DOI 10.15507/2079-6900.24.202201.76-95
Оригинальная статья

ISSN 2079-6900 (Print)
ISSN 2587-7496 (Online)

УДК 512.548.2

Эндоморфизмы и антиэндоморфизмы некоторых конечных группоидов

А. В. Литаврин

ФГАОУ ВО «Сибирский федеральный университет» (г. Красноярск, Российская Федерация)

Аннотация. В настоящей работе изучаются антиэндоморфизмы некоторых конечных группоидов. Ранее были введены специальные группоиды $S(k, q)$ с порождающим множеством из k элементов и порядком $k(1 + k)$. Ранее исследовались вопросы поэлементного описания моноида всех эндоморфизмов данного группоида (в частности, автоморфизмов). Было показано, что всякий конечный моноид изоморфно вложим в моноид всех эндоморфизмов подходящего группоида $S(k, q)$. В данной статье приводится поэлементное описание множества всех антиэндоморфизмов группоида $S(k, q)$. Установлено, что в зависимости от группоида $S(k, q)$ множество всех его антиэндоморфизмов может быть замкнутым или не замкнутым относительно композиции отображений. Для поэлементного описания антиэндоморфизмов изучается действие произвольного антиэндоморфизма на порождающих элементах группоида. При данном подходе антиэндоморфизм попадает в один из трех классов. Антиэндоморфизмы из двух полученных классов будут являться эндоморфизмами данного группоида. Оставшийся класс антиэндоморфизмов в зависимости от конкретного группоида $S(k, q)$ может состоять или не состоять из эндоморфизмов. В данной работе исследуются эндоморфизмы некоторых конечных группоидов G с порядком, удовлетворяющим некоторому неравенству. Построены некоторые эндоморфизмы таких группоидов и показано, что всякий конечный моноид изоморфно вкладывается в моноид всех эндоморфизмов подходящего группоида G. Для доказательства данного результата существенно используется обобщение теоремы Кэли на случай моноидов (полугрупп с единицей).

Ключевые слова: эндоморфизм, антиэндоморфизм, автоморфизм, антиавтоморфизм, конечный группоид, моноид

Для цитирования: Литаврин А. В. Эндоморфизмы и антиэндоморфизмы некоторых конечных группоидов // Журнал Средневолжского математического общества. 2022. Т. 24, № 1. С. 76–95. DOI: https://doi.org/10.15507/2079-6900.24.202201.76-95

Об авторе:
Литаврин Андрей Викторович, доцент кафедры высшей математики № 2, ФГАОУ ВО «Сибирский федеральный университет» (660041, Россия, г. Красноярск, пр. Свободный, д. 82А), кандидат физико-математических наук, ORCID: https://orcid.org/ 0000-0001-6285-0201, anm11@rambler.ru

Original article

MSC2020 20N02

Endomorphisms and anti-endomorphisms of some finite groupoids

A. V. Litavrin

Siberian Federal University (Krasnoyarsk, Russian Federation)

Abstract. In this paper, we study anti-endomorphisms of some finite groupoids. Previously, special groupoids $S(k,q)$ of order $k(1+k)$ with a generating set of k elements were introduced. Previously, the element-by-element description of the monoid of all endomorphisms (in particular, automorphisms) of a given groupoid was studied. It was shown that every finite monoid is isomorphically embeddable in the monoid of all endomorphisms of a suitable groupoid $S(k,q)$. In recent article, we give an element-by-element description for the set of all anti-endomorphisms of the groupoid $S(k,q)$. We establish that, depending on the groupoid $S(k,q)$, the set of all its anti-endomorphisms may be closed or not closed under the composition of mappings. For an element-by-element description of anti-endomorphisms, we study the action of an arbitrary anti-endomorphism on generating elements of a groupoid. With this approach, the anti-endomorphism will fall into one of three classes. Anti-endomorphisms from the two classes obtained will be endomorphisms of given groupoid. The remaining class of anti-endomorphisms, depending on the particular groupoid $S(k,q)$, may either consist or not consist of endomorphisms. In this paper, we study endomorphisms of some finite groupoids G whose order satisfies some inequality. We construct some endomorphisms of such groupoids and show that every finite monoid is isomorphically embedded in the monoid of all endomorphisms of a suitable groupoid G. To prove this result, we essentially use a generalization of Cayley's theorem to the case of monoids (semigroups with identity).

Keywords: endomorphism, anti-endomorphism, automorphism, anti-automorphism, finite groupoid, monoid

For citation: *A. V. Litavrin.* Endomorphisms and anti-endomorphisms of some finite groupoids. *Zhurnal Srednevolzhskogo matematicheskogo obshchestva.* 24:1(2022), 76–95. DOI: https://doi.org/10.15507/2079-6900.24.202201.76-95

About the author:

Andrey V. Litavrin, Associate Professor of the Department of Higher Mathematics No. 2, Siberian Federal University(82A Svobodny Ave., Krasnoyarsk 660041, Russia), PhD (Physics and Mathematics), ORCID: https://orcid.org / 0000-0001-6285-0201, anm11@rambler.ru

1. Введение

Пусть A – некоторое множество и $(*)$ – бинарная алгебраическая операция, определенная на множестве A. Тогда пару $\mathfrak{A} = (A, *)$ называем группоидом (также распространен термин *магма*). Для каждого группоида определены *эндоморфизмы* и *автоморфизмы*. Множество всех эндоморфизмов группоида $\mathfrak{A}$ традиционно обозначают символом $\mathrm{End}(\mathfrak{A})$, а множество всех автоморфизмов – символом $\mathrm{Aut}(\mathfrak{A})$. Хорошо известно, что относительно композиции двух эндоморфизмов множество $\mathrm{End}(\mathfrak{A})$ образует моноид ($\mathrm{Aut}(\mathfrak{A})$, образует подгруппу в моноиде $\mathrm{End}(\mathfrak{A})$). При этом следует упомянуть,

что каждый эндоморфизм, например, моноида будет являться эндоморфизмом соответствующего группоида, обратное не всегда верно.

Данная работа посвящена изучению эндоморфизмов и антиэндоморфизмов некоторых конечных группоидов, которые в общем случае не являются полугруппой или квазигруппой. Основные результаты работы сформулированы в виде теоремы 1 и теоремы 2. Прежде чем перейти к формулировке и обсуждению основных результатов дадим необходимые определения и рассмотрим примеры работ, имеющих отношение к теме исследования.

Приведем определение антиэндоморфизма группоида.

О п р е д е л е н и е 1.1. *Пусть* $\mathfrak{A} = (A, *)$ *– некоторый группоид. Тогда антиэндоморфизмом группоида* $\mathfrak{A}$ *называем отображение* $\phi : A \to A$*, если для любых* $x, y \in A$ *выполняется равенство*

$$(x * y)^{\phi} = y^{\phi} * x^{\phi}. \tag{1.1}$$

Если антиэндоморфизм ϕ *является биекцией множества* A *на множество* A*, то* ϕ *называют антиавтоморфизмом группоида* $\mathfrak{A}$*.*

В данной работе множество всех антиэндоморфизмов группоида $\mathfrak{A}$ будем обозначать символом $\mathrm{Aend}(\mathfrak{A})$, а множество всех антиавтоморфизмов обозначим символом $\mathrm{Aaut}(\mathfrak{A})$. Данные обозначения получаются из сокращения английских терминов «Anti-automorphism» и «Anti-endomorphism», полученных стандартным образом (см., например, работы [1–3] и др.).

Эндоморфизмы различных группоидов часто становятся объектом исследований. Большое количество исследований посвящено случаем, когда группоид является квазигруппой или полугруппой. Активно изучаются эндоморфизмы полугрупп (например, см. [4–6] и др.) и квазигрупп (см. [7] и др.). В частности, в работе [4] получена классификация всех эндоморфизмов полугруппы $G_n(R)$ $(n \geq 3)$, состоящей из матриц с неотрицательными коэффициентами из линейно упорядоченного кольца R с обратимой двойкой. Близкие объекты изучаются в работе [5]. Ранее в [8] изучались автоморфизмы и антиавтоморфизмы полугруппы $G_n(R)$ $(n \geq 2)$, когда R – линейно упорядоченное тело. Каждый автоморфизм там был разложен в произведения трех или четырех сомножителей специального вида.

Отметим, что результаты исследований неассоциативных группоидов могут быть использованы в криптографии (см., например, [9]). Автоморфизмы и антиавтоморфизмы различных систем (в т. ч., группоидов) часто используются в криптографии, в частности как техническое средство для проведения выкладок и построения новых алгебраических систем (с нужными свойствами). Антиэндоморфизмы различных объектов также используются в приложениях, например, в работе [10].

В работе [11] исследовались автоморфизмы конечноопределенных квазигрупп и было установлено, что всякая конечная группа изоморфна группе всех автоморфизмов подходящей конечноопределенной квазигруппы. Последний результат по структуре схож с результатами Г. Биркгофа и Д. Гроота, которые представили произвольную группу группами всех автоморфизмов некоторой алгебры (Г. Биркгоф, [12]) и некоторого кольца (Д. Гроот, [13]).

В работе [14] были введены группоиды $\mathfrak{S}(k, q)$ порядка $k + k^2$ и порождающим множеством из k элементов. Там же изучались автоморфизмы этих группоидов. В частности, было установлено, что всякая конечная группа G будет изоморфна некоторой подгруппе группы всех автоморфизмов подходящего группоида $\mathfrak{S}(|G|, q)$.

Аналогичные результаты были получены в работе [15] для группоидов

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

порожденных n элементами и порядком $|V|$, удовлетворяющим неравенствам

$$n + 1 \leq |V| < n^2 + n.$$

В работе [16] исследовались эндоморфизмы группоидов $\mathfrak{S} = \mathfrak{S}(k, q)$. Было получено поэлементное описание множества $\mathrm{End}(\mathfrak{S})$, установлены некоторые структурные свойства моноида $\mathrm{End}(\mathfrak{S})$ и показано, что всякий конечный моноид может быть изоморфно вложен в моноид $\mathrm{End}(\mathfrak{S})$ для подходящего группоида $\mathfrak{S}$.

Основные задачи исследования. Таким образом, всякую конечную группу можно изоморфно вложить в группу всех автоморфизмов подходящих группоидов $\mathfrak{S}(k, q)$ и $\mathfrak{G}$, а произвольный конечный моноид изоморфно вложить в моноид всех эндоморфизмов группоида $\mathfrak{S}(k, q)$. В связи с этим и результатами работ [11–13] возникает интерес к следующей задаче.

Задача 1. *Выяснить, можно ли произвольный конечный моноид изоморфно вложить в моноид всех эндоморфизмов подходящего группоида* $\mathfrak{G}(k, 1, M_1)$*?*

Положительный ответ на вопрос из задачи 1 дает теорема 2.2 (см. следующий раздел). Данный результат представляет особый интерес, в частности, потому, что группоиды $\mathfrak{G}(k, 1, M_1)$ определяются явно (см. определение 3 в данной работе) и не зависят от контекста задачи 1. Следует отметить, что хорошо известно, что всякий моноид можно изоморфно вложить в моноид всех эндоморфизмов некоторой алгебраической системы. Однако вопросы изоморфного вложения произвольного моноида в моноид всех эндоморфизмов алгебраической системы из фиксированного класса алгебраических систем являются, в общем случае, нетривиальными. Нетривиальность связана с тем, что данные вопросы требуют в каждом конкретном случае рассматривать эндоморфизмы конкретных алгебраических систем.

Иногда вопросы о вложении бывают тривиальными. Так, вложение произвольного моноида в моноид всех эндоморфизмов некоторого подходящего группоида из класса всех группоидов не вызывает никаких проблем и является простым упражнением, которое можно встретить в учебной литературе.

В связи с результатами работ [14] и [16] возник интерес к вопросу о классификации всех антиэндоморфизмов группоида $\mathfrak{S}(k, q)$. В данной работе решается следующая

Задача 2. *Привести поэлементное описание множества* $\mathrm{Aend}(\mathfrak{S}(k, q))$.

Решение этой задачи изложено в виде теоремы 2.1 (см. следующий раздел).

Хорошо известно, что множество всех антиэндоморфизмов некоторого группоида не обязано быть замкнутым относительно операции композиции. Например, f^2 не обязано быть антиэндоморфизмом группы G, когда $f: \ x \to x^{-1}$ $(x \in G)$. Проведем рассуждения. Пусть $\mathfrak{A} = (G, *)$ – некоторый произвольный группоид. Справедлива цепочка равенств

$$(x * y)^{\phi_1 \cdot \phi_2} = (y^{\phi_2} * x^{\phi_2})^{\phi_1} = (x^{\phi_2})^{\phi_1} * (y^{\phi_2})^{\phi_1} = x^{\phi_1 \cdot \phi_2} * y^{\phi_1 \cdot \phi_2} \tag{1.2}$$

$$(x, y \in G, \ \phi_1, \phi_2 \in \mathrm{Aend}(\mathfrak{A})),$$

которая показывает, что произведение двух антиэндоморфизмов является эндоморфизмом.

При этом если для $\varphi \in \mathrm{Aend}(\mathfrak{A}) \cdot \mathrm{Aend}(\mathfrak{A})$ образ

$$G^{\varphi} := \{g^{\varphi} \mid g \in G\}$$

является коммутативным группоидом, то $\varphi \in \mathrm{Aend}(\mathfrak{A})$. Последнее утверждение тривиально следует из равенства (1.2).

Когда $\mathfrak{A} = \mathfrak{S}(k,q)$, множество $\mathrm{Aend}(\mathfrak{S}(k,q))$ может содержать подмножество X, такое что $X \subseteq \mathrm{End}(\mathfrak{S}(k,q))$ и X – замкнуто относительно композиции двух антиэндоморфизмов (см. Пример 3.1).

При этом группоид $\mathfrak{S}(k,q)$ можно выбрать так, что множество $\mathrm{Aend}(\mathfrak{S}(k,q))$ будет содержать антиэндоморфизм, который не является эндоморфизмом. Кроме того, в этом случае множество $\mathrm{Aend}(\mathfrak{S}(k,q))$ будет не замкнутым относительно композиции двух отображений (см. Пример 3.2).

Естественно, возникает вопрос, может ли множество $\mathrm{Aend}(\mathfrak{S}(k,q))$ быть замкнутым относительно композиции. Ответ положительный. Самый простой пример дает второй пункт теоремы 2.1. При $k = 1$ выполняется равенство

$$\mathrm{Aend}(\mathfrak{S}(1,q)) = \mathrm{End}(\mathfrak{S}(1,q)).$$

В данном случае $q = (I, I)$. Данный пример не единственный.

Для $k = 2$ можно построить кортеж q такой, что множество $\mathrm{Aend}(\mathfrak{S}(2,q))$ будет замкнутым относительно композиции и состоять из эндоморфизмов группоида $\mathfrak{S}(2,q)$ (см. Пример 3.3).

В примерах 3.2 и 3.3 используется теорема 2.1.

2. Определения и формулировка основных результатов

Приведем определения и обозначения, необходимые для формулировки теорем 2.1 и 2.2.

Обозначения, связанные с симметрической полугруппой. Симметрическую полугруппу всех отображений множества $\{1,...,n\}$ в себя будем обозначать символом $\mathcal{I}_n$. Как обычно, символом S_n обозначаем *симметрическую группу* перестановок множества из n элементов. Композицию двух отображений из $\mathcal{I}_n$ будем обозначать $(\circ)$. Если x – произвольный элемент из $\{1,...,n\}$ и α – произвольное отображение из $\mathcal{I}_n$, то $\alpha(x)$ – образ элемента x под действием отображения α. Если $\alpha, \beta \in \mathcal{I}_n$ и $x \in \{1,...,n\}$, то полагаем $(\alpha \circ \beta)(x) := \alpha(\beta(x))$.

Группоиды $\mathfrak{S}(k,q)$ и теорема 2.1. Приведем определение 1 группоида $\mathfrak{S}(k,q)$ из [14].

О п р е д е л е н и е 2.1. *Пусть определены следующие объекты:*

1) k – некоторое натуральное число;

2) попарно различные символы $a_1,...,a_k$ и b_{ij} $(i,j = 1,...,k)$;

3) множества

$$M := \{a_1,...,a_k\}, \quad V := M \cup \{b_{ij} \mid i,j \in \{1,...,k\}\},$$

$$S_k^m := \{(\varepsilon_1,...,\varepsilon_m) \mid \varepsilon_i \in S_k,\ i = 1,...,m\};$$

4) кортеж $q = (\beta_1,...,\beta_k,\beta_1',...,\beta_k') \in S_k^{2k}$;

5) бинарная алгебраическая операция $(*)$ на множестве V, такая что справедливы равенства:

$$a_i * a_j = b_{ij}, \quad a_s * b_{ij} = b_{\beta_s(i),\beta_s(j)}, \tag{2.1}$$
$$b_{ij} * a_s = b_{\beta'_s(i),\beta'_s(j)}, \quad b_{mv} * b_{ij} = b_{mj} \quad (m, v, s, i, j \in \{1, ..., k\}).$$

Тогда через

$$\mathfrak{S}(k, q) = (V, *)$$

обозначим группоид с множеством носителем V и бинарной алгебраической операцией $(*)$, которую задают равенства (2.1).

В работе [16] вводятся отображения ϕ_γ, $\zeta[b_{uv}]$, $\rho[a_s, M']$ и доказывается (см. Теорема 1 из [16]), что они (при некоторых ограничениях на свои параметры) являются эндоморфизмами группоида $\mathfrak{S}(k, q)$. Для удобства читателя определим эти отображения ниже.

Полагаем, что определен группоид $\mathfrak{S}(k, q)$, следовательно, задан кортеж

$$q = (\beta_1, ..., \beta_k, \beta'_1, ..., \beta'_k).$$

В множестве $\mathcal{I}_k$ выделим подмножество $A_e(q)$ преобразований γ таких, что для любых $s, i \in \{1, ..., k\}$ выполняются равенства

$$\beta_{\gamma(s)}(\gamma(i)) = \gamma(\beta_s(i)), \quad \beta'_{\gamma(s)}(\gamma(i)) = \gamma(\beta'_s(i)). \tag{2.2}$$

Для каждого $\gamma \in A_e(q)$ введем отображение

$$\phi_\gamma : a_i \to a_{\gamma(i)}, \quad (a_i \in M); \quad b_{ij} \to b_{\gamma(i),\gamma(j)} \quad (b_{ij} \in M * M). \tag{2.3}$$

Для всякого элемента b_{uv} из $M * M$ вводится отображение $\zeta[b_{uv}]$, переводящее все элементы множества–носителя V в элемент b_{uv}:

$$\zeta[b_{uv}] : \quad a_i \to b_{uv}, \quad (a_i \in M); \quad b_{ij} \to b_{uv}, \quad (b_{ij} \in M * M). \tag{2.4}$$

Пусть $a_s \in M$, такой что $\beta_s(s) = \beta'_s(s) = s$ и M' – произвольное не пустое подмножество M, отличное от M. Тогда введем отображение

$$\rho[a_s, M'] : \quad a_i \to a_s \quad (a_i \in M'), \quad a_r \to b_{ss} \ (r \in M \setminus M'); \tag{2.5}$$
$$b_{ij} \to b_{ss}, \ (b_{ij} \in M * M).$$

Доказано (см. леммы 1, 5 и 6 из [16]), что отображения ϕ_γ, $\zeta[b_{uv}]$ и $\rho[a_s, M']$ являются эндоморфизмами группоида $\mathfrak{S}(k, q)$ при указанных ограничениях на свои параметры γ, b_{uv}, a_s и M'. Отметим, что отображения $\rho[a_s, M']$ определены не для всех группоидов $\mathfrak{S}(k, q)$.

В множестве $\mathrm{End}(\mathfrak{S}(k, q))$ выделим подмножества:

1. $E_1(\mathfrak{S}(k, q))$, состоящее из всевозможных эндоморфизмов ϕ_γ;
2. $E_2(\mathfrak{S}(k, q))$, состоящее из всевозможных эндоморфизмов $\zeta[b_{uv}]$ и тождественного эндоморфизма;
3. $E_3(\mathfrak{S}(k, q))$, состоящее из всевозможных эндоморфизмов $\rho[a_s, M']$ (если они существуют) и тождественного эндоморфизма.

Обозначения, связанные с действием эндоморфизмов и антиэндоморфизмов. Полагаем, что $x \in V$ и $\phi \in \mathrm{End}(\mathfrak{S}(k,q))$ (или $\phi \in \mathrm{Aend}(\mathfrak{S}(k,q))$). Тогда x^{ϕ} – образ элемента x под действием эндоморфизма (или антиэндоморфизма) ϕ. Композицию двух эндоморфизмов (антиэндоморфизмов) будем обозначать символом $(\cdot)$. Если $\phi_1, \phi_2 \in \mathrm{End}(\mathfrak{S}(k,q))$ (аналогично, $\mathrm{Aend}(\mathfrak{S}(k,q))$) и $x \in V$, то $x^{\phi_1 \cdot \phi_2} := (x^{\phi_2})^{\phi_1}$.

В работе [16] было установлено (см. теорема 1) равенство

$$\mathrm{End}(\mathfrak{S}(k,q)) = E_1(\mathfrak{S}(k,q)) \cdot E_2(\mathfrak{S}(k,q)) \cdot E_3(\mathfrak{S}(k,q)). \tag{2.6}$$

Ниже определим множества $AE_1(\mathfrak{S}(k,q))$, $AE_2(\mathfrak{S}(k,q))$ и $AE_3(\mathfrak{S}(k,q))$, которые необходимы для описания множества $\mathrm{Aend}(\mathfrak{S}(k,q))$.

Символом $A_{aend}(q)$ обозначим множество отображений $\alpha \in \mathcal{I}_k$, таких что для любых $s, u \in \{1, ..., k\}$ выполняются равенства

$$\alpha(\beta_s(u)) = \beta'_{\alpha(s)}(\alpha(u)), \quad \alpha(\beta'_s(u)) = \beta_{\alpha(s)}(\alpha(u)). \tag{2.7}$$

Для каждого $\gamma \in A_{aend}$ введем отображение

$$\phi'_\gamma : a_i \to a_{\gamma(i)}, \quad (a_i \in M); \quad b_{ij} \to b_{\gamma(j),\gamma(i)} \quad (b_{ij} \in M * M). \tag{2.8}$$

Множество всевозможных отображений ϕ'_γ обозначим символом $AE_1(\mathfrak{S}(k,q))$.

Единичный эндоморфизм будем обозначать символом I. Вводим множества

$$AE_2(\mathfrak{S}(k,q)) := E_2(\mathfrak{S}(k,q)) \setminus \{I\}, \quad AE_3(\mathfrak{S}(k,q)) := E_3(\mathfrak{S}(k,q)) \setminus \{I\}.$$

В данной работе доказывается

Т е о р е м а 2.1. *Справедливы утверждения:*

1) для любого натурального $k > 1$ справедливо равенство

$$\mathrm{Aend}(\mathfrak{S}(k,q)) = AE_1(\mathfrak{S}(k,q)) \cup AE_2(\mathfrak{S}(k,q)) \cup AE_3(\mathfrak{S}(k,q));$$

2) для $k = 1$ справедливы равенства

$$\mathrm{Aend}(\mathfrak{S}(k,q)) = \mathrm{End}(\mathfrak{S}(k,q)) = \{I, \zeta[b_{11}]\};$$

3) справедливо включение $\mathrm{Aaut}(\mathfrak{S}(k,q)) \subset AE_1(\mathfrak{S}(k,q))$.

Доказательство этой теоремы приводится в разделе 2. Видно, что результат первого пункта из теоремы 2.1 напоминает равенство (2.6). При этом справедливы включения

$$AE_i(\mathfrak{S}(k,q)) \subset E_i(\mathfrak{S}(k,q)), \quad i = 2, 3.$$

В общем случае множества $AE_1(\mathfrak{S}(k,q))$ и $E_1(\mathfrak{S}(k,q))$ могут иметь непустое пересечение (например, при $k = 1$ их пересечение равно $\{I\}$, см. теорему 2.1), но отображения ϕ_γ и ϕ'_γ строятся различными способами (см. (2.3) и (2.8)), как и параметризирующие их множества отображений из $\mathcal{I}_k$ (см. (2.2) и (2.7)). Таким образом, это принципиально различные множества.

Группоиды $\mathfrak{G}$ и теорема 2.2. Далее сформулируем основные определения и результаты, касающиеся группоидов $\mathfrak{G}(k, m, M_1, ..., M_m)$ из работы [15].

О п р е д е л е н и е 2.2. *Полагаем, что определены следующие объекты:*

1) *k и m – натуральные числа, такие что k больше единицы и верно неравенство $2m \leq k^2$;*

2) *попарно различные элементы $a_1, ..., a_k, c_1, ..., c_m, b_{ij}$ $(i, j = 1, ..., k)$;*

3) *множества*

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

4) *кортеж $(M_1, M_2, ..., M_m)$, состоящий из m попарно непересекающихся подмножеств множества $M \times M$, мощности ≥ 2;*

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 $(*)$ такую, что справедливы равенства

$$a_i * a_j = c_q, \ \text{если} \ \ (a_i, a_j) \in M_q; \quad a_i * a_j = b_{ij}, \quad \text{если} \ \ (a_i, a_j) \in D; \tag{2.9}$$

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

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

Символами

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

обозначаем группоид с множеством носителем V и алгебраической операцией $(*)$, которую задают равенства (2.9).

З а м е ч а н и е 2.1. *Далее символы a_i, b_{uv}, M, V, k будут относиться к объекту $\mathfrak{G}$, введенному определением 3. Путаницы не возникнет. В самом деле, до конца этого раздела речь будет идти только о группоидах $\mathfrak{G}(k, m, M_1, ..., M_m)$, в разделе 3 речь идет только о группоидах $\mathfrak{G}(k, q)$, а в четвертом – только о группоидах $\mathfrak{G}(k, m, M_1, ..., M_m)$.*

В данной работе доказывается следующая ниже теорема.

Т е о р е м а 2.2. *Для любого конечного моноида G существует группоид $\mathfrak{G}(k, 1, M_1)$, такой что число $k > |G|$ и моноид G изоморфен некоторому подмоноиду моноида* $\mathrm{End}(\mathfrak{G}(k, 1, M_1))$.

Теорема 2.2 доказывается конструктивно. Для каждого конечного моноида строится подходящий группоид $\mathfrak{G}(k, 1, M_1)$. В работе строятся эндоморфизмы (в явном виде), которых достаточно для доказательства теоремы 2.2. Ниже приведем эти эндоморфизмы (см. (2.11)). Но вначале дадим необходимые определения.

Пусть X – некоторое подмножество множества $M \times M$. Тогда будем использовать следующее обозначение:

$$X^{\alpha} := \{(a_{\alpha(i)}, a_{\alpha(j)}) \mid (a_i, a_j) \in X\}.$$

О п р е д е л е н и е 2.3. *Полагаем, что задан группоид* $\mathfrak{G}(k, m, M_1, ..., M_m)$. *В множестве* $\mathcal{I}_k$ *выделим множество* $Ae(M_1, ..., M_m)$ *отображений* α, *таких что выполняется включение*

$$D^\alpha \subseteq D \tag{2.10}$$

и для каждого номера $q \in \{1, ..., m\}$ *существует номер* $d \in \{1, ..., m\}$, *такой что справедливо включение* $M_q^\alpha \subseteq M_d$.

Если $\alpha \in Ae(M_1, ..., M_m)$, *то на множестве* $\{1, ..., m\}$ *можно определить отображение* $l_\alpha : \{1, ..., m\} \to \{1, ..., m\}$, *такое что* $l_\alpha(i) = j$ *тогда и только тогда, когда* $M_i^\alpha \subseteq M_j$. *Отметим, что* l_α – *отображение из* $\mathcal{I}_m$.

Пусть α – отображение из $Ae(M_1, ..., M_m)$. Тогда отображение

$$\mu_\alpha : \ a_i \to a_{\alpha(i)} \quad (1 \le i \le k), \qquad b_{uv} \to b_{\alpha(u),\alpha(v)} \quad ((a_u, a_v) \in D), \tag{2.11}$$

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

является эндоморфизмом системы $\mathfrak{G}$ (доказывается в лемме 4.2).

3. Доказательство теоремы 2.1

Для доказательства теоремы 2.1 докажем

Л е м м а 3.1. *Всякое отображение* ϕ *из множества*

$$AE_1(\mathfrak{S}(k, q)) \cup AE_2(\mathfrak{S}(k, q)) \cup AE_3(\mathfrak{S}(k, q)) \tag{3.1}$$

является антиэндоморфизмом группоида $\mathfrak{S}(k, q)$.

Д о к а з а т е л ь с т в о. Далее будем показывать, что для любого ϕ из объединения (3.1) элементы $(x*y)^\phi$ и $y^\phi * x^\phi$ совпадают (т. е. показывать, что выполняется равенство (1.1)).

1. Пусть $\phi := \phi'_\alpha$ – некоторый произвольный антиэндоморфизм из $AE_1(\mathfrak{S}(k, q))$. Далее проводим вычисления

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

$$(b_{ij} * b_{uv})^\phi = (b_{iv})^\phi = b_{\alpha(v),\alpha(i)}, \quad b_{uv}^\phi * b_{ij}^\phi = b_{\alpha(v),\alpha(u)} * b_{\alpha(j),\alpha(i)} = b_{\alpha(v),\alpha(i)};$$

$$(a_i * b_{uv})^\phi = (b_{\beta_i(u),\beta_i(v)})^\phi = b_{\alpha(\beta_i(v)),\alpha(\beta_i(u))},$$

$$b_{uv}^\phi * a_i^\phi = b_{\alpha(v),\alpha(u)} * a_{\alpha(i)} = b_{\beta'_{\alpha(i)}(\alpha(v)),\beta'_{\alpha(i)}(\alpha(u))}$$

В силу (2.7) получаем равенства

$$\beta'_{\alpha(i)}(\alpha(v)) = \alpha(\beta_i(v)), \quad \beta'_{\alpha(i)}(\alpha(u)) = \alpha(\beta_i(u)),$$

следовательно, выполняется равенство

$$b_{\beta'_{\alpha(i)}(\alpha(v)),\beta'_{\alpha(i)}(\alpha(u))} = b_{\beta'_{\alpha(i)}(\alpha(v)),\beta'_{\alpha(i)}(\alpha(u))}.$$

Равенство

$$(b_{uv} * a_i)^\phi = a_i^\phi * b_{uv}^\phi$$

проверяется аналогично.

Таким образом, мы показали, что множество $AE_1(\mathfrak{S}(k,q))$ состоит из антиэндоморфизмов.

2. Пусть $\phi := \zeta[b_{uv}]$ – произвольный эндоморфизм из $AE_2(\mathfrak{S}(k,q))$. Этот эндоморфизм переводит любой элемент в элемент b_{uv}. Пусть x, y – два произвольных элемента из V. Тогда справедливы равенства:

$$(x * y)^\phi = b_{uv}, \quad y^\phi * x^\phi = b_{uv} * b_{uv} = b_{uv}.$$

Таким образом, $AE_2(\mathfrak{S}(k,q))$ – подмножество множества всех антиэндоморфизмов.

3. Пусть $\phi := \rho[a_s, M']$ – произвольный эндоморфизм из $AE_3(\mathfrak{S}(k,q))$. Эндоморфизм ϕ действует на V следующим образом:

$$(M')^\phi = \{a_s\}, \quad (M * M)^\phi = \{b_{ss}\}, \quad (M \setminus M')^\phi = \{b_{ss}\}.$$

Полагаем, что

$$x_1, y_1 \in (M * M), \quad x_2 \in M \setminus M', y_2 \in (M * M), \quad x_3 \in M', y_3 \in (M * M),$$

$$x_4, y_4 \in M', \quad x_5, y_5 \in M \setminus M'.$$

Тогда справедливы равенства

$$(x_1 * y_1)^\phi = b_{ss}, \quad y_1^\phi * x_1^\phi = b_{ss} * b_{ss} = b_{ss};$$

$$(x_2 * y_2)^\phi = b_{ss}, \quad y_2^\phi * x_2^\phi = b_{ss} * b_{ss} = b_{ss};$$

$$(y_2 * x_2)^\phi = b_{ss}, \quad x_2^\phi * y_2^\phi = b_{ss} * b_{ss} = b_{ss};$$

$$(y_3 * x_3)^\phi = b_{ss}, \quad x_3^\phi * y_3^\phi = a_s * b_{ss} = b_{\beta_s(s),\beta_s(s)} = b_{ss};$$

$$(x_3 * y_3)^\phi = b_{ss}, \quad y_3^\phi * x_3^\phi = b_{ss} * a_s = b_{\beta'_s(s),\beta'_s(s)} = b_{ss};$$

$$(x_2 * x_2)^\phi = b_{ss}, \quad x_2^\phi * x_2^\phi = b_{ss} * b_{ss} = b_{ss};$$

$$(x_3 * x_3)^\phi = b_{ss}, \quad x_3^\phi * x_3^\phi = a_s * a_s = b_{ss};$$

$$(x_2 * x_3)^\phi = b_{ss}, \quad x_3^\phi * x_2^\phi = a_s * b_{ss} = b_{\beta_s(s),\beta_s(s)} = b_{ss};$$

$$(x_3 * x_2)^\phi = b_{ss}, \quad x_2^\phi * x_3^\phi = b_{ss} * a_s = b_{\beta'_s(s),\beta'_s(s)} = b_{ss};$$

$$(x_4 * y_4)^\phi = b_{ss}, \quad y_4^\phi * x_4^\phi = a_s * a_s = b_{ss};$$

$$(x_5 * y_5)^\phi = b_{ss}, \quad y_5^\phi * x_5^\phi = b_{ss} * b_{ss} = b_{ss}.$$

Таким образом, $AE_3(\mathfrak{S}(k,q))$ – подмножество множества всех антиэндоморфизмов. Доказательство завершено.

Для упрощения восприятия доказательства теоремы 2.1 приведем общую схему доказательства.

Общая схема доказательства первого утверждения теоремы 2.1. Зафиксируем произвольный антиэндоморфизм ϕ и рассмотрим два случая (совокупность которых дает альтернативу)

$$M^\phi \subseteq M \text{ и } M^\phi \cap (M * M) \neq \varnothing.$$

В первом случае покажем, что ϕ – антиэндоморфизм из $AE_1(\mathfrak{S}(k,q))$. Во втором случае будет рассмотрена альтернатива:

$$M^\phi \cap (M*M) \neq \varnothing,\ M^\phi \cap M \neq \varnothing \text{ либо } M^\phi \cap (M*M) \neq \varnothing,\ M^\phi \cap M = \varnothing.$$

Получим, что если $M^\phi \cap (M*M) \neq \varnothing$, то ϕ – антиэндоморфизм из

$$AE_2(\mathfrak{S}(k,q)) \cup AE_3(\mathfrak{S}(k,q)).$$

Рассмотрим более подробно.

Доказательство теоремы 2. 1.

1. Полагаем, что $k > 1$. Случай $k = 1$ будет рассмотрен отдельно (в конце). Лемма 3.1 дает включение

$$AE_1(\mathfrak{S}(k,q)) \cup AE_2(\mathfrak{S}(k,q)) \cup AE_3(\mathfrak{S}(k,q)) \subseteq \mathrm{Aend}(\mathfrak{S}(k,q)). \tag{3.2}$$

Далее ϕ – произвольный антиэндоморфизм из $\mathrm{Aend}(\mathfrak{S}(k,q))$.

Рассмотрим случай, когда $M^\phi \subseteq M$. Поскольку $M^\phi \subseteq M$, то ϕ определяет отображение $\alpha:\ \{1,...,k\} \to \{1,...,k\}$, которое определяется эквиваленцией

$$\alpha(i) = j \ \Leftrightarrow\ a_i^\phi = a_j.$$

Полагаем, что b_{ij} – произвольный элемент из $M*M$. Вычислим его ϕ – образ

$$b_{ij}^\phi = (a_i * a_j)^\phi = a_j^\phi * a_i^\phi = a_{\alpha(j)} * a_{\alpha(i)} = b_{\alpha(j),\alpha(i)}. \tag{3.3}$$

Вычисляя левые и правые части в равенствах

$$(a_s * b_{ij})^\phi = b_{ij}^\phi * a_s^\phi,\quad (b_{ij} * a_s)^\phi = a_s^\phi * b_{ij}^\phi,$$

получаем, что для α выполняются условия (2.7), следовательно, $\alpha \in A_{aend}(q)$. Значит, ϕ – антиэндоморфизм из $AE_1(\mathfrak{S}(k,q))$.

2. Рассмотрим случай $M^\phi \cap (M*M) \neq \varnothing$. В этом случае существуют $a_i \in M$ и $b_{uv} \in M*M$, такие что $a_i^\phi = b_{uv}$.

Выполняется включение

$$(M*M)^\phi \subseteq M*M. \tag{3.4}$$

В самом деле, пусть b_{ij} – произвольный элемент из $M*M$. Тогда справедливы равенства и включение

$$b_{ij}^\phi = (a_i * a_j)^\phi = a_j^\phi * a_i^\phi \in M*M.$$

Мы воспользовались простотой элементов из M (это следует из определения операции $(*)$).

В силу включения (3.4) существуют преобразования δ_1 и δ_2 множества $\{1,...,k\}$, такие что для любого $b_{sd} \in M*M$ справедливы равенства

$$b_{sd}^\phi = b_{\delta_1(s,d),\delta_2(s,d)}.$$

Для любых $s,d \in \{1,...,k\}$ должно выполняться равенство

$$(a_i * b_{sd})^\phi = b_{sd}^\phi * a_i^\phi.$$

Вычисляем правую и левую часть этого равенства

$$b_{sd}^{\phi} * a_i^{\phi} = b_{\delta_1(s,d),\delta_2(s,d)} * b_{uv} = b_{\delta_1(s,d),v},$$

$$(a_i * b_{sd})^{\phi} = (b_{\beta_i(s),\beta_i(d)})^{\phi} = b_{\delta_1(\beta_i(s),\beta_i(d)),\delta_2(\beta_i(s),\beta_i(d))}.$$

Отсюда получаем

$$b_{\delta_1(\beta_i(s),\beta_i(d)),\delta_2(\beta_i(s),\beta_i(d))} = b_{\delta_1(s),v}.$$

Последнее равенство выполняется для любых $s, d \in \{1, ..., k\}$. Поскольку β_i является перестановкой, то

$$\{(\beta_i(s), \beta_i(d)) \mid s, d \in \{1, ..., k\}\} = \{1, ..., k\}^2.$$

Значит, $\delta_2(s, d) = v$ при любом $(s, d) \in \{1, ..., k\}^2$.

Проводя аналогичные рассуждения для равенства

$$(b_{sd} * a_i)^{\phi} = a_i^{\phi} * b_{sd}^{\phi},$$

можно показать, что $\delta_1(s, d) = u$ при любом $(s, d) \in \{1, ..., k\}$.

Таким образом, мы показали, что

$$(M * M)^{\phi} = \{b_{uv}\}. \tag{3.5}$$

Пусть $a_j \in M$, такой что $a_j^{\phi} \in M * M$. Тогда $a_j^{\phi} = b_{uv}$. Предположим противное $a_j^{\phi} = b_{gh}$, тогда по доказанному получаем

$$(M * M)^{\phi} = \{b_{uv}\}, \quad (M * M)^{\phi} = \{b_{gh}\},$$

что является противоречием. Таким образом, мы показали включение

$$M^{\phi} \cap (M * M) = \{b_{uv}\}. \tag{3.6}$$

3. Полагаем, что $M^{\phi} \cap (M * M) \neq \varnothing$, $M^{\phi} \cap M \neq \varnothing$. Далее b_{uv} – фиксированный элемент из п. 2 (т. е. $a_i^{\phi} = b_{uv}$). В этом случае в множестве M существует непустое подмножество $M' := \{a_{q_1}, ..., a_{q_d}\}$, такое что $(M')^{\phi} \subseteq M$. Пусть теперь a_s – произвольный элемент из M' и $(a_s)^{\phi} = a_{s'}$. Тогда справедливы равенства

$$b_{uv} = (b_{ss})^{\phi} = (a_s * a_s)^{\phi} = a_{s'} * a_{s'} = b_{s's'}.$$

Следовательно, $s' = u = v$. Поскольку $u = v$, то обозначим их индексом u. Из произвольности элемента a_s из M' получаем, что для любого элемента $a_s \in M'$ справедливо равенство $(a_s)^{\phi} = a_u$.

Равенства

$$b_{uu} = (a_s * b_{uu})^{\phi} = b_{uu}^{\phi} * a_s^{\phi} = b_{uu} * a_u = b_{\beta'_u(u),\beta'_u(u)},$$

$$b_{uu} = (b_{uu} * a_s)^{\phi} = a_s^{\phi} * b_{uu}^{\phi} = a_u * b_{uu} = b_{\beta_u(u),\beta_u(u)}$$

показывают, что $\beta_u(u) = \beta'_u(u) = u$.

Мы показали, что если ϕ – образ элемента a_s – лежит в M, то $(a_s)^{\phi} = a_u$, где a_u – фиксированный элемент, не зависящий от s, и справедливы равенства

$$b_{uu} = b_{uv}, \quad \beta_u(u) = \beta'_u(u) = u.$$

Учитывая равенство (3.6), получаем, что ϕ – это антиэндоморфизм $\rho[a_s, M']$ из $AE_3(\mathfrak{S}(k,q))$.

4. Полагаем, что $M^\phi \cap (M * M) \neq \varnothing$, $M^\phi \cap M = \varnothing$. В этом случае $M^\phi \subseteq M * M$. Тогда в силу (3.6) получаем, что антиэндоморфизм ϕ – это антиэндоморфизм $\zeta[b_{uv}]$ из $AE_2(\mathfrak{S}(k,q))$.

5. Если ϕ – такой, что выполняется неравенство $M^\phi \cap (M * M) \neq \varnothing$, то выполняются посылки либо пункта 3, либо 4. Поэтому справедливо включение

$$\phi \in AE_2(\mathfrak{S}(k,q)) \cup AE_3(\mathfrak{S}(k,q)).$$

Учитывая, что обязательно выполнится один из случаев $M^\phi \subseteq M$ либо $M^\phi \cap (M * *M) \neq \varnothing$, получаем, что при $k > 1$ всякий $\phi \in \mathrm{Aend}(\mathfrak{S}(k,q))$ будет лежать в объединении

$$AE_1(\mathfrak{S}(k,q)) \cup AE_2(\mathfrak{S}(k,q)) \cup AE_3(\mathfrak{S}(k,q)).$$

Мы показали, что

$$\mathrm{Aend}(\mathfrak{S}(k,q)) = AE_1(\mathfrak{S}(k,q)) \cup AE_2(\mathfrak{S}(k,q)) \cup AE_3(\mathfrak{S}(k,q)) \quad (k > 1).$$

При $k = 1$ простой перебор показывает, что выполняются равенства

$$\mathrm{Aaut}(\mathfrak{S}(k,q)) = \mathrm{Aut}(\mathfrak{S}(k,q)) = \{I\}, \quad \mathrm{Aend}(\mathfrak{S}(k,q)) = \mathrm{End}(\mathfrak{S}(k,q)) = \{I, \zeta[b_{11}]\}.$$

Последнее утверждение данной теоремы следует из того, что отображения из множеств $AE_2(\mathfrak{S}(k,q))$ и $AE_3(\mathfrak{S}(k,q))$ не являются обратимыми.
Доказательство теоремы 2.1. завершено.

Пример 3.1. Далее в множестве $\mathrm{Aend}(\mathfrak{S}(k,q))$ выделим подмножества X_1 и X_2, такие что X_1 и X_2 – подполугруппы в моноиде всех эндоморфизмов группоида $\mathfrak{S}(k,q)$.

1. Построим X_1. Пусть $G = (G, *)$ – некоторый группоид, содержащий идемпотенты, и $I(G)$ – множество всех идемпотентов в группоиде G. Тогда для каждого $a \in I(G)$ можно определить отображение f_a, которое все элементы группоида G переводит в элемент a. Отображения f_a $(a \in I(G))$ являются эндоморфизмами (эндоморфизмами в смысле группоида) и антиэндоморфизмами. Это следует из равенств

$$(g_1 * g_2)^{f_a} = a, \quad g_1^{f_a} * g_2^{f_a} = a * a = a;$$

$$(g_1 * g_2)^{f_a} = a, \quad g_2^{f_a} * g_1^{f_a} = a * a = a.$$

В этом случае множество $\{f_a \mid a \in I(G)\}$ образует сингулярную по первому аргументу полугруппу в множествах $\mathrm{End}(G)$ и $\mathrm{Aend}(G)$. Действительно,

$$g^{f_a \cdot f_b} = (g^{f_b})^{f_a} = b^{f_a} = a = g^{f_a}, \quad (a, b \in I(G)),$$

где g – произвольный элемент из G.

Если $G = \mathfrak{S}(k,q)$, то $I(G) = M * M$ и $f_a = \zeta[b_{uv}]$, где $a = b_{uv}$. Таким образом,

$$X_1 = \{f_a \mid a \in I(G)\} = AE_2(\mathfrak{S}(k,q)).$$

2. Полагаем, что $X_2 = AE_2(\mathfrak{S}(k,q)) \cup AE_3(\mathfrak{S}(k,q))$. По определению множества $AE_2(\mathfrak{S}(k,q))$ и $AE_3(\mathfrak{S}(k,q))$ состоят из эндоморфизмов. Замкнутость в X_2 следует из

теоремы 1 в работе [16]. Также из теоремы 1 в [16] следует, что $AE_2(\mathfrak{S}(k,q))$ – двухсторонний идеал в моноиде всех эндоморфизмов. Поэтому

$$AE_2(\mathfrak{S}(k,q)) \cdot AE_3(\mathfrak{S}(k,q)),\ AE_3(\mathfrak{S}(k,q)) \cdot AE_2(\mathfrak{S}(k,q)) \subseteq AE_2(\mathfrak{S}(k,q)).$$

Таким образом, X_2 – замкнуто.

Пример 3.2. Группоид $\mathfrak{S}(k,q)$ можно выбрать так, что множество всех антиэндоморфизмов будет содержать антиэндоморфизм, который не является эндоморфизмом. В самом деле, пусть $k > 1$ и q – кортеж, составленный из единичных перестановок. Определим отображение

$$\phi:\ a_i \to a_i; \quad b_{ij} \to b_{ji} \quad (i,j \in \{1,...,k\}).$$

Несложно увидеть, что данное отображение является антиавтоморфизмом, но не является автоморфизмом. Действительно, последнее утверждение следует из равенств

$$a_i^{\phi} = a_i, \quad a_j^{\phi} = a_j, \quad (a_i * a_j)^{\phi} = b_{ij}^{\phi} = b_{ji}, \quad a_j^{\phi} * a_i^{\phi} = a_j * a_i = b_{ji}.$$

Произведение $\phi \cdot \phi$ равно тождественному отображению I множества V. Из теоремы 2.1 следует, что $I \notin \mathrm{Aend}(\mathfrak{S}(k,q))$, следовательно, в этом случае множество $\mathrm{Aend}(\mathfrak{S}(k,q))$ не является замкнутым относительно композиции двух отображений. В самом деле, поскольку I – биекция V, то I не может попасть в множества $AE_2(\mathfrak{S}(k,q))$ и $AE_3(\mathfrak{S}(k,q))$ (отсутствует биекция). Однако и в множество $AE_1(\mathfrak{S}(k,q))$ при $k > 1$ оно тоже не попадает (см. (2.8) – общий вид отображений из множества $AE_1(\mathfrak{S}(k,q))$).

Пример 3.3. Построим пример группоида $\mathfrak{S}(k,q)$, такого что множество $\mathrm{Aend}(\mathfrak{S}(k,q))$ замкнуто относительно композиции двух антиэндоморфизмов и $\mathrm{Aend}(\mathfrak{S}(k,q)) \subseteq \mathrm{End}(\mathfrak{S}(k,q))$. Через I обозначим тождественное преобразование из $\mathcal{I}_k$.

1. Из теоремы 2.1 следует, что при $k = 1$ будет выполняться равенство

$$\mathrm{Aend}(\mathfrak{S}(k,q)) = \mathrm{End}(\mathfrak{S}(k,q)).$$

2. Пусть $k = 2$ и $q = (\beta_1, \beta_2, \beta_1', \beta_2')$, где

$$\beta_1 = \beta_2 = I, \quad \beta_1' = \beta_2' = (1,2).$$

В данном случае $AE_3(\mathfrak{S}(k,q)) = \varnothing$. В самом деле, нет $a_s \in M$, такого что $\beta_s(s) = s$ и $\beta_s'(s) = s$.

В данном случае $\mathcal{I}_2 = \{I, (2,1), \alpha_1, \alpha_2\}$, где $\alpha_1(x) = 1$ и $\alpha_2(x) = 2$ (константы) для любого $x \in \{1,2\}$.

Прямая проверка показывает, что условия (2.7) не выполняются ни при каком отображении из $\mathcal{I}_2$. Поэтому множество $AE_1(\mathfrak{S}(k,q)) = \varnothing$. Таким образом, в силу теоремы 2.1 получаем равенства

$$\mathrm{Aend}(\mathfrak{S}(k,q)) = AE_2(\mathfrak{S}(k,q)) = \{\zeta[b_{11}], \zeta[b_{22}], \zeta[b_{12}], \zeta[b_{21}]\} \subset \mathrm{End}(\mathfrak{S}(k,q)).$$

4. Доказательство теоремы 2.2

Для доказательства теоремы 2.2 докажем леммы 4.1 и 4.2.

Л е м м а 4.1. *Пусть* $\alpha_1, \alpha_2 \in Ae(M_1, ..., M_m)$. *Тогда* $\alpha_1 \circ \alpha_2 \in Ae(M_1, ..., M_m)$ *и справедливо равенство*

$$l_{\alpha_1 \cdot \alpha_2}(i) = l_{\alpha_1}(l_{\alpha_2}(i)) \quad (i \in \{1, ..., m\}). \tag{4.1}$$

Д о к а з а т е л ь с т в о. В самом деле, пусть $\alpha_1, \alpha_2 \in Ae(M_1, ..., M_m)$. Покажем, что композиция $\alpha_1 \circ \alpha_2$ лежит в $Ae(M_1, ..., M_m)$. Справедливы равенства и включения

$$j = l_{\alpha_2}(i), \quad s = l_{\alpha_1}(j), \quad M_i^{\alpha_1 \circ \alpha_2} = (M_i^{\alpha_2})^{\alpha_1} \subseteq M_j^{\alpha_1} \subseteq M_s.$$

Поскольку $D^{\alpha_2} \subseteq D$ и $D^{\alpha_1} \subseteq D$, то $D^{\alpha_1 \circ \alpha_2} \subseteq D$. Таким образом, мы показали включение $\alpha_1 \circ \alpha_2 \in Ae(M_1, ..., M_m)$.

Далее пусть q – произвольный индекс из $\{1, ..., m\}$. Тогда выполняются условия

$$M_q^{\alpha_2} \subseteq M_u \ \Rightarrow \ l_{\alpha_2}(q) = u;$$

$$M_u^{\alpha_1} \subseteq M_v \ \Rightarrow \ l_{\alpha_1}(u) = v;$$

$$M_q^{\alpha_1 \circ \alpha_2} = (M_q^{\alpha_2})^{\alpha_1} \subseteq (M_u)^{\alpha_1} \subseteq M_v \ \Rightarrow \ l_{\alpha_1 \circ \alpha_2}(q) = v.$$

Наконец, равенства $l_{\alpha_2}(q) = u$ и $l_{\alpha_1}(u) = v$ приводят к равенствам

$$l_{\alpha_1 \circ \alpha_2}(q) = v = l_{\alpha_1}(u) = l_{\alpha_1}(l_{\alpha_2}(q)),$$

которые выполняются для любого $q \in \{1, ..., m\}$.
Д о к а з а т е л ь с т в о з а в е р ш е н о.

Л е м м а 4.2. *Пусть* α *– отображение из* $Ae(M_1, ..., M_m)$. *Тогда отображение* μ_α, *заданное правилом* (2.11), *является эндоморфизмом системы* $\mathfrak{G}$. *Отображения вида* (2.11) *существуют.*

Д о к а з а т е л ь с т в о. Единичное отображение является частным случаем отображения (2.11).

Вводим обозначение $\phi := \mu_\alpha$. Далее покажем, что для любых $x, y \in V$ выполняется равенство

$$(x * y)^\phi = x^\phi * y^\phi. \tag{4.2}$$

1. Полагаем, что $(a_i, a_j) \in M_q$, где $q \in \{1, ..., m\}$. Тогда для $q' = l_\alpha(q)$ выполняется равенство $(a_i^\phi, a_j^\phi) = (a_{\alpha(i)}, a_{\alpha(j)}) \in M_{q'}$. Вычисления показывают, что справедливы равенства

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

которые показывают, что $(a_i * a_j)^\phi = a_i^\phi * a_j^\phi$.

2. Отображение α удовлетворяет условиям (2.10). 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

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

которые показывают справедливость равенства (4.2) для всех пар $(x, y) \in D$.

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

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

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

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

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

Далее из соотношений

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

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

получаем справедливость равенств $(c_i * a_q)^\phi = c_i^\phi * a_q^\phi$, $(a_q * c_i)^\phi = a_q^\phi * c_i^\phi$.

4. Покажем, что $(x * y)^\phi = x^\phi * y^\phi$, когда $x, y \in M * M$. Равенства

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

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

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

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

показывают, что

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

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

Доказательство завершено.

В множестве всех эндоморфизмов $\mathrm{End}(\mathfrak{G}(k, 1, M_1))$ группоида $\mathfrak{G}(k, 1, M_1)$ выделим подмножество

$$E := \{\mu_\alpha \mid \alpha \in Ae(M_1, ..., M_m)\}.$$

Для любых $\alpha_1, \alpha_2 \in Ae(M_1, ..., M_m)$ выполняется равенство

$$\mu_{\alpha_1} \cdot \mu_{\alpha_2} = \mu_{\alpha_1 \circ \alpha_2}. \tag{4.3}$$

В самом деле, проведем вычисления

$$a_i^{\mu_{\alpha_1} \cdot \mu_{\alpha_2}} = (a_i^{\mu_{\alpha_2}})^{\mu_{\alpha_1}} = a_{\alpha_2(i)}^{\mu_{\alpha_1}} = a_{\alpha_1(\alpha_2(i))} = a_{(\alpha_1 \circ \alpha_2)(i)} = a_i^{\mu_{\alpha_1 \circ \alpha_2}}. \tag{4.4}$$

$$c_q^{\mu_{\alpha_1} \cdot \mu_{\alpha_2}} = (c_{l_{\alpha_2}(q)})^{\mu_{\alpha_1}} = c_{l_{\alpha_1}(l_{\alpha_2}(q))} = c_{l_{\alpha_1 \circ \alpha_2}(q)} = c_q^{\mu_{\alpha_1 \circ \alpha_2}}. \tag{4.5}$$

$$b_{uv}^{\mu_{\alpha_1} \cdot \mu_{\alpha_2}} = (b_{uv}^{\mu_{\alpha_2}})^{\mu_{\alpha_1}} = b_{\alpha_2(u),\alpha_2(v)}^{\mu_{\alpha_1}} = b_{\alpha_1(\alpha_2(u)),\alpha_1(\alpha_2(v))} = b_{uv}^{\mu_{\alpha_1 \circ \alpha_2}}. \tag{4.6}$$

Равенства (4.4), (4.5) и (4.6) показывают справедливость равенства (4.3).

Множество E является замкнутым относительно композиции двух эндоморфизмов. Это следует из леммы 4.1 и равенства (4.3).

Кроме того, имеет место изоморфизм

$$Ae(M_1, ..., M_m) \cong E. \tag{4.7}$$

Изоморфизм будет осуществлять отображение $\xi : \ Ae(M_1, ..., M_m) \to E$, заданное правилом

$$\xi(\alpha) = \mu_\alpha \quad (\alpha \in Ae(M_1, ..., M_m), \quad \mu_\alpha \in E).$$

Доказательство теоремы 2.2. Пусть G – некоторый конечный моноид и k – натуральное число больше $|G|$. Пусть $m := |G|$ и I'_m – множество отображений α из $\mathcal{I}_k$, таких что α переводит множество $\{1, ..., m\}$ в себя, а на $\{m+1, ..., k\}$ отображения α действуют как тождественное отображение. Множество I'_m – замкнуто относительно композиции двух отображений и содержит тождественное отображение (тривиально проверяется). Очевидно, что $I'_m \cong \mathcal{I}_m$.

Далее вводим множество M_1 с помощью равенства

$$M_1 := \{(a_{\alpha_1(1)}, a_{\alpha_2(1)}) \in M \times M \mid \alpha_1, \alpha_2 \in I'_m\}.$$

Несложно увидеть, что выполняется равенство

$$M_1 = \{(a_i, a_j) \in M \times M \mid i, j = 1, ..., m\}.$$

Теорема 1′ на стр. 419 из [17] утверждает: *всякая конечная полугруппа с единицей G изоморфно вкладывается в симметрическую полугруппу на множестве G.*

Поскольку $m = |G|$, то получаем, что G – изоморфен $H_1(G)$, где $H_1(G)$ – некоторый подмоноид в $\mathcal{I}_m$. Поскольку $I'_m \cong \mathcal{I}_m$, то $H_1(G)$ будет изоморфен некоторому подмоноиду I'_m, который обозначим $H_2(G)$. Следовательно, моноид G изоморфен $H_2(G)$, где $H_2(G)$ – некоторый подмоноид в I'_m.

При этом $H_2(G)$ является подмоноидом в $\mathcal{I}_k$. В силу определений множеств I'_m и M_1 получаем, что для любого отображения $\alpha \in H_2(G)$ выполняется включение

$$M_1^\alpha \subseteq M_1.$$

Зная множество M_1, мы можем вычислить множество D:

$$D = (M \times M) \setminus M_1 = \{(a_i, a_j) \mid i, j \in \{m+1, ..., k\}\}.$$

Далее вычисляем множество D^α:

$$D^\alpha = \{(a_{\alpha(i)}, a_{\alpha(j)}) \mid i, j \in \{m+1, ..., k\}\} = \{(a_i, a_j) \mid i, j \in \{m+1, ..., k\}\} = D.$$

Таким образом, мы получаем, что $\alpha \in Ae(M_1)$. Следовательно,

$$H_2(G) \subseteq Ae(M_1).$$

Учитывая изоморфизм $Ae(M_1) \cong E$ (в силу (4.7)), получаем, что $H_2(G)$ изоморфен некоторому подмоноиду $H_3(G)$ моноида E. Таким образом, получаем

$$G \cong H_1(G) \cong H_2(G) \cong H_3(G) \subset E \subset \mathrm{End}(\mathfrak{G}(k, 1, M_1)).$$

Доказательство завершено.

Благодарности. Работа поддержана Красноярским математическим центром, финансируемым Минобрнауки РФ (Соглашение 075-02-2022-876).

Список литературы

1. Gewirtzman L. Anti-isomorphisms of the endomorphism rings of a class of free module // Math. Ann., 1965. Vol. 159. pp. 278–284.

2. Gewirtzman L. Anti-isomorphisms of endomorphism rings of torsion-free module // Math. Z. 1967. Vol. 98. pp. 391–400.

3. Balaba I. N., Mikhalev A. V. Anti-isomorphisms of graded endomorphism rings of graded modules close to free ones // J. Math. Sci. 2010. Vol. 164, No 2. pp. 168–177. DOI: https://doi.org/10.1007/s10958-009-9747-x

4. Semenov P. P. Endomorphisms of semigroups of invertible nonnegative matrices over ordered rings // Journal of Mathematical Sciences. 2013. Vol. 193, No. 4. pp. 591–600. DOI: https://doi.org/10.1007/s10958-013-1486-3

5. Tsarkov O. I. Endomorphisms of the Semigroup $G_2(r)$ Over Partially Ordered Commutative Rings Without Zero Divisors and with 1/2 // Journal of Mathematical Sciences. 2014. Vol. 201, No. 4. pp. 534–551. DOI: https://doi.org/10.1007/s10958-014-2010-0

6. Zhuchok Yu. V. Endomorphism semigroups of some free products // Journal of Mathematical Sciences. 2012. Vol. 187, No. 2. pp. 146–152. DOI: http://dx.doi.org/1072-3374/12/1872-0146

7. Tabarov A. Kh. Homomorphisms and endomorphisms of linear and alinear quasigroups // Discrete Mathematics and Applications. 2007. Vol. 17, No. 3. pp. 253–260. DOI: https://doi.org/10.4213/dm21

8. Михалёв А. В., Шаталова М. А. Автоморфизмы и антиавтоморфизмы, полугруппы обратимых матриц с неотрицательными элементами // Матем. сб. 1970. Т. 81, № 4. С. 600–609.

9. Katyshev S. YU., Markov V. T., Nechayev A. A. Application of non-associative groupoids to the realization of an open key distribution procedure // Discrete Mathematics and Applications. 2015. Vol. 25, No. 1. pp. 9–24. DOI: https://doi.org/10.4213/dm1289

10. Горнова М. Н., Кукина Е. Г., Романьков В. А. Криптографический анализ протокола аутентификации Ушакова–Шпильрайна, основанного на проблеме бинарно скрученной сопряжённости // Прикладная дискретная математика. 2015. Т. 28, № 2. С. 46–53. DOI: https://doi.org/10.17223/20710410/28/5

11. Тимофеенко Г. В., Глухов М. М. Группа автоморфизмов конечно-определенных квазигрупп // Матем. заметки. 1985. Т. 37, № 5. С. 617–626.

12. Birkhoff G.O. Automorphism groups // Revista de la Union Math. 1946. Vol. 4. pp. 155–157.

13. Groot J. Automorphism groups of rings // Int. Congr. of Mathematicians. 1958. P. 18.

14. Литаврин А. В. Автоморфизмы некоторых магм порядка $k + k^2$ // Известия Иркутского государственного университета. Серия Математика. 2018. Т. 26. С. 47–61. DOI: https://doi.org/10.26516/1997-7670.2018.26.47

15. 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. DOI: https://doi.org/10.26516/1997-7670.2018.26.47

16. Litavrin A. V. Endomorphisms of Some Groupoids of Order $k + k^2$ // Bulletin of Irkutsk State University. Series Mathematics. 2020. Vol. 32. pp. 64–78. DOI: https://doi.org/10.26516/1997-7670.2020.32.64

17. Курош А. Г. Лекции по общей алгебре. М.: ИД «Лань», 2007. 560 с.

Поступила 23.11.2021; доработана после рецензирования 16.02.2021; принята к публикации 24.02.2022

Автор прочитал и одобрил окончательный вариант рукописи.
Конфликт интересов: автор заявляет об отсутствии конфликта интересов.

References

1. L. Gewirtzman, "Anti-isomorphisms of the endomorphism rings of a class of free module", *Math. Ann.*, **159** (1965), 278–284.

2. L. Gewirtzman, "Anti-isomorphisms of endomorphism rings of torsion-free module", *Math. Z.*, **98** (1967), 391–400.

3. I. N. Balaba, A. V. Mikhalev, "Anti-isomorphisms of graded endomorphism rings of graded modules close to free ones", *J. Math. Sci.*, **164**:2 (2010), 168–177. DOI: https://doi.org/10.1007/s10958-009-9747-x

4. P. P. Semenov, "Endomorphisms of semigroups of invertible nonnegative matrices over ordered rings", *Journal of Mathematical Sciences*, **193**:4 (2013), 591–600. DOI: https://doi.org/10.1007/s10958-013-1486-3

5. O. I. Tsarkov, "Endomorphisms of the semigroup $G_2(r)$ over partially ordered commutative rings without zero divisors and with 1/2", *Journal of Mathematical Sciences*, **201**:4 (2014), 534–551. DOI: https://doi.org/10.1007/s10958-014-2010-0

6. Yu. V. Zhuchok, "Endomorphism semigroups of some free products", *Journal of Mathematical Sciences*, **187**:2 (2012), 146–152. DOI: http://dx.doi.org/1072-3374/12/1872-0146

7. A. Kh. Tabarov, "Homomorphisms and endomorphisms of linear and alinear quasigroups", *Discrete Mathematics and Applications*, **17**:3 (2007), 253–260. DOI: https://doi.org/10.4213/dm21

8. A. V. Mikhalev, M. A. Shatalova, "Automorphisms and anti-automorphisms of a semigroup of invertible matrices with nonnegative elements", *Mat. Sb.*, **81**:4 (1970), 600–609 (In Russ.).

9. S. Yu. Katyshev, V. T. Markov, A. A. Nechayev, "Application of non-associative groupoids to the realization of an open key distribution procedure", *Discrete Mathematics and Applications*, **25**:1 (2015), 9–24. DOI: https://doi.org/10.4213/dm1289

10. M. N. Gornova, E. G. Kukina, V. A. Roman'kov, "Cryptographic analysis of the Ushakov-Shpilrain authentication protocol based on the binary twisted conjugacy problem", *Applied Discrete Mathematics*, **28**:2 (2015), 46–53 (In Russ). DOI: https://doi.org/10.17223/20710410/28/5

11. G. V. Timofeenko, M. M. Glukhov, "Groups of automorphisms of finitely presented quasigroups", *Math. Notes*, **37**:5 (1985), 617–626 (In Russ.). DOI: https://doi.org/10.1007/BF01157961

12. G. O. Birkhoff, "Automorphism groups", *Revista de la Union Math.*, **4** (1946), 155–157.

13. J. Groot, "Automorphism groups of rings", *Int. Congr. of Mathematicians*, 1958, 18.

14. A. V. Litavrin, "Automorphisms of some magmas of order $k + k^2$", *Bulletin of Irkutsk State University. Series Mathematics*, **26** (2018), 47–61 (In Russ.). DOI: https://doi.org/10.26516/1997-7670.2018.26.47

15. A. V. Litavrin, "Automorphisms of some finite magmas with order strictly less than N(N+1) and a generating set of N elements", *Vestnik TVGU. Series: Applied Mathematics*, **2** (2019), 70–87 (In Russ.). DOI: https://doi.org/10.26516/1997-7670.2018.26.47

16. A. V. Litavrin, "Endomorphisms of Some Groupoids of Order $k + k^2$", *Bulletin of Irkutsk State University. Series Mathematics*, **32** (2020), 64–78. DOI: https://doi.org/10.26516/1997-7670.2020.32.64

17. A. G. Kurosh, *Lektsii po obshchey algebre [Lectures on general algebra]*, Publishing House «Lan», Moscow, 2007, 560 p.

Submitted 23.11.2021; Revised 16.02.2021; Accepted 24.02.2022

The author have read and approved the final manuscript.
Conflict of interest: The author declare no conflict of interest.