrak{G}(k, 1, M_1)$ такую, что $G \subseteq A(M_1)$. При этом группа $Aut\ (\mathfrak{G})$ не обязана быть изоморфна $S_{|G|}$.

1. Доказательство Теоремы 1

В данном разделе доказывается Теорема 1. Для этого сформулируем и докажем леммы 1, 2, 3, 4, 5 и 6.

В этом разделе и далее k и m – пара натуральных чисел из Определения 1, $\mathfrak{G} := \mathfrak{G}(k, m, M_1, ..., M_m)$ – магма, введенная Определением 1 и символы V, D, B, M, M_i обозначают объекты, связанные с магмой $\mathfrak{G}$. Кроме того, с магмой $\mathfrak{G}$ связываем множество $A(M_1, ..., M_m)$, введенное в Определении 2.

Обозначения, связанные с действием композиции двух перестановок. Если $\alpha, \beta \in S_n$ и $x \in \{1, ..., n\}$, то $(\alpha \cdot \beta)(x) := \alpha(\beta(x))$.

Лемма 1. *Множество $A(M_1, ..., M_m)$ – является подгруппой группы S_k.*

Доказательство. В самом деле, очевидно, что единичная перестановка I лежит в множестве $A(M_1, ..., M_m)$.

Далее, покажем замкнутость. Пусть $\alpha, \beta \in A(M_1, ..., M_m)$. Тогда для произвольного номера $q \in \{1, ..., m\}$ существует номер $q' \in \{1, ..., m\}$, а для номера q' существует номер $q'' \in \{1, ..., m\}$ такие, что верны равенства:

$$M_q^\beta = M_{q'}, \quad M_{q'}^\alpha = M_{q''}, \quad (M_q)^{\alpha \cdot \beta} = (M_q^\beta)^\alpha = M_{q'}^\alpha = M_{q''}, \;\; q' = r_\beta(q), \;\; q'' = r_\alpha(q').$$

Получаем, что $(M_q)^{\alpha \cdot \beta} = M_{q''}$, следовательно, $\alpha \cdot \beta \in A(M_1, ..., M_m)$ и верно равенство $r_{\alpha \cdot \beta}(q) = r_\alpha(r_\beta(q))$.

Покажем, что $\alpha^{-1} \in A(M_1, ..., M_m)$, если $\alpha \in A(M_1, ..., M_m)$. В самом деле, по определению M_q^α $(1 \leq q \leq m)$ имеем равенства

$$M_q^\alpha = \{(a_{\alpha(i)}, a_{\alpha(j)}) \mid (a_i, a_j) \in M_q\} = M_{q'}, \quad q' = r_\alpha(q),$$

которые приводят к условиям $(M_q^\alpha)^{\alpha^{-1}} = M_q$, $(M_q^\alpha)^{\alpha^{-1}} = M_{q'}^{\alpha^{-1}}$.

Получаем, что $M_q = M_{q'}^{\alpha^{-1}}$, для произвольного номера $q \in \{1, ..., m\}$ и номера $q' = r_\alpha(q)$. Поскольку $\alpha \in A(M_1, ..., M_m)$, отображение r_α – перестановка из S_m. Значит, когда номер q пробегает множество $\{1, ..., m\}$, номер $q' = r_\alpha(q)$ пробегает это же множество: $\{q' = r_\alpha(q) \mid q \in \{1, ..., m\}\} = \{1, ..., m\}$. Окончательно для произвольного номера $q' \in \{1, ..., m\}$ существует подходящий номер $q \in \{1, ..., m\}$ такой, что $M_{q'}^{\alpha^{-1}} = M_q$. Отсюда, $\alpha^{-1} \in A(M_1, ..., M_m)$. Лемма доказана. □

Лемма 2. *Пусть $a_u, a_v, a_x, a_y \in M$ для некоторых $u, v, x, y \in \{1, ..., k\}$ и выполняется равенство $a_u * a_v = a_x * a_y$. Тогда возможен один из случаев:*

1. *справедливы равенства $u = x, v = y$;*

2. *существует номер $q \in \{1, ..., m\}$ такой, что $(a_u, a_v), (a_x, a_y) \in M_q$.*

Доказательство. Возможны следующие случаи: а) $(a_u, a_v) \in M_q$ для некоторого подходящего номера q; б) $(a_u, a_v) \in D$.

Предположим, что выполняется случай б). Тогда $a_u * a_v = b_{u,v}$ и $a_x * a_y = b_{u,v}$. Отсюда получаем, что $a_x * a_y = b_{x,y} = b_{u,v}$ и $x = u$, $y = v$. Таким образом, выполняется ситуация 1).

Предположим, что выполняется случай а). Тогда $a_u * a_v = c_q$ и $a_x * a_y = c_q$. Значит, верно включение $(a_x, a_y) \in M_q$ и выполняется случай 2). Лемма доказана. □

Обозначения, связанные с действием автоморфизма. Пусть $\mathfrak{A} = (V, *)$ – магма, $\phi \in Aut\ (\mathfrak{A})$ и x – некоторый элемент из V. Тогда x^ϕ – образ элемента $x \in V$ под действием ϕ (еще элемент x^ϕ называем ***ϕ–образом*** элемента x). Кроме того, если $\phi_1, \phi_2 \in Aut\ (\mathfrak{A})$ и $x \in V$, то $x^{\phi_1 \cdot \phi_2} := (x^{\phi_2})^{\phi_1}$. Пусть $Q \subseteq V$ и $\phi \in Aut\ (\mathfrak{A})$. Тогда

$$Q^\phi := \{x^\phi \mid x \in Q\}.$$

Лемма 3. *Для любого $\phi \in Aut(\mathfrak{G})$ справедливы включения*

$$M^\phi \subseteq M, \quad (M * M)^\phi \subseteq M * M.$$

Доказательство. 1) Покажем, что $M^\phi \subseteq M$. Действительно, предположим противное. Тогда выполняется один из двух вариантов:

a) $a_i^\phi = b_{uv}$ для некоторых подходящих i, u, v;

b) $a_i^\phi = c_q$ для некоторых подходящих i, q.

Предположим, что выполняется случай a). Тогда верны равенства

$$a_i^\phi * a_i^\phi = b_{uv} * b_{uv} = b_{uv}, \quad a_i^\phi * a_i^\phi = (a_i * a_i)^\phi = \begin{cases} (b_{ii})^\phi, & (a_i, a_i) \in D, \\ (c_q)^\phi, & (a_i, a_i) \in M_q. \end{cases}$$

В этом случае в элемент b_{uv} есть ϕ–образ элементов a_i, b_{ii} либо элементов a_i, c_q. В обоих случаях элементы различны, и поэтому (и в силу конечности V) нарушается обратимость отображения ϕ.

Предположим, что выполняется условие б). Тогда справедливы равенства

$$a_i^\phi * a_i^\phi = c_q * c_q = c_q, \quad a_i^\phi * a_i^\phi = (a_i * a_i)^\phi = \begin{cases} (b_{ii})^\phi, & (a_i, a_i) \in D, \\ (c_{q'})^\phi, & (a_i, a_i) \in M_{q'}. \end{cases}$$

В этом случае элемент c_q есть ϕ – образ элементов a_i, b_{ii} либо элементов $a_i, c_{q'}$. В обоих случаях элементы различны, и поэтому (и в силу конечности V) нарушается обратимость отображения ϕ.

Таким образом, справедливо равенство $M^\phi \subseteq M$.

2) Покажем, что $(M * M)^\phi \subseteq M * M$. В самом деле, справедливы условия

$$(M * M)^\phi = M^\phi * M^\phi \subseteq M * M.$$

Лемма доказана. □

Замечание 3. Пусть q – некоторый номер из $\{1, ..., m\}$, (a_i, a_j) – некоторый фиксированный элемент из M_q и ϕ – произвольный автоморфизм из Aut $(\mathfrak{G})$. Если $(a_i * a_j)^\phi = x$, то для любой пары $(a_{i'}, a_{j'}) \in M_q$ справедливо равенство $(a_{i'} * a_{j'})^\phi = x$.

Действительно, для всяких двух элементов $(a_i, a_j),\ (a_{i'}, a_{j'}) \in M_q$ выполняются равенства

$$(a_i * a_j) = (a_{i'} * a_{j'}) = c_q, \quad (a_i * a_j)^\phi = (a_{i'} * a_{j'})^\phi = c_q^\phi.$$

Лемма 4. *Пусть $\alpha \in S_k$ и $\phi \in Aut$ $(\mathfrak{G})$ такой, что $\phi: \ a_i \to a_{\alpha(i)}$ $(i = 1, ..., k)$. Тогда перестановка $\alpha \in A(M_1, ..., M_m)$ и для любого номера $q \in \{1, ..., m\}$ справедливы равенства*

$$(c_q)^\phi = c_{q'}, \quad q' = r_\alpha(q).$$

Кроме того, для всякой пары $(a_i, a_j) \in D$ справедливы включение $(a_{\alpha(i)}, a_{\alpha(j)}) \in D$ и равенство:

$$b_{ij}^\phi = b_{\alpha(i),\alpha(j)}.$$

Доказательство. Далее, ϕ – автоморфизм из условия леммы. По определению множество M_q $(1 \leq q \leq m)$ содержит не менее двух различных пар: $(a_{i_1}, a_{j_1}),\ (a_{i_2}, a_{j_2})$. Далее, справедливы равенства

$$c_q^\phi = (a_{i_1} * a_{j_1})^\phi = a_{i_1}^\phi * a_{j_1}^\phi = a_{\alpha(i_1)} * a_{\alpha(j_1)}, \ \ c_q^\phi = (a_{i_2} * a_{j_2})^\phi = a_{i_2}^\phi * a_{j_2}^\phi = a_{\alpha(i_2)} * a_{\alpha(j_2)},$$

$$a_{\alpha(i_1)} * a_{\alpha(j_1)} = a_{\alpha(i_2)} * a_{\alpha(j_2)}.$$

Последнее равенство и лемма 2 приводят к альтернативе: либо $\alpha(i_1) = \alpha(i_2), \ \ \alpha(j_1) = \alpha(j_2)$, либо $(a_{\alpha(i_1)}, a_{\alpha(j_1)}), \ \ (a_{\alpha(i_2)}, a_{\alpha(j_2)}) \in M_{q'}$, где q' – некоторый подходящий номер. Первые равенства невозможны. Предположим, что $\alpha(i_1) = \alpha(i_2), \ \ \alpha(j_1) = \alpha(j_2)$, тогда справедливо равенство $(i_1, j_1) = (i_2, j_2)$, что не возможно в силу выбора этих пар. Значит, выполняются включения и равенства

$$(a_{\alpha(i_1)}, a_{\alpha(j_1)}),\quad (a_{\alpha(i_1)}, a_{\alpha(j_1)}) \in M'_q,\quad a_{\alpha(i_1)} * a_{\alpha(j_1)} = a_{\alpha(i_2)} * a_{\alpha(j_2)} = c_{q'}.$$

Получаем, что $(c_q)^\phi = c_{q'}$.

Последнее равенство и замечание 3 дают включение $(a_{\alpha(i)}, a_{\alpha(j)}) \in M_{q'}$, для любого $(a_i, a_j) \in M_q$.

Таким образом, при любом $q \in \{1, ..., m\}$ имеем равенство $M_q^\alpha = M_{q'}$, для подходящего q'. *Значит, перестановка* $\alpha \in A(M_1, ..., M_m)$*, определено отображение* r_α *и* $q' = r_\alpha(q)$.

Покажем последнее утверждение леммы. Пусть $(a_i, a_j) \in D$. Тогда пара $(a_{\alpha(i)}, a_{\alpha(j)}) \in D$. Докажем последнее утверждение, предположим противное. Значит, существует номер q такой, что $(a_{\alpha(i)}, a_{\alpha(j)}) \in M_q$ и $1 \le q \le m$. В этом случае имеем равенства

$$(b_{ij})^\phi = (a_i * a_j)^\phi = a_i^\phi * a_j^\phi = a_{\alpha(i)} * a_{\alpha(j)} = c_q,\quad (b_{ij})^\phi = c_q.$$

Из равенства $(b_{ij})^\phi = c_q$ вытекает равенство $c_q^{\phi^{-1}} = b_{ij}$.

Учитывая лемму 3 и обратимость ϕ, получаем, что для ϕ^{-1} справедливы равенства

$$a_i^{\phi^{-1}} = a_{\phi^{-1}(i)},\quad i = 1, ..., k.$$

Поэтому ϕ^{-1} удовлетворяет условиям этой леммы, а равенство $c_q^{\phi^{-1}} = b_{ij}$ дает противоречие с утверждением этой леммы ($(c_q)^\phi = c_{q'},\quad q' = r_\alpha(q)$), доказанным выше.

Мы показали, что если $(a_i, a_j) \in D$*, то* $(a_{\alpha(i)}, a_{\alpha(j)}) \in D$. Далее, равенства

$$(b_{ij})^\phi = (a_i * a_j)^\phi = a_i^\phi * a_j^\phi = a_{\alpha(i)} * a_{\alpha(j)} = b_{\alpha(i),\alpha(j)}$$

завершают доказательство леммы. Лемма доказана.

□

Лемма 5. *Пусть* α *– перестановка из* $A(M_1, ..., M_m)$*. Тогда отображение*

$$\phi_\alpha:\ a_i \to a_{\alpha(i)}\quad (1 \le i \le k),\qquad b_{uv} \to b_{\alpha(u),\alpha(v)}\quad ((a_u, a_v) \in D), \tag{4}$$

$$c_q \to c_{q'},\quad q' = r_\alpha(q)\quad (1 \le q \le m)$$

является автоморфизмом системы $\mathfrak{G}$*. Отображения вида (4) существуют.*

Доказательство. Единичная подстановка удовлетворяет условию леммы. Поэтому отображения ϕ_α вида (4) существуют. Отображение ϕ_α обратимо. Действительно, $\phi_\alpha^{-1} = \phi_{\alpha^{-1}}$. Далее, покажем, что для любых $x, y \in V$ выполняется равенство

$$(x * y)^{\phi_\alpha} = x^{\phi_\alpha} * y^{\phi_\alpha}.$$

а) Пусть $(a_i, a_j) \in M_q$, при $1 \le q \le m$. Тогда $(a_i^{\phi_\alpha}, a_j^{\phi_\alpha}) = (a_{\alpha(i)}, a_{\alpha(j)}) \in M_{q'}$, где $q' = r_\alpha(q)$. Справедливы равенства

$$(a_i * a_j)^{\phi_\alpha} = (c_q)^{\phi_\alpha} = c_{q'},\quad a_i^{\phi_\alpha} * a_j^{\phi_\alpha} = a_{\alpha(i)} * a_{\alpha(j)} = c_{q'},$$

которые показывают, что $(a_i * a_j)^{\phi_\alpha} = a_i^{\phi_\alpha} * a_j^{\phi_\alpha}$.

б) Автоморфизм ϕ_α удовлетворяет условиям леммы 4. Значит, если $(a_i, a_j) \in D$, то $(a_{\alpha(i)}, a_{\alpha(j)}) \in D$. Пусть $(a_i, a_j) \in D$. Тогда справедливы равенства

$$(b_{ij})^{\phi_\alpha} = b_{\alpha(i),\alpha(j)}, \quad (b_{ij})^{\phi_\alpha} = (a_i * a_j)^{\phi_\alpha}, \quad a_i^{\phi_\alpha} * a_j^{\phi_\alpha} = a_{\alpha(i)} * a_{\alpha(j)} = b_{\alpha(i),\alpha(j)},$$

которые показывают справедливость равенства $(a_i * a_j)^{\phi_\alpha} = a_i^{\phi_\alpha} * a_j^{\phi_\alpha}$.

в) Пусть $a_q \in M$, $b_{ij} \in B$. Тогда $(a_i, a_j) \in D$ и равенства

$$(b_{ij})^{\phi_\alpha} = b_{\alpha(i),\alpha(j)}, (b_{ij})^{\phi_\alpha} = (a_q * b_{ij})^{\phi_\alpha}, a_q^{\phi_\alpha} * (b_{ij})^{\phi_\alpha} = a_{\alpha(q)} * b_{\alpha(i),\alpha(j)} = b_{\alpha(i),\alpha(j)};$$

$$(b_{ij})^{\phi_\alpha} = (b_{ij} * a_q)^{\phi_\alpha}, \ b_{ij}^{\phi_\alpha} * a_q^{\phi_\alpha} = b_{\alpha(i),\alpha(j)} * a_{\alpha(q)} = b_{\alpha(i),\alpha(j)}$$

показывают, что $(a_q * b_{ij})^{\phi_\alpha} = a_q^{\phi_\alpha} * b_{ij}^{\phi_\alpha}$, $(b_{ij} * a_q)^{\phi_\alpha} = b_{ij}^{\phi_\alpha} * a_q^{\phi_\alpha}$.

Далее, из соотношений

$$(c_i)^{\phi_\alpha} = c_{i'}, \quad (c_i)^{\phi_\alpha} = (c_i * a_q)^{\phi_\alpha} = (a_q * c_i)^{\phi_\alpha},$$

$$a_q^{\phi_\alpha} * c_i^{\phi_\alpha} = a_{\alpha(q)} * c_{i'} = c_{i'}, \quad c_i^{\phi_\alpha} * a_q^{\phi_\alpha} = c_{i'} * a_{\alpha(q)} = c_{i'}$$

получаем справедливость равенств $(c_i * a_q)^{\phi_\alpha} = c_i^{\phi_\alpha} * a_q^{\phi_\alpha}$, $(a_q * c_i)^{\phi_\alpha} = a_q^{\phi_\alpha} * c_i^{\phi_\alpha}$.

г) Покажем, что $(x * y)^{\phi_\alpha} = x^{\phi_\alpha} * y^{\phi_\alpha}$, когда $x, y \in M * M$. Равенства

$$(b_{ij})^{\phi_\alpha} = b_{\alpha(i),\alpha(j)}, \quad (c_i)^{\phi_\alpha} = c_{i'}, \quad (c_w)^{\phi_\alpha} = c_{w'},$$

$$(b_{ij})^{\phi_\alpha} = (b_{ij}*b_{uv})^{\phi_\alpha}, \ (c_i)^{\phi_\alpha} = (c_i*c_j)^{\phi_\alpha}, \ (b_{ij})^{\phi_\alpha} = (b_{ij}*c_w)^{\phi_\alpha}, \ (c_w)^{\phi_\alpha} = (c_w*b_{ij})^{\phi_\alpha},$$

$$b_{ij}^{\phi_\alpha} * b_{uv}^{\phi_\alpha} = b_{\alpha(i),\alpha(j)} * b_{\alpha(u),\alpha(v)} = b_{\alpha(i),\alpha(i)}, \quad c_i^{\phi_\alpha} * c_j^{\phi_\alpha} = c_{i'} * c_{j'} = c_{i'},$$

$$b_{ij}^{\phi_\alpha} * c_w^{\phi_\alpha} = b_{\alpha(i),\alpha(j)} * c_{w'} = b_{\alpha(i),\alpha(j)}, \quad c_w^{\phi_\alpha} * b_{ij}^{\phi_\alpha} = c_{w'} * b_{\alpha(i),\alpha(j)} = c_{w'}$$

показывают, что

$$(b_{ij} * b_{uv})^{\phi_\alpha} = b_{ij}^{\phi_\alpha} * b_{uv}^{\phi_\alpha}, \quad (c_i * c_j)^{\phi_\alpha} = c_i^{\phi_\alpha} * c_j^{\phi_\alpha}, \quad (b_{ij} * c_w)^{\phi_\alpha} = b_{ij}^{\phi_\alpha} * c_w^{\phi_\alpha}$$

$$(c_w * b_{ij})^{\phi_\alpha} = c_w^{\phi_\alpha} * b_{ij}^{\phi_\alpha}.$$

Лемма доказана. □

Лемма 6. *Пусть $\alpha, \beta \in A(M_1, ..., M_m)$ и ϕ_α, ϕ_β – автоморфизмы системы $\mathfrak{G}$, заданные условиями (4). Тогда справедливо равенство*

$$\phi_\alpha \cdot \phi_\beta = \phi_{\alpha \cdot \beta}, \tag{5}$$

а перестановка $\alpha \cdot \beta \in A(M_1, ..., M_2)$.

Доказательство. Если расписать действие отображений $\phi_{\alpha\cdot\beta}$ и $\phi_\alpha \cdot \phi_\beta$ на множестве V, то получим равенство 5. Лемма доказана. □

Доказательство Теоремы 1. Введем обозначение

$$R := \{\phi_\alpha \mid \alpha \in A(M_1, ..., M_m)\}.$$

В силу Леммы 5 справедливо включение $R \subseteq Aut\ (\mathfrak{G})$.

Пусть ϕ – произвольный автоморфизм магмы $\mathfrak{G}$. Покажем, что $\phi \in R$. Учитывая результаты Леммы 3 и свойства системы $\mathfrak{G}$ имеем условия:

$$M^\phi \subseteq M, \quad (M * M)^\phi \subseteq M * M, \tag{6}$$

$$V = M \cup (M * M), \quad M \cap (M * M) = \varnothing,$$

которые дают равенства $a_i^\phi = a_{\gamma(i)}$ для $i = 1, ..., k$. В силу обратимости ϕ и условий (6) получаем, что $\gamma \in S_k$ и $M^\phi = M$. Значит, ϕ удовлетворяет условиям лемма 4, следовательно, справедливы включение $\gamma \in A(M_1, ..., M_m)$ и равенства:

$$(c_q)^\phi = c'_q, \quad q' = r_\gamma(q), \quad (b_{ij})^\phi = b_{\gamma(i),\gamma(j)}, \quad (a_i, a_j) \in D.$$

Таким образом, мы показали, что произвольный автоморфизм ϕ из $Aut\ (\mathfrak{G})$ является автоморфизмом $\phi_\gamma \in R$. Отсюда,

$$Aut\ (\mathfrak{G}) \subseteq R, \quad Aut\ (\mathfrak{G}) = R.$$

Первая часть теоремы доказана.

Далее, отображение $\zeta :\ A(M_1, ..., M_m) \to Aut\ (\mathfrak{G})$, заданное правилом

$$\zeta(\alpha) = \phi_\alpha \quad (\alpha \in A(M_1, ..., M_m), \quad \phi_\alpha \in R),$$

реализует биекцию множества $A(M_1, ..., M_m)$ на множество $Aut\ (\mathfrak{G})$. Действительно, это следует из первого утверждения данной теоремы, которое доказано выше. Лемма 6 показывает, что ζ – изоморфизм группы $A(M_1, ..., M_m)$ на группу $Aut\ (\mathfrak{G})$. Теорема 1 доказана. □

2. Примеры и доказательство Теоремы 2

В данном разделе строятся Примеры 1, 2, 3, 4 и 5. Эти примеры показывают существование магм $\mathfrak{G}_i,\ i = 1, 2, 3, 4, 5$ из Теоремы 2. Таким образом, приведенные примеры доказывают Теорему 2.

Элемент множества $(a_i, a_j) \in M \times M$ будем обозначать (для удобства) символом $P_{i,j}$. Кроме того, в этом разделе множества $\{1, ..., k\},\ k \in \mathbb{N}$ считаем подмножеством множества $\mathbb{N}$. Это дает возможность применять арифметические операции и сравнивать числа.

Из Определения 2 следует, что перестановка $\alpha \in S_k$ лежит в группе $A(M_1)$ тогда и только тогда, когда $M_1^\alpha = M_1$.

Пример 1. Пусть $k \in \mathbb{N},\ k > 1$ и задана магма $\mathfrak{G} = \mathfrak{G}(k, m, M_1, ..., M_m)$ такая, что $m = 1$ и

$$M_1 := \{P_{1,1}, P_{2,2}, ..., P_{k,k}\}.$$

Используя Определение 2, получаем равенство $A(M_1) = S_k$. Действительно, с одной стороны $A(M_1) \subseteq S_k$. С другой стороны видим, что всякая перестановка $\alpha \in S_k$ удовлетворяет равенству $M_1^\alpha = M_1$, следовательно, $A(M_1) = S_k$.

Теорема 1 показывает, что справедливы условия

$$Aut\ (\mathfrak{G}) \cong A(M_1) = S_k.$$

Таким образом, магма $\mathfrak{G}$ является магмой $\mathfrak{G}_1$ из Теоремы 2.

Пример 2. Пусть $k, k' \in \mathbb{N},\ \ 1 \leq k' \leq k,\ k > 1$ и $L := \{s_1, s_2, ..., s_{k'}\}$ – подмножество множества $\{1, ..., k\}$, состоящее из k' различных элементов ($|L| = k'$). Задаем магму $\mathfrak{G} = \mathfrak{G}(k, m, M_1, ..., M_m)$ такую, что $m = 1$ и

$$M_1 := \{P_{s_1,s_1}, P_{s_2,s_2}, ..., P_{s_{k'},s_{k'}}\}.$$

Имеем равенство $A(M_1) = St(L)$. Покажем справедливость этого равенства. Не трудно увидеть, что любая перестановка $\alpha \in St(L)$ будет удовлетворять равенству $M_1^\alpha = M_1$, следовательно, $St(L) \subseteq A(M_1)$. С другой стороны, если $\alpha \notin St(L)$, то существует элемент $s_w \in L$ такой, что $\alpha(s_w) \notin L$. Значит, $M_1^\alpha \neq M_1$. Отсюда получаем равенство $A(M_1) = St(L)$.

Тогда Теорема 1 показывает существование изоморфизма

$$Aut\ (\mathfrak{G}) \cong A(M_1) = St(L).$$

Мы получили, что $\mathfrak{G}$ является магмой $\mathfrak{G}_2$ из Теоремы 2.

Пример 3. Пусть $k \in \mathbb{N},\ k > 1$ и задана магма $\mathfrak{G} = \mathfrak{G}(k, m, M_1, ..., M_m)$ такая, что $m = 1$ и

$$M_1 := \{P_{1,k}, P_{2,1}, P_{3,2}, P_{4,3}, ..., P_{x,x-1}, ..., P_{k,k-1}\} \qquad (x < k).$$

Очевидно, что элемент $P_{a,b} \in M_1\ \ (a, b \in \{1, ..., k\})$ тогда и только тогда, когда $(a, b) = (1, k)$ или $a - b = 1$.

Далее, вводим группу

$$a := \begin{pmatrix} 1 & 2 & 3 & ... & k \\ 2 & 3 & 4 & ... & 1 \end{pmatrix}, \qquad C_k := \langle a \rangle\,.$$

Очевидно, что имеет место равенство $a^k = 1$ и C_k – циклическая группа порядка k, порожденная элементом a (C_k реализована как подгруппа S_k).

Перестановка $\beta \in S_k$ лежит в группе C_k тогда и только тогда, когда для любых двух $x, y \in \{1, ..., k\}$ таких, что $x - y = 1$ будет выполняться одно из равенств

$$\beta(x) - \beta(y) = 1, \quad \beta(x) - \beta(y) = -k + 1. \tag{7}$$

Отметим, что для каждой перестановки $\beta \in C_k$ существует только одна пара $(a, b),\ \ a, b \in \{1, ..., k\}$ такая, что $\beta(a) - \beta(b) = -k + 1$.

Имеем равенство $A(M_1) = C_k$. В самом деле, легко увидеть, что для любой перестановки $\alpha \in C_k$ выполняется равенство $M_1^\alpha = M_1$, которое показывает справедливость включения $C_k \subseteq A(M_1)$. Далее, полагаем $\alpha \in A(M_1)$ и $\alpha \notin C_k$. Тогда, в силу условия (7), получаем, что существуют элементы $a, b \in \{1, ..., k\}$ такие, что

$a - b = 1$ и $\alpha(a) - \alpha(b) \neq 1$ и $\alpha(a) - \alpha(b) \neq -k+1$. Это означает, что элементы $P_{\alpha(a),\alpha(b)} \notin M_1$, следовательно, $\alpha \notin A(M_1)$. Полученное противоречие и включение $C_k \subseteq A(M_1)$ дают равенство $A(M_1) = C_k$.

Далее, Теорема 1 показывает, что справедливо равенство и изоморфизм

$$Aut\ (\mathfrak{G}) \cong A(M_1) = C_k.$$

Магма $\mathfrak{G}$ будет является магмой $\mathfrak{G}_3$ из Теоремы 2.

Пример 4. *Четвертная группа Клейна.* Зададим магму $\mathfrak{G} = \mathfrak{G}(4, 1, M_1)$ такую, что

$$M_1 = \{P_{1,4}, P_{4,1}\}.$$

Далее, $a := (1, 4),\ b := (2, 3),\ ab = (1, 4)(2, 3)$. Для этих перестановок справедливы равенства $a^2 = b^2 = (ab)^2 = 1$. Рассмотрим D_4 – перестановочную реализацию четвертной группы Клейна:

$$D_4 = \{1, (1, 4), (2, 3), (1, 4)(2, 3)\}.$$

Прямое вычисление множества $A(M_1)$ показывает, что справедливо равенство $A(M_1) = D_4$. Теорема 1 дает изоморфизмы $Aut\ (\mathfrak{G}) \cong D_4$.

Магма $\mathfrak{G}$ является магмой $\mathfrak{G}_4$ из Теоремы 2.

Пример 5. Полагаем, что $k \in \mathbb{N},\ k > 1$ и a, b – два различных элемента из множества $\{1, ..., k\}$. Пусть задана магма $\mathfrak{G} = \mathfrak{G}(k, m, M_1, ..., M_m)$ такая, что $m = 1$ и выполняются равенства

$$M_1 := \{P_{a,a}, P_{a,b}\}.$$

Докажем равенство $A(M_1) = Stab(a) \cap Stab(b)$. Пусть $\alpha \in Stab(a) \cap Stab(b)$. Тогда непосредственно из определения M_1 видно, что $M_1^\alpha = M_1$. Значит, справедливо включение $Stab(a) \cap Stab(b) \subseteq A(M_1)$. С другой стороны, если $a \notin Stab(a) \cap Stab(b)$, то выполняется хотя бы одно из условий $\alpha(a) \neq a$ или $\alpha(b) \neq b$. Последние условия показывают, что $M_1^\alpha \neq M_1$, следовательно, $A(M_1) = Stab(a) \cap Stab(b)$.

Тогда Теорема 1 показывает, что справедливо условие

$$Aut\ (\mathfrak{G}) \cong A(M_1) = Stab(a) \cap Stab(b).$$

Магма $\mathfrak{G}$ является магмой $\mathfrak{G}_5$ из Теоремы 2.

Пример 6. Пусть $n \in \mathbb{N},\quad n \geq 2$ и

$$a := \begin{pmatrix} 1 & 2 & ... & n & n+1 & ... & 2n-2 & 2n-1 & 2n \\ 3 & 4 & ... & n+2 & n+3 & ... & 2n & 1 & 2 \end{pmatrix},$$

$$b := \begin{pmatrix} 1 & 2 & 3 & ... & n & n+1 & n+2 & ... & 2n \\ 2n & 2n-1 & 2n-2 & ... & n+1 & n & n-1 & ... & 1 \end{pmatrix}.$$

Тогда справедливы равенства $a^n = b^2 = (ab)^2 = 1$, и группа $D_{2n} := \langle a, b \rangle$ является группой Диэдра порядка $2n$.

Далее, полагаем, что $k := 2n$ и строим магму $\mathfrak{G} = \mathfrak{G}(k, 1, M_1)$. Мы хотим построить магму $\mathfrak{G}$ так, чтобы группа D_{2n} содержалась в группе $A(M_1)$. Строим множество M_1 по следующему алгоритму:

1. фиксируем пару $P_{i,j}$;
2. задаем множество M_1:

$$M_1 = \{P_{\alpha(i),\alpha(j)} \mid \alpha \in D_{2n}\}.$$

В нашем случае выбираем $P_{i,j} = P_{1,k}$ и получаем:

$$M_1 := \{P_{1,k}, P_{3,2}, P_{5,4}, ..., P_{x,x-1}, P_{x+2,x+1}, ..., P_{k-1,k-2}\} \cup$$

$$\cup \{P_{k,1}, P_{2,3}, P_{4,5}, ..., P_{x-1,x}, P_{x+1,x+2}, ..., P_{k-2,k-1}\}.$$

Непосредственная проверка показывает, что всякая перестановка $\alpha \in D_{2n}$ оставляет на месте множество M_1 (т.е. $M_1^\alpha = M_1$), следовательно, $\alpha \in A(M_1)$.

Таким образом, мы показали, что группа D_{2n} изоморфна подгруппе H группы $Aut\ (\mathfrak{G})$ и справедливо равенство $H := \{\phi_\alpha \mid \alpha \in D_{2n}\}$.

В этом случае вся группа $A(M_1) \cong Aut\ (\mathfrak{G})$ будет порождаться всевозможными перестановками $\alpha_{a,b} \in S_k$ такими, что $P_{\alpha_{a,b}(a),\alpha_{a,b}(b)} \in M_1$, $\alpha_{a,b}^2 = 1$ и для всякого $x \neq a, b, \alpha_{a,b}(a), \alpha_{a,b}(b)$ справедливо равенство $\alpha_{a,b}(x) = x$.

Четвертная группа Клейна. Рассмотрим случай $n = 2$ подробней. В этом случае:

$$M_1 = \{P_{1,4}, P_{2,3}, P_{3,2}, P_{4,1}\},$$

$$D_4 = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}.$$

Прямые вычисления множества $A(M_1)$ показывают, что справедливы условия

$$Aut\ (\mathfrak{G}) \cong A(M_1) = \langle D_4, (1,4), (2,3) \rangle .$$

Способ построения множества M_1, который мы использовали в примере 6 позволяет для произвольной конечной группы перестановок G построить магму $\mathfrak{G} = \mathfrak{G}(k, 1, M_1)$ такую, что $G \subseteq A(M_1)$. В самом деле, если G – единичная группа, то она изоморфна единичной подгруппе любой группы. Если $|G| \neq 1$, то полагаем $k = |G|$, фиксируем пару $P_{i,j}$ и задаем множество $M_1 = \{P_{\alpha(i),\alpha(j)} \mid \alpha \in G\}$. В этом случае группа $Aut\ (\mathfrak{G})$ не обязана быть изоморфна группе $S_{|G|}$ (этот способ построения магмы $\mathfrak{G}$ отличается от того, который приводится во ведение для доказательства Следствия 1).

Заключение

Результаты Теоремы 1 могут быть использованы для теоретического исследования групп автоморфизмов магмы $\mathfrak{G} = \mathfrak{G}(k, m, M_1, ..., M_m) = (V, *)$. Это иллюстрирует Теорема 2, которая доказывается с помощью результатов Теоремы 1. При этом Теорема 2 дает примеры магм $\mathfrak{G}$, которые имеют в качестве группы автоморфизмов некоторые хорошо известные группы. Кроме того, Теорема 2 дает Следствие 1, которое показывает, что всякая конечная группа G будет изоморфна некоторой подгруппе группы $Aut\ (\mathfrak{G}(k, 1, M_1))$; если $|G| \neq 1$, то $k = |G|$.

Определение 2 дает достаточно простой практический способ вычисления множества $A(M_1, ..., M_m)$. В частности, с помощью результатов Теоремы 1 и Определения 2 можно организовать поэлементное нахождение группы $Aut\ (\mathfrak{G})$ с помощью перебора перестановок из S_k. При этом проверка (с помощью определению 2) принадлежности перестановки $\alpha \in S_k$ множеству $A(M_1, ..., M_m)$ проще, чем проверка того, что перестановка $\beta \in S_{|V|}$ (справедливо неравенство $|V| \geq k + 1$) сохраняет операцию умножения $*$.

Список литературы

[1] Плоткин Б.И. Группы автоморфизмов алгебраических систем. М.: Наука, 1966.

[2] Литаврин А.В. Автоморфизмы некоторых магм порядка $k + k^2$ // Известия Иркутского государственного университета. Серия: Математика. 2018. Т. 26. С. 47–61.

[3] Schreier O. Die Automorphismen der projektiven Gruppen // Abhandlungen aus dem Mathematischen Seminar der Universitat Hamburg. 1928. Vol. 6. Pp. 303–322.

[4] Мерзляков Ю.И. Автоморфизмы классических групп. М.: Мир, 1976.

[5] Hahn A.J., James A.J., Hahn D.G., Weisfeiler B. Homomorphisms of algebraic and classical groups: a survey // Canadian Journal of Mathematics. 1984. № 4. Pp. 249–296.

[6] Петечук В.М. Автоморфизмы матричных групп над коммутативными кольцами // Математический сборник. 1982. Т. 117, № 4. С. 534–547.

[7] Abe E. Automorphisms of Chevalley groups over commutative rings // Algebra and Analysis. 1993. Vol. 5, № 2. Pp. 74–90.

[8] Gibbs J. Automorphisms of certain unipotent groups // Journal of Algebra. 1970. Vol. 14, № 2. Pp. 203–228.

[9] Левчук В.М. Автоморфизмы унипотентных подгрупп групп Шевалле // Алгебра и логика. 1990. Т. 29, № 2. С. 141–161.

[10] Левчук В.М. Связи унитреугольной группы с некоторыми кольцами. Ч. 2. Группы автоморфизмов // Сибирский математический журнал. 1983. Т. 24, № 4. С. 543–557.

[11] Bunina E.I. Automorphisms of Chevalley groups of different types over commutative rings // Journal of Algebra. 2012. Vol. 355, № 1. Pp. 154–170.

[12] Глускин Л.М. Автоморфизмы мультипликативных полугрупп матричных алгебр // Успехи математических наук. 1956. Т. 11, № 1. С. 199–206.

[13] Михалев А.В., Шаталова М.А. Автоморфизмы и антиавтоморфизмы, полугруппы обратимых матриц с неотрицательными элементами // Математический сборник. 1970. Т. 81, № 4. С. 600–609.

[14] Бунина Е.И., Семенов П.П. Автоморфизмы полугруппы обратимых матриц с неотрицательными элементами над коммутативными частично упорядоченными кольцами // Фундаментальная и прикладная математика. 2008. Т. 14, № 2. С. 69–100.

[15] Халезов Е.А. Автоморфизмы матричных полугрупп // Доклады Академии наук СССР. 1954. Т. 96, № 2. С. 245–248.

[16] Халезов Е.А. Автоморфизмы примитивных квазигрупп // Математический сборник. 1961. Т. 53, № 3. С. 329–342.

[17] Ильиных А.П. Классификация конечных группоидов с 2 транзитивной группой автоморфизмов // Математический сборник. 1994. Т. 185, № 6. С. 51–78.

[18] Ильиных А.П. Группоиды порядка $q(q \pm 1)/2, q = 2r$, имеющие группу автоморфизмов, изоморфную SL(2,q) // Сибирский математический журнал. 1995. Т. 36, № 6. С. 1336–1341.

[19] Мальцев А.И. Алгебраические системы. М.: Наука, 1970.

Образец цитирования

Литаврин А.В. Автоморфизмы некоторых конечных магм с порядком строго меньше числа N(N+1) и порождающим множеством из N элементов // Вестник ТвГУ. Серия: Прикладная математика. 2019. № 2. С. 70–87. https://doi.org/10.26456/vtpmk533

Сведения об авторах

1. **Литаврин Андрей Викторович**
старший преподаватель кафедры высшей математики № 2 института математики и фундаментальной информатики Сибирского федерального университета.

Россия, 660041, г. Красноярск, пр. Свободный, д. 79, СФУ.
E-mail: anm11@rambler.ru

AUTOMORPHISMS OF SOME FINITE MAGMAS WITH AN ORDER STRICTLY LESS THAN THE NUMBER N(N+1) AND A GENERATING SET OF N ELEMENTS

Litavrin Andrey Viktorovich
Senior Lecturer in the Department of Higher Mathematics No. 2, Institute of Mathematics and Fundamental Informatics, Siberian Federal University
Russian Federation, 660041, Krasnoyarsk, Svobodny av., 79, SFU.
E-mail: anm11@rambler.ru

Received 29.11.2018, revised 19.03.2019.

In this paper, we study the problems of describing automorphism groups of certain finite magmas. Some finite magmas $\mathfrak{G} = (V, *)$, generated by n elements and order $|V|$, satisfying the inequalities $n + 1 \leq |V| < n^2 + n$. Constructed magmas $\mathfrak{G}$ are not semigroups or quasigroups. For the magmas $\mathfrak{G}$, the general form of the automorphism is indicated and the description of the group of all automorphisms is given. It is shown that the group of all automorphisms is isomorphic to a certain subgroup (the description of this group is given) of the symmetric permutation group S_n, where n is the number of elements of a suitable generating set of the magma $\mathfrak{G}$. It is proved that every finite cyclic group of order $n \geq 2$ is isomorphic to the group of all automorphisms of the appropriate magma $\mathfrak{G}$. A similar result was obtained for the fourth Klein group. In addition, it was shown that for any finite group G you can choose a suitable magma $\mathfrak{G}$ such that G is isomorphic to some subgroup of Aut ($\mathfrak{G}$) (an algorithm for constructing magma is given $\mathfrak{G}$ for an arbitrary finite group G).

Keywords: magmas, groupoids, finite magma automorphisms, finite groupoid automorphisms, finite cyclic group, Dihedron group.

Citation

Litavrin A.V., "Automorphisms of some finite magmas with an order strictly less than the number N(N+1) and a generating set of N elements", *Vestnik TvGU. Seriya: Prikladnaya Matematika [Herald of Tver State University. Series: Applied Mathematics]*, 2019, № 2, 70–87 (in Russian). https://doi.org/10.26456/vtpmk533

References

[1] Plotkin B.I., *Gruppy avtomorfizmov algebraicheskikh sistem [Automorphism groups of algebraic systems]*, Nauka Publ., Moscow, 1966 (in Russian).

[2] Litavrin A.V., "Automorphisms of some magmas of order $k + k^2$", *Izvestiya Irkutskogo gosudarstvennogo universiteta. Seriya: Matematika [Bulletin of the Irkutsk State University. Series: Mathematics]*, **26** (2018), 47–61 (in Russian).

[3] Schreier O., "Die Automorphismen der projektiven Gruppen", *Abhandlungen aus dem Mathematischen Seminar der Universitat Hamburg*, **6** (1928), 303–322.

[4] Merzlyakov Yu.I., *Avtomorfizmy klassicheskikh grupp [Automorphisms of classical groups]*, Mir Publ., Moscow, 1976 (in Russian).

[5] Hahn A.J., James A.J., Hahn D.G., Weisfeiler B., "Homomorphisms of algebraic and classical groups: a survey", *Canadian Journal of Mathematics*, 1984, № 4, 249–296.

[6] Petechuk V.M., "Automorphisms of matrix groups over commutative ring", *Mathematics of the USSR-Sbornik*, **45**:4 (1983), 527–542.

[7] Abe E., "Automorphisms of Chevalley groups over commutative rings", *Algebra and Analysis*, **5**:2 (1993), 74–90.

[8] Gibbs J., "Automorphisms of certain unipotent groups", *Journal of Algebra*, **14**:2 (1970), 203–228.

[9] Levchuk V.M., "Automorphisms of unipotent subgroups of Chevalley groups", *Algebra i logika [Algebra and logic]*, **29**:2 (1990), 141–161 (in Russian).

[10] Levchuk V.M., "Connections of the unitriangular group with some rings. Part 2. Automorphism groups", *Siberian Mathematical Journal*, **24**:4 (1983), 543–557 (in Russian).

[11] Bunina E.I., "Automorphisms of Chevalley groups of different types over commutative rings", *Journal of Algebra*, **355**:1 (2012), 154–170.

[12] Gluskin L.M., "Automorphisms of multiplicative semigroups of matrix algebras", *Uspekhi Matematicheskikh Nauk [Russian Mathematical Surveys]*, **11**:1 (1956), 199–206 (in Russian).

[13] Mikhalev A.V., Shatalova M.A., "Automorphisms and anti-automorphisms of a semigroup of invertible matrices with nonnegative elements", *Mathematics of the USSR-Sbornik*, **10**:4 (1970), 547–555.

[14] Bunina E.I., Semenov P.P., "Automorphisms of the semigroup of invertible matrices with nonnegative elements over commutative partially ordered rings", *Fundamentalnaya i prikladnaya matematika [Fundamental and Applied Mathematics]*, **14**:2 (2008), 69–100 (in Russian).

[15] Khalezov E.A., "Automorphisms of matrix semigroups", *Soviet Mathematics. Doklady*, **96**:2 (1954), 245–248 (in Russian).

[16] Khalezov E.A., "Automorphisms of primitive quasigroups", *Sbornik: Mathematics*, **53**:3 (1961), 329–342 (in Russian).

[17] Ilinykh A.P., "Classification of finite groupoids with 2 transitive automorphism groups", *Sbornik: Mathematics*, **185**:6 (1994), 51–78 (in Russian).

[18] Ilinykh A.P., "Groupoids of order $q(q \pm 1)/2, q = 2r$ with automorphism group isomorphic to SL (2, q)", *Siberian Mathematical Journal*, **36**:6 (1995), 1336–1341 (in Russian).

[19] Maltsev A.I., *Algebraicheskie sistemy [Algebraic systems]*, Nauka Publ., Moscow, 1970 (in Russian).