УДК 512.54+512.57

Подсистемы и автоморфизмы некоторых конечных магм порядка $k + k^2$

А. В. Литаврин

Литаврин Андрей Викторович, кандидат физико-математических наук, доцент кафедры высшей математики № 2, Сибирский федеральный университет, Россия, 660041, г. Красноярск, просп. Свободный, д. 79, anm11@rambler.ru

Данная работа посвящена изучению подсистем некоторых конечных магм $\mathfrak{S} = (V, *)$ с порождающим множеством из k элементов и порядком $k + k^2$. При $k > 1$ магмы $\mathfrak{S}$ не являются полугруппами и квазигруппами. Приводится поэлементное описание всех подсистем магмы $\mathfrak{S}$. Было установлено, что все магмы $\mathfrak{S}$ обладают подсистемами, являющимися полугруппами. При $k > 1$ явно указываются подсистемы, являющиеся идемпотентными не единичными полугруппами. Ранее для магм $\mathfrak{S}$ было получено описание группы автоморфизмов. В частности, всякая симметрическая группа перестановок S_k изоморфна группе всех автоморфизмов подходящей магмы $\mathfrak{S}$. В данной работе получен общий вид автоморфизма для более широкого класса конечных магм порядка $k + k^2$.

Ключевые слова: магма, группоид, подсистемы магм, автоморфизмы группоидов, автоморфизмы магм, подгруппоиды.

Поступила в редакцию: 01.09.2019 / Принята: 30.09.2019 / Опубликована: 30.11.2020

DOI: https://doi.org/10.18500/1816-9791-2020-20-4-457-467

ВВЕДЕНИЕ

Как и в [1], *магмой* называем пару $(V, *)$, где V — некоторое множество и $(*)$ — бинарная алгебраическая операция, определенная на множестве V (также распространен термин *группоид*).

В данной работе исследуются вопросы об автоморфизмах и подсистемах некоторых конечных магм. В частности, обобщаются результаты работы [2] и приводится поэлементное описание всех подсистем конечных магм $\mathfrak{S} = \mathfrak{S}(k, q) = (V, *)$ (см. [2, определение 1]) порядка $k + k^2$. Основные результаты статьи сформулированы в теоремах 1 и 2.

Ниже приведем примеры исследований магм, не являющихся, в общем случае, полугруппами и квазигруппами.

А. И. Мальцев вводит в работе [3] операцию умножения на подмногообразиях фиксированного многообразия (данная операция использовалась в исследованиях классов алгебраических систем). Структуры некоторых магм, введенных в [3], вместе с другими вопросами (из теории классов алгебраических систем) исследовались, например, в работах [4–6] (см. также [7–9]).

Другим естественным подходом к исследованию магм является введение дополнительных ограничений, например требование выполнения некоторых тождеств или условий. В [10] рассматриваются магмы с тождеством $xy \cdot zx = (x \cdot yz)x$. В работе [11] авторы Г. Б. Белявская и А. Х. Табаров изучают некоторые классы магм с тождеством $xy \cdot xz = x^2 \cdot yz$ (см. также [12]). А. А. Степанова и Н. В. Трикашная

в [13] рассматривают магмы, являющиеся абелевыми алгебрами и гамильтоновыми алгебрами с дополнительными ограничениями (например наличием единицы).

Естественным обобщением понятия «магма» является понятие *n-арный группоид* (также распространен термин *n-оператив*, например, в [14]). Примерами исследований данных объектов являются работы С. С. Давидова [15–17].

Вопросы перестановочности элементов в некоторых n-арных группоидах специального вида (*полиадических группоидах с полиадической операцией*) изучаются в работах А. М. Гальмака [18, 19].

В [20] автор изучает вопросы введения метрики на магмах и практического использования этих конструкций в биологии.

С. Ю. Катышев, В. Т. Марков и А. А. Нечаев в работе [21] изучают возможностнь использовать неассоциативные магмы в криптографии. Авторы используют *ППС-группоиды* (все правые степени перестановочны) и *ПЛС-группоиды* (все левые степени перестановочны), которые обладают неассоциативными степенями для реализации процедуры открытого распределения ключей. (см. также работу [22]). В обзоре В. Т. Маркова, А. В. Михалёва и А. А. Нечаева [23] рассмотрены примеры использования неассоциативных алгебраических структур (в частности, *ПС-группоидов*) для построения криптосхем и линейно-оптимальных кодов.

Отметим серию исследований [24–26], в которых Д. А. Бредихин изучает вопросы, связанные с *группоидами отношений* и многообразиями алгебраических систем. В [27] Л. М. Глускин исследовал автоморфизмы полугрупп бинарных отношений.

Изучению автоморфизмов некоторых матричных полугрупп посвящено множество работ, например [28–30] (также активно изучались автоморфизмы квазигрупп [31]).

Автоморфизмы некоторых специальных матричных магм изучаются в работе [32].

Исследованию вопросов, связанных с автоморфизмами конечных магм, посвящены статьи А. П. Ильиных [33, 34]. В [33] приведена классификация конечных магм $\mathfrak{X} = (X, *)$, имеющих 2-транзитивную на множестве X группу автоморфизмов $Aut\,(\mathfrak{X})$. В [34] построены две серии магм, допускающие $SL(2, q)$ транзитивной (транзитивной на множестве-носителе) подгруппой автоморфизмов.

В работе [35] строятся некоторые конечные магмы $\mathfrak{G} = (V, *)$, порожденные n элементами и порядком $|V|$, удовлетворяющим неравенствам $n + 1 \leqslant |V| < n^2 + n$. Для этих магм получено описание группы автоморфизмов (см. [35, теорема 1]) и показано, что всякая конечная группа будет изоморфна некоторой подгруппе группы $Aut\,(\mathfrak{G})$ для подходящей магмы $\mathfrak{G}$ (см. [35, следствие 1]).

Для удобства читателя приведем определение 1 из [2] магм $\mathfrak{S} = \mathfrak{S}(k, q) = (V, *)$. Как обычно, S_k — симметрическая группа перестановок множества из k элементов.

Определение 1. Для каждого натурального числа k вводим следующие множества: $M := \{a_1, ..., a_k\}$, $B := \{b_{ij} \mid i, j = 1, ..., k\}$, $V := M \cup B$, $S_k^m := \{(\varepsilon_1, ..., \varepsilon_m) \mid \varepsilon_i \in \in S_k,\ i = 1, ..., m\}$.

Далее фиксируем кортеж $q = (\beta_1, ..., \beta_k, \beta'_1, ..., \beta'_k) \in S_k^{2k}$. На множестве V зададим бинарную алгебраическую операцию $(*)$ такую, что справедливы равенства

$$\begin{gathered} a_i * a_j = b_{ij}, \quad a_s * b_{ij} = b_{\beta_s(i),\beta_s(j)}, \\ b_{ij} * a_s = b_{\beta'_s(i),\beta'_s(j)}, \quad b_{mv} * b_{ij} = b_{mj} \quad (m, v, s, i, j = 1, ..., k). \end{gathered} \tag{1}$$

Тогда через $\mathfrak{S} = \mathfrak{S}(k, q) = (V, *)$ обозначим магму $\mathfrak{S}$ с множеством-носителем V и операцией $(*)$, которую задают равенства (1).

Несложно проверить, что магмы $\mathfrak{S}(k,q)$ являются неассоциативными магмами при $k > 1$ и любом кортеже $q \in S_k^{2k}$. Данные магмы интересны, в частности, тем, что всякую конечную группу можно представить некоторой подгруппой группы автоморфизмов подходящей магмы $\mathfrak{S}(k,q)$.

Определение *подсистемы* и *порождающего* множества алгебраической системы можно найти в [36, с. 53, 55]).

Далее рассмотрим общую и хорошо известную задачу

Задача 1. *Описать подсистемы некоторой фиксированной алгебраической системы* $\mathfrak{A}$.

Данная задача исследуется в этой работе, когда $\mathfrak{A} = \mathfrak{S}(k,q)$. Основной результат, относящийся к задаче 1, сформулирован в виде теоремы 1.

Для всякого подмножества Q множества-носителя V магмы $\mathfrak{S}(k,q)$ строится подсистема $\mathfrak{D}(Q)$ (см. (2)), порожденная этим множеством. Таким образом, теорема 1 дает решение задачи 1 в виде поэлементного описания подсистем, когда $\mathfrak{A} = \mathfrak{S}(k,q)$.

Кроме того, было установлено, что всякая магма $\mathfrak{S}(k,q)$ будет иметь подсистемы (эти подсистемы явно указаны в замечании 2), которые являются идемпотентными полугруппами.

В данной работе формулируется и доказывается теорема 2, которая обобщает некоторые результаты теоремы 2 из [2]. Теорема 2 дает результат для более широкого класса конечных магм порядка $k+k^2$, чем теорема 2 из [2]. В частности, теорема 2 устанавливает общий вид автоморфизма (см. отображение (7)), параметризуя его некоторыми перестановками порождающего множества из k элементов.

1. ФОРМУЛИРОВКА И ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 1

Формулировке и доказательству теоремы 1 предпошлем необходимые определения и обозначения.

В этом разделе символы V, M, q, k, β_i, β_i' обозначают объекты, введенные в определение 1, связанные с магмой $\mathfrak{S} = \mathfrak{S}(k,q) = (V,*)$. Чтобы однозначно задать индивидуальную магму $\mathfrak{S}$, нужно задать множество-носитель V (равносильно определению натурального числа $k \geqslant 1$) и операцию $(*)$, которая при заданном k определяется выбором кортежа перестановок $q \in S_k^{2k}$ и равенствами (1).

Обозначения, необходимые для формулировки теоремы 1. Для каждого непустого множества $M' = \{a_{s_1}, ..., a_{s_m}\} \subseteq M$ введем множество перестановок $P(M') \subset S_k$, состоящее из единичной перестановки I и всевозможных произведений перестановок $\beta_{s_1}, ..., \beta_{s_m}, \beta'_{s_1}, ..., \beta'_{s_m}$. Если M' — пустое множество, то полагаем, что $P(M')$ содержит только единичную перестановку.

Перестановки β_i, β_i' являются компонентами кортежа q из определения 1 магмы $\mathfrak{S}(k,q)$. Для каждой фиксированной магмы $\mathfrak{S}(k,q)$ и множества M' единственным образом определяется множество $P(M')$.

Таким образом, $(P(M'),\cdot)$ — моноид, порожденный множеством $\{I, \beta_{s_1}, ..., \beta_{s_m}, \beta'_{s_1}, ..., \beta'_{s_m}\}$ в смысле порождаемости в моноиде; $(\cdot)$ — композиция двух перестановок.

Пусть X и Y — два подмножества множества-носителя V и, как обычно, определены множества $X * Y := \{x * y \mid x \in X,\ y \in Y\}$, $X^2 := X * X$, $\varnothing * X := \varnothing$, $X * \varnothing := \varnothing$.

Замечание 1. Непосредственно из определения операции $(*)$ следует, что выражения вида a^n $(a \in M)$ в общем случае не определены однозначно, когда $n > 2$.

В самом деле, значение произведения a^n зависит от расстановки скобок. Поэтому мы не определяем множество X^n, когда $n > 2$. В произведениях, состоящих из более чем двух множеств, явно расставляем скобки. Таким образом, множество $(X^2) * (X^2)$ определенно корректно, а запись X^4 в данной работе не имеет смысла. Введение произведения множества на пустое множество целесообразно в данной работе для единообразной записи выкладок, которые используются при доказательстве теоремы 1.

Пусть Q — произвольное не пустое подмножество в V такое, что $Q = Q_1 \cup Q_2$ для подходящего $Q_1 \subseteq M$ и $Q_2 \subseteq M * M$. Тогда задаем обозначения

$$D(Q) := \left\{ b_{\gamma_1(u),\gamma_2(v)} \mid b_{u,v} \in (Q^2) * (Q^2),\ \gamma_1, \gamma_2 \in P(Q_1) \right\} \cup Q_1,\ \mathfrak{D}(Q) =: (D(Q), *). \quad (2)$$

Теорема 1. *Пусть задана магма $\mathfrak{S}(k, q) = (V, *)$ и Q — некоторое не пустое подмножество множества-носителя V. Тогда магма $\mathfrak{D}(Q)$ является подсистемой магмы $\mathfrak{S}(k, q)$, а множество Q — порождающим множеством подсистемы $\mathfrak{D}(Q)$.*

Доказательство. Символом $X(Q)$ обозначим подмножество в V такое, что $(X(Q), *)$ — подсистема магмы $\mathfrak{S}(k, q)$, порожденная множеством Q.

Полагаем, что $Q = Q_1 \cup Q_2$ для подходящих подмножеств $Q_1 \subseteq M$ и $Q_2 \subseteq M * M$.

Для удобства введем следующие обозначения:

$$R := (Q^2) * (Q^2), \quad (3)$$

$$F := \left\{ b_{\gamma_1(u),\gamma_2(v)} \mid b_{u,v} \in R,\ \ \gamma_1, \gamma_2 \in P(Q_1) \right\}. \quad (4)$$

1. Покажем замкнутость множества $D(Q)$. Множество F обладает подмножеством R. Действительно, это вытекает из наличия тождественной перестановки в $P(Q_1)$.

Справедливы равенства и включения

$$\begin{gathered} Q^2 = (Q_1 \cup Q_2) * (Q_1 \cup Q_2) = (Q_1 * Q_1) \cup (Q_2 * Q_2) \cup (Q_1 * Q_2) \cup (Q_2 * Q_1), \\ Q^2 \subseteq R \subseteq F \subseteq M * M. \end{gathered} \quad (5)$$

Прямые вычисления показывают, что R — замкнуто относительно операции $(*)$.

Пусть $b_{\gamma_1(u),\gamma_2(v)}, b_{\gamma_1'(u'),\gamma_2'(v')} \in F$ и $\gamma_1, \gamma_2, \gamma_1', \gamma_2' \in P(Q_1)$. Тогда элементы

$$b_{\gamma_1(u),\gamma_2(v)} * b_{\gamma_1'(u'),\gamma_2'(v')} = b_{\gamma_1(u),\gamma_2'(v')}, \quad b_{\gamma_1'(u'),\gamma_2'(v')} * b_{\gamma_1(u),\gamma_2(v)} = b_{\gamma_1'(u'),\gamma_2(v)}$$

лежат в $D(Q)$, поскольку γ_1, γ_2, γ_1', $\gamma_2' \in P(Q_1)$ и $b_{u,v'}, b_{u',v} \in R$.

Мы показали, что множество F замкнуто относительно операции $(*)$.

Далее, пусть $b_{\gamma_1(u),\gamma_2(v)} \in F$, $a_{s_i} \in Q_1$, где $\gamma_1, \gamma_2 \in P(Q_1)$. Проводим вычисления:

$$a_{s_i} * b_{\gamma_1(u),\gamma_2(v)} = b_{\beta_{s_i}\cdot\gamma_1(u),\beta_{s_i}\cdot\gamma_2(v)}, \quad b_{\gamma_1(u),\gamma_2(v)} * a_{s_i} = b_{\beta'_{s_i}\cdot\gamma_1(u),\beta'_{s_i}\cdot\gamma_2(v)}.$$

Справедливы включения $\beta_{s_i} \cdot \gamma_1$, $\beta_{s_i} \cdot \gamma_2$, $\beta'_{s_i} \cdot \gamma_1$, $\beta'_{s_i} \cdot \gamma_2 \in P(Q_1)$, следовательно, $b_{\beta_{s_i}\cdot\gamma_1(u),\beta_{s_i}\cdot\gamma_2(v)}$, $b_{\beta'_{s_i}\cdot\gamma_1(u),\beta'_{s_i}\cdot\gamma_2(v)} \in D(Q)$.

Пусть $a_i, a_j \in Q_1$. Тогда $a_i * a_j \in Q_1 * Q_1 \subset Q^2 \subset R \subset D(Q)$ (см. (5)). Таким образом, множество $D(Q)$ замкнуто относительно операции $(*)$.

2. Покажем, что справедливо включение $D(Q) \subseteq X(Q)$. Для этого покажем, что каждый элемент из $D(Q)$ является произведением некоторых элементов из Q либо

лежит в Q. Очевидно, что элементы из R (см. определение) являются некоторыми произведениями элементов из Q либо элементами Q.

Всякий элемент $b_{\gamma_1(u),\gamma_2(v)}$ ($b_{uv} \in R$, $\gamma_1, \gamma_2 \in P(Q_1)$) множества F является произведением элементов $b_{\gamma_1(u),\gamma_1(v)}$ и $b_{\gamma_2(u),\gamma_2(v)}$. Элементы $b_{\gamma_1(u),\gamma_1(v)}$ и $b_{\gamma_2(u),\gamma_2(v)}$ являются некоторыми произведениями элементов из множества R и множества Q_1 либо элементами из R. Таким образом, каждый элемент из F является произведением элементов из Q либо элементом из Q.

Мы показали, что всякий элемент из $D(Q)$ является некоторым произведением элементов из Q либо лежит в Q. Включение $D(Q) \subseteq X(Q)$ доказано.

3. Покажем, что $X(Q) \subseteq D(Q)$. Поскольку $\mathfrak{D}(Q) = (D(Q), *)$ — подсистема магмы $\mathfrak{S}(k, q)$, то множество $D(Q)$ замкнуто относительно операции $(*)$. Поэтому для доказательства включения $X(Q) \subseteq D(Q)$ достаточно показать, что $Q \subseteq D(Q)$.

Из (2) следует включение $Q_1 \subseteq D(Q)$. Из (5) следует цепочка включений

$$Q_2 * Q_2 \subseteq Q^2 \subseteq F \subseteq D(Q).$$

Прямая проверка показывает, что всякий элемент $b_{ij} \in M * M$ является идемпотентом, следовательно, $Q_2 \subseteq Q_2 * Q_2$. Таким образом, $Q_2 \subseteq D(Q)$. Поскольку $Q = Q_1 \cup Q_2$, то $Q \in D(Q)$. Поэтому $X(Q) \subseteq D(Q)$.

Значит, справедливо равенство $X(Q) = D(Q)$. Теорема доказана. □

Элемент x некоторой магмы $(X, \cdot)$ называют идемпотентом, если выполняется равенство $x \cdot x = x$. Полугруппу называют *идемпотентной полугруппой*, если каждый ее элемент является идемпотентом.

Сформулируем некоторые важные замечания к теореме 1, которые устанавливают связь между подсистемами магмы $\mathfrak{S}(k, q)$ и некоторыми хорошо известными классами полугрупп.

Замечание 2. Предположим, что Q — произвольное не пустое подмножество множества $M * M$. Тогда несложно показать, что для любой магмы $\mathfrak{S}(k, q)$ выполняется равенство $D(Q) = Q^2$ и $\mathfrak{D}(Q)$ является идемпотентной полугруппой и сепаративной полугруппой (значит, и Клифордовой полугруппой).

Замечание 3. Если $Q \subseteq V$ содержит элементы из M, то в общем случае подсистема $\mathfrak{D}(Q)$ не является полугруппой.

Замечание 4. Пусть в множестве M содержится элемент a_i такой, что перестановки β_i и β_i' являются тождественными. Полагаем, что $Q = \{a_i\} \cup Q_2$, где Q_2 — произвольное подмножество в $M * M$. Тогда непосредственная проверка показывает, что подсистема $\mathfrak{D}(Q)$ является полугруппой. Все элементы полугруппы $\mathfrak{D}(Q)$, кроме a_i, являются идемпотентами.

2. ФОРМУЛИРОВКА И ДОКАЗАТЕЛЬСТВО ТЕОРЕМЫ 2

Как обычно, через $|X|$ обозначаем мощность множества X. В данном разделе символы M и V будут введены в теореме 2.

Теорема 2. *Пусть $\mathfrak{A} = (V, *)$ — магма с конечным множеством-носителем V и множеством $M \subseteq V$ таким, что справедливы условия*

$$\begin{gathered} V = M \cup (M * M), \quad |M * M| = |M| \cdot |M|, \quad M \cap (M * M) = \varnothing, \\ V * (M * M) \subseteq M * M, \quad (M * M) * V \subseteq M * M. \end{gathered} \tag{6}$$

Тогда справедливы следующие утверждения:

1) для элементов из V можно ввести обозначения $M = \{a_1, ..., a_{|M|}\}$, $M * M = \{b_{ij} \mid i, j = 1, ..., |M|\}$ такие, что элементы из M и $M * M$ связаны равенствами $b_{ij} = a_i * a_j$, $i, j = 1, ..., |M|$;

2) в группе $S_{|M|}$ существует подгруппа $X(\mathfrak{A})$ такая, что для любой перестановки $\alpha \in X(\mathfrak{A})$ отображение

$$\phi_\alpha : \ a_i \to a_{\alpha(i)}, \quad i = 1, ..., |M|; \quad b_{uv} \to b_{\alpha(u),\alpha(v)} \quad u, v = 1, ..., |M| \tag{7}$$

есть автоморфизм магмы $\mathfrak{A}$ и справедливы утверждения

$$Aut\,(\mathfrak{A}) = \{\phi_\alpha |\ \alpha \in X(\mathfrak{A})\}, \quad Aut\,(\mathfrak{A}) \cong X(\mathfrak{A});$$

3) всякая конечная группа G будет изоморфна некоторой подгруппе H группы автоморфизмов $Aut\,(\mathfrak{A})$ для подходящей магмы $\mathfrak{A}$, удовлетворяющей условиям данной теоремы.

Доказательство. Пусть $\mathfrak{A} = (V, *)$ — магма, M — порождающее множество этой магмы, удовлетворяющее условиям данной теоремы.

1. Первый пункт теоремы следует непосредственно из условий (6).

2. Покажем, что для всякого автоморфизма $\phi \in Aut\,(\mathfrak{A})$ выполняются включения

$$M^\phi \subseteq M, \quad (M * M)^\phi \subseteq M * M. \tag{8}$$

В силу (6) получаем включение $(M * M)^\phi = M^\phi * M^\phi \subseteq M * M$, которое приводит к условиям

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

Отсюда получаем, что

$$|V^\phi| \leqslant |M^\phi \cup (M * M)| = |M^\phi| + |M|^2 - |M^\phi \cap (M * M)|.$$

Поскольку $M^\phi \cup (M * M) \subseteq V$ и справедливы равенства $|V^\phi| = |V| = |M| + |M|^2$, $|M^\phi| = |M|$, то справедливы условия

$$|M| + |M|^2 \leqslant |M| + |M|^2 - |M^\phi \cap (M * M)| \leqslant |V| = |M| + |M|^2.$$

Значит, $|M| + |M|^2 - |M^\phi \cap (M * M)| = |M| + |M|^2$, следовательно, $|M^\phi \cap (M * M)| = 0$ и $M^\phi \subseteq M$.

Таким образом, мы доказали включения (8).

Поскольку справедливы включения (8) и $V = M \cup (M * M)$, $M \cap (M * M) = \varnothing$, то имеет место равенство $M^\phi = M$. Действительно, в противном случае будет нарушена обратимость.

Множество M конечно и $M^\phi = M$, следовательно, ϕ задает перестановку множества M. Обозначим эту перестановку символом $\alpha \in S_{|M|}$. Эту перестановку можно рассматривать как перестановку на конечном множестве индексов $\{1, ..., |M|\}$. Подробней, $(a_i)^\phi = a_{\alpha(i)}$.

Пусть a_i, a_j — два произвольных элемента из M. Тогда

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

Таким образом, мы показали, что для всякого автоморфизма ϕ $(\phi = \phi_\alpha)$ существует перестановка $\alpha \in S_{|M|}$ такая, что автоморфизм ϕ действует по правилу

$$\phi_\alpha : \ a_i \to a_{\alpha(i)}, \quad i = 1, ..., |M|; \quad b_{uv} \to b_{\alpha(u),\alpha(v)} \quad u, v = 1, ..., |M|. \tag{9}$$

Множество всевозможных перестановок α, задающих автоморфизмы по правилу (9), обозначим символом $X(\mathfrak{A})$. Очевидно имеем равенство $Aut\,(\mathfrak{A}) = \{\phi_\alpha | \ \alpha \in X(\mathfrak{A})\}$. Отображение $\zeta(\alpha) : X(\mathfrak{A}) \to Aut\,(\mathfrak{A})$, действующее по правилу $\zeta(\alpha) = \phi_\alpha$ $(\alpha \in X(\mathfrak{A}),\ \phi_\alpha \in Aut\,(\mathfrak{A}))$, реализует изоморфизм $Aut\,(\mathfrak{A}) \cong X(\mathfrak{A})$. Пункт 2 доказан.

3. Можно показать, что магмы $\mathfrak{S}(k, q)$ удовлетворяют условиям теоремы 1. Для магмы $\mathfrak{S}$ приводилось описание группы автоморфизмов (см. [2, теорема 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. [2, теорема 1]). Последний изоморфизм вместе с известной теоремой Кэлли показывают, что любую конечную группу G можно представить подгруппой автоморфизмов подходящей магмы $\mathfrak{S}(k, q)$. Теорема доказана. □

Замечание 5. Приведенная ранее теорема 2 не дает исчерпывающей информации о группе автоморфизмов $Aut\,(\mathfrak{A})$. В частности, теорема 2 не дает структурного или поэлементного описания подгруппы перестановок $X(\mathfrak{A})$ (значит, и $Aut\,(\mathfrak{A})$). При этом она устанавливает однозначное соответствие между произвольным автоморфизмом из $Aut\,(\mathfrak{A})$ и перестановкой порождающего множества M.

Замечание 6. Отметим, что хорошо известно и интуитивно понятно, что автоморфизм характеризуется действием на порождающем множестве. Теорема 2 дает более сильное утверждение о характеризации автоморфизма магмы $\mathfrak{A}$ перестановкой порождающего множества M. Из общего вида автоморфизма (7) видно, что элементы порождающего множества переходят в элементы порождающего множества.

Замечание 7. Для практического вычисления группы автоморфизмов прямым перебором теорема 2 означает, что можно проверить сохранение умножения для $|M|!$ явно указанных отображений (7). Без знания общего вида автоморфизма (7) такой метод предполагал бы проведение этой проверки для $(|M| + |M|^2)!$ перестановок множества V.

Благодарности. Работа выполнена при поддержке Красноярского математического центра, финансируемого Минобрнауки РФ в рамках мероприятий по созданию и развитию региональных НОМЦ (Соглашение 075-02-2020-1534/1).

Библиографический список

1. *Bourbaki N.* Elements de Mathematique Algebre Chapitres 1 a 3. Springer Science Business Media, 2007. 636 p.
2. *Литаврин А. В.* Автоморфизмы некоторых магм порядка $k + k^2$ // Изв. Иркут. гос. ун-та. Сер. Математика. 2018. Т. 26. С. 47–61. DOI: https://doi.org/10.26516/1997-7670.2018.26.47
3. *Мальцев А. И.* Об умножении классов алгебраических систем // Сиб. матем. журн. 1967. Т. 8, № 2. С. 346–365.
4. *Князев О. В.* О группоиде многообразий вполне простых полугрупп // Изв. вузов. Матем. 1988. № 10. С. 5–11.
5. *Мартынова Т. А.* О произведении многообразий полугрупп // Изв. вузов. Матем. 1988. № 1. С. 36–41.
6. *Мартынов Л. М.* Об умножении многообразий алгебр // Изв. вузов. Матем. 1994. № 11. С. 53–58.

7. *Jones P. R.* Mal'cev products of varieties of completely regular semigroups // J. Austral. Math. Soc. 1987. Vol. 42, iss. 2. P. 227–246. DOI: https://doi.org/10.1017/S1446788700028226
8. *Day A.* Idempotents in the groupoid of all SP classes of lattices // Canad. Math. Bull. 1978. Vol. 21, iss. 4. P. 499–501. DOI: https://doi.org/10.4153/CMB-1978-085-2
9. *Grätzer G., Kelly D.* Products of lattice varieties // Algebra Universalis. 1985. Vol. 21, iss. 1. P. 33–45. DOI: https://doi.org/10.1007/BF01187554
10. *Novikov B. V.* On decomposition of Moufang groupoids // Quasigroups Related Systems. 2008. Vol. 16, № 1. P. 97–101.
11. *Белявская Г. Б., Табаров А. Х.* Группоиды с тождеством, определяющим коммутативные лупы Муфанг // Фундамент. и прикл. матем. 2008. Т. 14, вып. 6. С. 33–39.
12. *Щербаков В. А., Табаров А. Х., Пушкашу Д. И.* О конгруэнциях группоидов, тесно связанных с квазигруппами // Фундамент. и прикл. матем. 2008. Т. 14, вып. 5. С. 237–251.
13. *Степанова А. А., Трикашная Н. В.* Абелевы и гамильтоновы группоиды // Фундамент. и прикл. матем. 2009. Т. 15, вып. 7. С. 165–177.
14. *Глускин Л. М.* Позиционные оперативы // Матем. сб. 1965. Т. 68 (110), вып. 3. С. 444–472.
15. *Давидов С. С.* О структуре медиальных делимых n-арных группоидов // Матем. заметки. 2018. Т. 104, № 1. С. 33–44. DOI: https://doi.org/10.4213/mzm11372
16. *Давидов С. С.* Свободные коммутативные медиальные n-арные группоиды // Дискрет. матем. 2015. Т. 27, вып. 1. С. 34–43. DOI: https://doi.org/10.4213/dm1313
17. *Давидов С. С.* О разрешимости эквациональной теории коммутативных медиальных n-арных группоидов // Дискрет. матем. 2013. Т. 25, вып. 1. С. 121–136. DOI: https://doi.org/10.4213/dm1225
18. *Гальмак А. М.* О не n-полуабелевости полиадических группоидов специального вида // ПФМТ. 2019. Т. 38, № 1. С. 31–39.
19. *Гальмак А. М.* Перестановочность элементов в полиадических группоидах специального вида // ПФМТ. 2018. Т. 36, № 3. С. 70–75.
20. *Назаров М. Н.* Собственная метрика на группоидах и ее приложение к анализу межклеточных взаимодействий в биологии // Фундамент. и прикл. матем. 2013. Т. 18, № 3. С. 149–160.
21. *Катышев С. Ю., Марков В. Т., Нечаев А. А.* Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей // Дискрет. матем. 2014. Т. 26, вып. 3. С. 45–64. DOI: https://doi.org/10.4213/dm1289
22. *Барышников А. В., Катышев С. Ю.* Использование неассоциативных структур для построения алгоритмов открытого распределения ключей // Матем. вопр. криптогр. 2018. Т. 9, вып. 4. С. 5–30. DOI: https://doi.org/10.4213/mvk267
23. *Марков В. Т., Михалёв А. В., Нечаев А. А.* Неассоциативные алгебраические структуры в криптографии и кодировании // Фундамент. и прикл. матем. 2016. Т. 21, вып. 4. С. 99–124.
24. *Бредихин Д. А.* О многообразиях группоидов отношений с диофантовыми операциями // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2013. Т. 13, вып. 4, ч. 2. С. 28–34. DOI: https://doi.org/10.18500/1816-9791-2013-13-4-28-34
25. *Бредихин Д. А.* Тождества группоидов отношений с операцией оцилиндрованного пересечения // Изв. вузов. Матем. 2018. № 8. С. 12–20.
26. *Бредихин Д. А.* О базисах тождеств многообразий группоидов отношений // Чебышевский сб. 2018. Т. 19, № 1. С. 26–34. DOI: https://doi.org/10.22405/2226-8383-2018-19-1-26-34

27. *Глускин Л. М.* Автоморфизмы полугрупп бинарных отношений // Матем. зап. Урал. гос. ун-та. 1967. Т. 6. С. 44–54.
28. *Глускин Л. М.* Автоморфизмы мультипликативных полугрупп матричных алгебр // УМН. 1956. Т. 11, вып. 1 (67). С. 199–206.
29. *Халезов Е. А.* Автоморфизмы матричных полугрупп // Докл. АН СССР. 1954. Т. 96, № 2. С. 245 –248.
30. *Бунина Е. И., Семенов П. П.* Автоморфизмы полугруппы обратимых матриц с неотрицательными элементами над коммутативными частично упорядоченными кольцами // Фундамент. и прикл. матем. 2008. Т. 14, вып. 2. С. 69–100.
31. *Халезов Е. А.* Автоморфизмы примитивных квазигрупп // Матем. сб. 1961. Т. 53 (95), № 3. С. 329–342.
32. *Шматков В. Д.* Изоморфизмы и автоморфизмы алгебр матриц над решетками // Фундамент. и прикл. матем. 2014. Т. 19, вып. 1. С. 195–204.
33. *Ильиных А. П.* Классификация конечных группоидов с 2-транзитивной группой автоморфизмов // Матем. сб. 1994. Т. 185, № 6. С. 51–78.
34. *Ильиных А. П.* Группоиды порядка $q(q \pm 1)/2, q = 2r$, имеющие группу автоморфизмов, изоморфную $SL(2, q)$ // Сиб. матем. журн. 1995. Т. 36, № 6. С. 1336–1341.
35. *Литаврин А. В.* Автоморфизмы некоторых конечных магм с порядком строго меньше числа $N(N+1)$ и порождающим множеством из N элементов // Вестн. ТвГУ. Сер. Прикладная математика. 2019. Вып. 2. С. 70–87. DOI: https://doi.org/10.26456/vtpmk533
36. *Мальцев А. И.* Алгебраические системы. М. : Наука, 1970. 392 с.

Образец для цитирования:
Литаврин А. В. Подсистемы и автоморфизмы некоторых конечных магм порядка $k + k^2$ // Изв. Сарат. ун-та. Нов. сер. Сер. Математика. Механика. Информатика. 2020. Т. 20, вып. 4. С. 457–467. DOI: https://doi.org/10.18500/1816-9791-2020-20-4-457-467

Subsystems and Automorphisms of Some Finite Magmas of Order $k + k^2$

A. V. Litavrin

Litavrin Andrey Viktorovich, https://orcid.org/0000-0001-6285-0201, Siberian Federal University, 79 Svobodny Ave., Krasnoyarsk 660041, Russia, anm11@rambler.ru

This work is devoted to the study of subsystems of some finite magmas $\mathfrak{S} = (V, *)$ with a generating set of k elements and order $k + k^2$. For $k > 1$, the magmas $\mathfrak{S}$ are not semigroups and quasigroups. An element-by-element description of all magmas $\mathfrak{S}$ subsystems is given. It was found that all the magmas $\mathfrak{S}$ have subsystems that are semigroups. For $k > 1$, subsystems that are idempotent nonunit semigroups are explicitly indicated. Previously, a description of an automorphism group was obtained for magmas $\mathfrak{S}$. In particular, every symmetric permutation group S_k is isomorphic to the group of all automorphisms of a suitable magma $\mathfrak{S}$. In this paper, a general form of automorphism for a wider class of finite magmas of order $k + k^2$ is obtained.

Keywords: magma, groupoid, subsystems of magmas, automorphisms of groupoids, automorphisms of magmas, subgroupoids.

Received: 01.09.2019 / Accepted: 30.09.2019 / Published: 30.11.2020

Acknowledgements: This work is supported by the Krasnoyarsk Mathematical Center, which is financed by the Ministry of Science and Higher Education of the Russian Federation within the framework of the project for the establishment and development of regional centers for mathematical research and education (agreement No. 075-02-2020-1534/1).

References

1. Bourbaki N. *Elements de Mathematique Algebre Chapitres 1 a 3*. Springer Science Business Media, 2007. 636 p.
2. Litavrin A. V. Automorphisms of some magmas of order $k + k^2$. *The Bulletin of the Irkutsk State University. Ser. Mathematics*, 2018, vol. 26, pp. 47–61 (in Russian). DOI: https://doi.org/10.26516/1997-7670.2018.26.47
3. Maltsev A. I. On the multiplication of classes of algebraic systems. *Sib. Mat. Jour.* [Siberian Mathematical Journal], 1967, vol. 8, no. 2, pp. 346–365 (in Russian).
4. Knyazev O. V. On the groupoid of varieties of completely simple semigroups. *Soviet Math. (Iz. VUZ)*, 1988, vol. 32, no. 10, pp. 1–12.
5. Martynova T. A. On the product of semigroup varieties. *Soviet Math. (Iz. VUZ)*, 1988, vol. 32, no. 1, pp. 43–50.
6. Martynov L. M. On the multiplication of varieties of algebras. *Russian Math. (Iz. VUZ)*, 1994, vol. 38, no. 11, pp. 50–55.
7. Jones P. R. Mal'cev products of varieties of completely regular semigroups. *J. Austral. Math. Soc.*, 1987, vol. 42, iss. 2, pp. 227–246. DOI: https://doi.org/10.1017/S1446788700028226
8. Day A. Idempotents in the groupoid of all SP classes of lattices. *Canad. Math. Bull.*, 1978, vol. 21, iss. 4, pp. 499–501. DOI: https://doi.org/10.4153/CMB-1978-085-2
9. Grätzer G., Kelly D. Products of lattice varieties. *Algebra Universalis*, 1985, vol. 21, iss. 1, pp. 33–45. DOI: https://doi.org/10.1007/BF01187554
10. Novikov B. V. On decomposition of Moufang groupoids. *Quasigroups Related Systems*, 2008, vol. 16. no. 1, pp. 97–101.
11. Belyavskaya G. B., Tabarov A. Kh. Groupoids with the identity defining the commutative Moufang loops. *J. Math. Sci.*, 2010, vol. 164, iss. 1, pp. 21–25. DOI: https://doi.org/10.1007/s10958-009-9733-3
12. Shcherbakov V. A., Tabarov A. Kh., Puskash D. I. On congruences of groupoids closely connected with quasigroups. *J. Math. Sci.*, 2009, vol. 163, iss. 6, pp. 785–795. DOI: https://doi.org/10.1007/s10958-009-9716-4
13. Stepanova A. A., Trikashnaya N. V. Abelian and Hamiltonian groupoids. *J. Math. Sci.*, 2010, vol. 169, iss. 5, pp. 671–679. DOI: https://doi.org/10.1007/s10958-010-0068-x
14. Gluskin L. M. Positional operatives. *Mat. sb.* [Sbornik: Mathematics], 1965, vol. 68 (110), iss. 3, pp. 444–472 (in Russian).
15. Davidov S. S. On the Structure of Medial Divisible n-Ary Groupoids. *Math. Notes*, 2018, vol. 104, no. 1, pp. 29–38. DOI: https://doi.org/10.1134/S0001434618070040
16. Davidov S. S. Free commutative medial n-ary groupoids. *Discrete Math. Appl.*, 2015, vol. 25, iss. 4, pp. 203–210. DOI: https://doi.org/10.1515/dma-2015-0020
17. Davidov S. S. On the solvability of the equational theory of commutative medial n-ary groupoids. *Discrete Math. Appl.*, 2013, vol. 23, iss. 2, pp. 125–143. DOI: https://doi.org/10.1515/dma-2013-007
18. Gal'mak A. M. On non-n-semiabelianism polyadic groupoids of special class. *PFMT* [Problems of Physics, Mathematics and Technology], 2019, vol. 38, no. 1, pp. 31–39 (in Russian).
19. Gal'mak A. M. Permutability of elements in polyadic groupoids of special form. *PFMT* [Problems of Physics, Mathematics and Technology], 2018, vol. 36, no. 3, pp. 70–75 (in Russian).
20. Nazarov M. N. A Self-Induced Metric on Groupoids and its Application to the Analysis of

Cellular Interactions in Biology. *J. Math. Sci.*, 2015, vol. 206, iss. 5, pp. 561–569. DOI: https://doi.org/10.1007/s10958-015-2333-5

21. Katyshev S. Yu., Markov V. T., Nechaev A. A. Application of non-associative groupoids to the realization of an open key distribution procedure. *Discrete Math. Appl.*, 2015, vol. 25, iss. 1, pp. 9–24. DOI: https://doi.org/10.1515/dma-2015-0002
22. Baryshnikov A. V., Katyshev S. Yu. Application of non-associative structures to the construction of public key distribution algorithms. *Matematicheskiye voprosy kriptografii* [Mathematical Aspects of Cryptography], 2018, vol. 9, iss. 4, pp. 5–30 (in Russian).
23. Markov V. T., Mikhalev A. V., Nechaev A. A. Nonassociative algebraic structures in cryptography and coding. *Fundam. Prikl. Mat.*, 2016, vol. 21, iss. 4, pp. 99–124 (in Russian).
24. Bredikhin D. A. On Elasses of Groupoids of Relations with Diophantine Operations. *Izv. Saratov Univ. (N. S.), Ser. Math. Mech. Inform.*, 2013, vol. 13, iss. 4, pt. 2, pp. 28–34 (in Russian). DOI: https://doi.org/10.18500/1816-9791-2013-13-4-28-34
25. Bredikhin D. A. Identities of Groupoids of Relations With Operation of Cylindered Intersection. *Russian Math. (Iz. VUZ)*, 2018, vol. 62, no. 8, pp. 9–16. DOI: https://doi.org/10.3103/S1066369X18080029
26. Bredikhin D. A. On bases of identities for varieties of groupoids of relations. *Chebyshevskii Sbornik*, 2018, vol. 19, no. 1, pp. 26–34 (in Russian). DOI: https://doi.org/10.22405/2226-8383-2018-19-1-26-34
27. Gluskin L. M. Automorphisms of semigroups of binary relations. *Matem. zap. Ural. gos. un-ta* [Mathematical notes of the Ural State University], 1967, vol. 6, pp. 44–54 (in Russian).
28. Gluskin L. M. Automorphisms of multiplicative semigroups of matrix algebras. *Uspekhi Mat. Nauk*, 1956, vol. 11, iss. 1 (67), pp. 199–206 (in Russian).
29. Halezov E. A. Automorphisms of matrix semigroups. *Doklady Akademii nauk SSSR* [Soviet Mathematics Doklady], 1954, vol. 96, no. 2, pp. 245–248 (in Russian).
30. Bunina E. I., Semenov P. P. Automorphisms of the semigroup of invertible matrices with nonnegative elements over commutative partially ordered rings. *Fundam. Prikl. Mat.*, 2008, vol. 14, iss. 4, pp. 75–85; *J. Math. Sci.*, 2009, vol. 162, iss. 5, pp. 633–655. DOI: https://doi./10.1007/s10958-009-9650-5
31. Khalezov E. A. Automorphisms of primitive quasigroups. *Mat. Sb.* [Sbornik: Mathematics], 1961, vol. 53 (95), no. 3, pp. 329–342 (in Russian).
32. Shmatkov V. D. Isomorphisms and Automorphisms of Matrix Algebras Over Lattices. *J. Math. Sci.*, 2015, vol. 211, iss. 3, pp. 434–440. DOI: https://doi.org/10.1007/s10958-015-2614-z
33. Il'inykh A. P. Classification of finite groupoids with 2-transitive automorphism groups. *Russian Acad. Sci. Sb. Math.*, 1995, vol. 82, no. 1, pp. 175–197.
34. Ilinykh A. P. Groupoids of order $q(q \pm 1)/2$, $q = 2r$ with automorphism group isomorphic to $SL(2, q)$. *Sib. Math. J.*, 1995, vol. 36, no. 6, pp. 1159–1163. DOI: https://doi.org/10.1007/BF02106838
35. 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. Ser. Prikl. Matem.* [Herald of Tver State University. Ser. Applied Mathematics], 2019, iss. 2, pp. 70–87 (in Russian). DOI: https://doi.org/10.26456/vtpmk533
36. Maltsev A. I. *Algebraicheskie sistemy* [Algebraic systems]. Moscow, Nauka, 1970. 392 p. (in Russian).

Cite this article as: Litavrin A. V. Subsystems and Automorphisms of Some Finite Magmas of Order $k + k^2$. *Izv. Saratov Univ. (N. S.), Ser. Math. Mech. Inform.*, 2020, vol. 20, iss. 4, pp. 457–467 (in Russian). DOI: https://doi.org/10.18500/1816-9791-2020-20-4-457-467