Серия «Математика»
2020. Т. 32. С. 64—78

Онлайн-доступ к журналу:
http://mathizv.isu.ru

ИЗВЕСТИЯ
Иркутского
государственного
университета

УДК 512.548.2+512.54
MSC 17B40, 17B30
DOI https://doi.org/10.26516/1997-7670.2020.32.64

Endomorphisms of Some Groupoids of Order $k+k^2$ *

A. V. Litavrin
Siberian Federal University, Krasnoyarsk, Russian Federation

Abstract. Automorphisms and endomorphisms are actively used in various theoretical studies. In particular, the theoretical interest in the study of automorphisms is due to the possibility of representing elements of a group by automorphisms of a certain algebraic system. For example, in 1946, G. Birkhoff showed that each group is the group of all automorphisms of a certain algebra. In 1958, D. Groot published a work in which it was established that every group is a group of all automorphisms of a certain ring. It was established by M. M. Glukhov and G. V. Timofeenko: every finite group is isomorphic to the automorphism group of a suitable finitely defined quasigroup.

In this paper, we study endomorphisms of certain finite groupoids with a generating set of k elements and order $k+k^2$, which are not quasigroups and semigroups for $k > 1$. A description is given of all endomorphisms of these groupoids as mappings of the support, and some structural properties of the monoid of all endomorphisms are established. It was previously established that every finite group embeds isomorphically into the group of all automorphisms of a certain suitable groupoid of order $k + k^2$ and a generating set of k elements.

It is shown that for any finite monoid G and any positive integer $k \geq |G|$ there will be a groupoid S with a generating set of k elements and order $k + k^2$ such that G is isomorphic to some submonoid of the monoid of all endomorphisms of the groupoid S.

Keywords: endomorphism of the groupoid, endomorphisms, groupoids, magmas, monoids.

* This work is supported by the Krasnoyarsk Mathematical Center and financed by the Ministry of Science and Higher Education of the Russian Federation in the framework of the establishment and development of regional Centers for Mathematics Research and Education (Agreement No. 075-02-2020-1534/1).

1. Introduction

Let A be some set and $(*)$ be a binary algebraic operation defined on the set A. Then the pair $\mathfrak{A} = (A, *)$ is called a groupoid (so-called *magma*). For each groupoid, *endomorphisms* and *automorphisms* are defined (see [8]). The set of all endomorphisms of a groupoid $\mathfrak{A}$ is denoted as $\mathrm{End}(\mathfrak{A})$, and the set of all automorphisms as $\mathrm{Aut}(\mathfrak{A})$. It is well known that with respect to the composition of two endomorphisms, the set $\mathrm{End}(\mathfrak{A})$ generates a monoid ($\mathrm{Aut}(\mathfrak{A})$ forms a subgroup in the monoid $\mathrm{End}(\mathfrak{A})$).

In [5], groupoids $\mathfrak{S}(k, q)$ of order $k + k^2$ and a generating set of k elements were introduced. Automorphisms of these groupoids were also studied there. In particular, it was established that every finite group G will be isomorphic to some subgroup of the group of all automorphisms of a suitable groupoid $\mathfrak{S}(|G|, q)$.

Similar results were obtained in [6] for groupoids $\mathfrak{G} = (V, *)$ generated by n elements and order $|V|$ satisfying the inequalities $n+1 \leq |V| < n^2+n$.

In connection with the results of the work [5], [6] on studies of finite groupoids and works on the description of monoids of endomorphisms (for example, [9]) of some groupoids, interest in studying the problem arose

Problem 1. To obtain an elementwise description of the monoid of endomorphisms of the groupoid $\mathfrak{S}(k, q)$.

As an outcome of scientific work of G. Birkhoff (see [2]), D. Groot (see [12]) and [11] (M.M. Glukhov and G.V. Timofeenko) has been considerable interest in studying the problem

Problem 2. To find out if every finite monoid is isomorphic to some submonoid of the monoid of all endomorphisms of a suitable groupoid $\mathfrak{S}(k, q)$.

This paper is devoted to the study of problems 1 and 2. The main results are stated as Theorems 1 and 2. Theorem 1 gives a description of the endomorphisms of the groupoid $\mathfrak{S}(k, q)$ and some structural properties of the monoid $\mathrm{End}(\mathfrak{S}(k, q))$. The affirmative answer to the question from Problem 2 follows from Theorem 2.

2. Statement of Theorems 1 and 2

We give the definitions and notation necessary for the statement of Theorems 1 and 2.

Symbols associated with a symmetric semigroup. By the symbol $\mathcal{I}_n$ we denote *a symmetric semigroup* of all mappings of the set $\{1, ..., n\}$ into itself. As usual, the symbol S_n denotes the *symmetric group* permutations of the set of n elements. The composition of two mappings from $\mathcal{I}_n$ will be denoted by $(\circ)$. Let x be an arbitrary element from $\{1,...,n\}$ and α an arbitrary map from $\mathcal{I}_n$. Then $\alpha(x)$ is the image of the element x under the action of the map α. If $\alpha, \beta \in \mathcal{I}_n$ and $x \in \{1,...,n\}$, then we put $(\alpha \circ \beta)(x) := \alpha(\beta(x))$.

We give the definition 1 of groupoid $\mathfrak{S}(k,q)$ from [5].

Definition 1. *For each natural number k, we introduce the following sets:*

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

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

Next, fix the tuple $q = (\beta_1,...,\beta_k,\beta'_1,...,\beta'_k) \in S_k^{2k}$. On the set V, we define a binary algebraic operation $(*)$ such that the following equalities are satisfied

$$a_i * a_j = b_{ij}, \quad a_s * b_{ij} = b_{\beta_s(i),\beta_s(j)}, \tag{2.1}$$

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

Then

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

we denote the groupoid $\mathfrak{S}$ with the set support V and the binary algebraic operation $(*)$ defined by the equalities (2.1).

Note that for $k > 1$ the groupoids $\mathfrak{S}(k,q)$ will be non-associative. In fact, it suffices to calculate the elements $(a_1 * a_2) * b_{21}$ and $a_1 * (a_2 * b_{21})$.

We assume that the groupoid $\mathfrak{S}(k,q)$ is given; therefore, the tuple is given

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

In the set $\mathcal{I}_k$, select a subset of $A_e(q)$ transformations of γ such that for any $s,i \in \{1,...,k\}$ the equalities hold

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

For each $\gamma \in A_e(q)$ we introduce the mapping

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

For each element b_{uv} from $M * M$ mapping is introduced $\zeta[b_{uv}]$, maps all elements of the set–carrier V in b_{uv}:

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

Let $a_s \in M$ such that $\beta_s(s) = \beta'_s(s) = s$ and M' is an arbitrary non-empty subset of M other than M. Then introduced the mapping

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

$$b_{ij} \to b_{ss},\ (b_{ij} \in M * M).$$

It is proved (see in this article lemmas 1, 5 and 6), what mappings ϕ_γ, $\zeta[b_{uv}]$ and $\rho[a_s, M']$ are endomorphisms of a groupoid $\mathfrak{S}(k,q)$.

In the set $\mathrm{End}(\mathfrak{S}(k,q))$ select the subsets:

1. $E_1(\mathfrak{S}(k,q))$, consisting of all kinds of endomorphisms ϕ_γ;
2. $E_2(\mathfrak{S}(k,q))$, consisting of all kinds of endomorphisms $\zeta[b_{uv}]$ and identical endomorphism
3. $E_3(\mathfrak{S}(k,q))$, consisting of all kinds of endomorphisms $\rho[a_s, M']$ and identical endomorphism.

By I we denote the identity transformation of the set V. Easy to verify conditions

$$E_i(\mathfrak{S}(k,q)) \cap E_j(\mathfrak{S}(k,q)) = \{I\} \quad (i \neq j,\ i,j = 1,2,3).$$

Wherein $E_1(\mathfrak{S}(k,q))$ and $E_2(\mathfrak{S}(k,q))$ are submonoids in a monoid of all endomorphisms $\mathrm{End}(\mathfrak{S}(k,q))$ (proved in the lemma 8), but set $E_3(\mathfrak{S}(k,q))$ not closed.

Symbols associated with the action of endomorphisms. Let $x \in V$ and $\phi \in \mathrm{End}\ (\mathfrak{S}(k,q))$. Then x^ϕ is the image of an element x under the influence of endomorphism ϕ. The composition of two endomorphisms will be denoted by $(\cdot)$. If $\phi_1, \phi_2 \in \mathrm{End}\ (\mathfrak{S}(k,q))$ and $x \in V$, then $x^{\phi_1 \cdot \phi_2} := (x^{\phi_2})^{\phi_1}$.

Semigroup definitions. A semigroup $\mathfrak{A} = (A, \star)$ will be called singular in the first argument if, for any $x, y \in A$ equality holds $x \star y = x$. If B is subset of the set A then through $\langle B\rangle$ denote the set containing B and all kinds of products of some finite number of elements from B. If B, D are some subsets of the set A, then in the standard way we define the set

$$B \star D := \{b \star d \mid b \in B,\ d \in D\}.$$

The main result of this work is

Theorem 1. *For any groupoid $\mathfrak{S}(k,q)$ statements are true*

1. the equality is true

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

2. the inclusion is true

$$\mathrm{Aut}(\mathfrak{S}(k,q)) \subseteq E_1(\mathfrak{S}(k,q));$$

3. the set $E_2(\mathfrak{S}(k,q)) \setminus \{I\}$ is a singular semigroup relative to the first argument and a two-sided ideal in the monoid $\mathrm{End}(\mathfrak{S}(k,q))$*;*

4. the following inclusions are valid

$$\langle E_3(\mathfrak{S}(k,q))\rangle \subseteq E_3(\mathfrak{S}(k,q)) \cdot E_2(\mathfrak{S}(k,q)),$$

$$E_1(\mathfrak{S}(k,q)) \cdot E_3(\mathfrak{S}(k,q)) \subseteq E_3(\mathfrak{S}(k,q)).$$

By $|X|$ we denote the cardinality of the set X.

Theorem 2. *For every finite monoid G and any natural number $k \geq |G|$ there is a groupoid $\mathfrak{S}(k,q)$ such that the monoid G isomorphic to some submonoid of a monoid $E_1(\mathfrak{S}(k,q))$.*

Theorem 2 is proved constructively. In the proof, for each finite monoid, an infinite series of groupoids is constructed $\mathfrak{S}(k,q)$, realizing the statement of the theorem (the tuple q in these groupoids may include non-identical permutations, in contrast to a similar result for automorphisms from [5]).

3. Proof of Theorems 1 and 2

To prove Theorems 1 and 2, we state and prove Lemmas 1, 2, 3, 4, 5, 6, 7, and 8.

Let $\mathfrak{A} = (A,*)$ is some groupoid. Mapping $\phi : A \to A$ is an endomorphism of a groupoid $\mathfrak{A}$ if and only if for any $x, y \in A$ equality holds

$$(x * y)^{\phi} = x^{\phi} * y^{\phi}. \tag{3.1}$$

Lemma 1. *Let $\gamma \in A_e(q)$. Then the mapping ϕ_γ, specified by rule* (2.3)*, is an endomorphism of a groupoid $\mathfrak{S}(k,q)$.*

Proof. The proof is based on the verification of equalities (3.1). The scheme of the proof coincides with the scheme of the proof of Lemma 3 from [5]. □

Lemma 2. *Let γ is some mapping from $\mathcal{I}_k$ and ϕ is endomorphism of a groupoid $\mathfrak{S}(k,q)$ such that the equalities hold*

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

Then $\gamma \in A_e(q)$.

Proof. The proof carries over verbatim from the proof of Lemma 4 from [5]. □

Lemma 3. *For any endomorphism ϕ of groupoid $\mathfrak{S}(k,q)$ the inclusion is fulfilled $(M * M)^{\phi} \subseteq M * M$.*

Proof. Let b_{ij} is an arbitrary element of $M * M$. Then the equalities and inclusion

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

are true. We took advantage of the fact that elements from M cannot be obtained, like the products of some elements from V (this follows from the definition of the operation $*$). □

Lemma 4. *Let $k > 1$. We assume that ϕ is some transformation of the set V. If intersection M^{ϕ} and $M * M$ not empty then ϕ was an endomorphism of a groupoid $\mathfrak{S}(k, q)$, it is necessary that $(M * M)^{\phi}$ consisted of only one element.*

Proof. Assume that ϕ is transformation of the set V, satisfying the conditions of the lemma, and $(a_i)^{\phi} = b_{uv}$ for some suitable $b_{uv} \in M * M$. Suppose that ϕ is endomorphism of a groupoid$\mathfrak{S}(k, q)$. By lemma 3 we have $(M * M)^{\phi} \subseteq M * M$ therefore there are transformations δ_1 and δ_2 of the set $\{1, ..., k\}$ such that for any $b_{sd} \in M * M$ equalities are fulfilled

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

For any $s, d \in \{1, ..., k\}$ equality must be fulfilled

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

We calculate the right and left sides of this equality

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

From here we get

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

The last equality holds for all $s, d \in \{1, ..., k\}$. Note that β_i is permutation, therefore,

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

So $\delta_1(s) = u$ for any $s \in \{1, ..., k\}$.

On the other hand, for any $s, d \in \{1, ..., k\}$ equality must be fulfilled

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

Calculate the right and left sides of the last equality

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

Hence, the equality

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

is true.

The last equality holds for all $s, d \in \{1, ..., k\}$, hence, $\delta_2(d) = v$ for any $d \in \{1, ..., k\}$.

So for any $s, d \in \{1, ..., k\}$ equality is fulfield

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

where b_{uv} is some fixed element, therefore

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

The lemma is proved. □

Lemma 5. *Let a groupoid be given $\mathfrak{S}(k,q) = (V,*)$. Then for every element $b_{uv} \in M * M$ the mapping $\zeta[b_{uv}]$, specified by rule* (2.4)*, is an endomorphism of a groupoid $\mathfrak{S}(k,q)$.*

Proof. Mapping $\zeta := \zeta[b_{uv}]$ converts any element from V in element b_{uv}. We verify that ζ preserves multiplication. Let $x, y \in V$. For any $x, y \in V$ equalities are justified

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

From here for any $x, y \in V$ the equality is true

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

So ζ is endomorphism of a groupoid $\mathfrak{S}(k,q)$. The lemma is proved. □

Lemma 6. *Let a groupoid be given $\mathfrak{S}(k,q) = (V,*)$ and some element a_s such that $\beta_s(s) = \beta'_s(s) = s$. We assume that M' is an arbitrary non-empty subset M other than M. Then the mapping $\rho[a_s, M']$, specified by rule* (2.5)*, is an endomorphism of a groupoid $\mathfrak{S}(k,q)$.*

Proof. We introduce the notation $\phi := \rho[a_s, M']$. We verify that ϕ preserves multiplication (equality holds 3.1).

Let b_{df} is an arbitrary element from $M * M$ and $a_i \in M'$. The relation are valid

$$(a_i * b_{df})^{\phi} = a_i^{\phi} * b_{df}^{\phi}, \quad (b_{df} * a_i)^{\phi} = b_{df}^{\phi} * a_i^{\phi}.$$

In fact, these relations follow from the equalities

$$(a_i * b_{df})^{\phi} = (b_{\beta_i(d),\beta_i(f)})^{\phi} = b_{ss}, \quad (b_{df} * a_i)^{\phi} = (b_{\beta'_i(d),\beta'_i(f)})^{\phi} = b_{ss},$$

$$a_i^{\phi} * b_{df}^{\phi} = a_s * b_{ss} = b_{\beta_s(s),\beta_s(s)} = b_{ss},$$

$$b_{df}^{\phi} * a_i^{\phi} = b_{ss} * a_s = b_{\beta'_s(s),\beta'_s(s)} = b_{ss}.$$

In the last two chains of equalities, we used the condition

$$\beta_s(s) = \beta'_s(s) = s.$$

Verification of the remaining relations is similar. The lemma is proved. □

Lemma 7. *Let $k > 1$ and ϕ is endomorphism of a groupoid $\mathfrak{S}(k, q)$ such that the intersection of sets M^ϕ and $M * M$ not empty. Then ϕ is an endomorphism $\zeta[b_{uv}]$ either endomorphism $\rho[a_s, M']$.*

Proof. 1. Since the intersection M^ϕ and $M * M$ not empty then by lemma 4 set $(M*M)^\phi$ must contain only one element. Denote this element by b_{uv}.

2. Since the intersection of sets M^ϕ and $M * M$ not empty then exists a_q such that $(a_q)^\phi = b_{ij}$. Further, the equalities

$$(b_{qq})^\phi = b_{uv}, \quad (b_{qq})^\phi = (a_q * a_q)^\phi = a_q^\phi * a_q^\phi = b_{ij} * b_{ij} = b_{ij}$$

show that $b_{ij} = b_{uv}$.

Thus, we have shown that if ϕ is image of the element a_q lies in $M * M$, then $(a_q)^\phi = b_{uv}$.

3. Suppose that in the set M there is no empty subset $M' := \{a_{q_1}, ..., a_{q_d}\}$ such that $(M')^\phi \subseteq M$. Let a_s is an arbitrary element of M' and $(a_s)^\phi = a_{s'}$.

Then the equalities

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

show that $s' = u = v$. Since $u = v$, we denote them by the index f. Due to the arbitrariness of the element a_s from M' we get that for any element $a_s \in M'$ equality $(a_s)^\phi = a_f$ is true.

Equalities

$$b_{uv} = b_{ff} = (a_s * b_{ff})^\phi = a_s^\phi * b_{ff}^\phi = a_f * b_{ff} = b_{\beta_f(f), \beta_f(f)},$$

$$b_{uv} = b_{ff} = (b_{ff} * a_s)^\phi = b_{ff}^\phi * a_s^\phi = b_{ff} * a_f = b_{\beta'_f(f), \beta'_f(f)}$$

show that $\beta_f(f) = \beta'_f(f) = f$.

We have shown that if ϕ is image of the element a_s lies in M, then $(a_s)^\phi = a_f$, where a_f is estsblished element independent of s, and equalities

$$b_{ff} = b_{uv}, \quad \beta_f(f) = \beta'_f(f) = f$$

are true.

Given the second task, we obtain that ϕ is an endomorphism $\rho[a_s, M']$ of kind (2.5).

4. Supposing that $M^\phi \subseteq M * M$. Then, as proved in the second paragraph, we obtain that the endomorphism ϕ is an endomorphism $\zeta[b_{uv}]$ of kind (2.4).

5. Since endomorphism ϕ will satisfy the premises of the third or fourth paragraph and these premises are mutually exclusive, then ϕ this is endomorphism $\rho[a_s, M']$ or $\zeta[b_{uv}]$. The lemma is proved. □

Lemma 8. *The following statements are true:*

1. sets $E_1(\mathfrak{S}(k,q))$ *and* $E_2(\mathfrak{S}(k,q))$ *closed relative to the composition of two endomorphisms;*

2. the set $E_2(\mathfrak{S}(k,q)) \setminus \{I\}$ *is the singular semigroup relative to the first argument and a two-sided ideal in the monoid* $\mathrm{End}(\mathfrak{S}(k,q))$*;*

3. the inclusions are true

$$\langle E_3(\mathfrak{S}(k,q))\rangle \subseteq E_3(\mathfrak{S}(k,q)) \cdot E_2(\mathfrak{S}(k,q)), \tag{3.2}$$

$$E_1(\mathfrak{S}(k,q)) \cdot E_3(\mathfrak{S}(k,q)) \subseteq E_3(\mathfrak{S}(k,q)). \tag{3.3}$$

Proof. 1. Let us prove the first statement. Let be $\gamma_1, \gamma_2 \in A_e(q)$. Direct calculations show that

$$\phi_{\alpha\circ\beta} = \phi_\alpha \cdot \phi_\beta.$$

Next, we show that $\gamma_1 \circ \gamma_2 \in A_e(q)$. Equalities (and similar equalities for β'_s)

$$\beta_{\gamma_1(\gamma_2(s))}(\gamma_1(\gamma_2(i))) = \gamma_1(\beta_{\gamma_2(s)}(\gamma_2(i))) = \gamma_1(\gamma_2(\beta_s(i)))$$

show that $\gamma_1 \circ \gamma_2 \in A_e(q)$. Thus $E_1(\mathfrak{S}(k,q))$ is closed under composition.

Let $\zeta[b_{ab}], \zeta[b_{uv}]$ are two arbitrary non-identical endomorphisms from $E_2(\mathfrak{S}(k,q))$ and x is an arbitrary element of V. Then the equalities

$$x^{\zeta[b_{ab}]\cdot\zeta[b_{uv}]} = (b_{uv})^{\zeta[b_{ab}]} = b_{ab}$$

show that endomorphism $\zeta[b_{ab}] \cdot \zeta[b_{uv}]$ coincides with endomorphism $\zeta[b_{ab}]$. Thus, we showed closure $E_2(\mathfrak{S}(k,q))$ and showed the singularity in the first argument of the semigroup $E_2(\mathfrak{S}(k,q)) \setminus \{I\}$.

2. We show that $E_2(\mathfrak{S}(k,q)) \setminus \{I\}$ is two-sided ideal in a monoid $\mathrm{End}(\mathfrak{S}(k,q))$. Let ϕ is an arbitrary endomorphism from $\mathrm{End}(\mathfrak{S}(k,q))$, $\zeta[b_{uv}]$ is an arbitrary endomorphism from $E_2(\mathfrak{S}(k,q)) \setminus \{I\}$ and x is an arbitrary element of V. We carry out calculations

$$x^{\phi\cdot\zeta[b_{uv}]} = (b_{uv})^{\phi}.$$

By the lemma 3 we have the inclusion $(b_{uv})^{\phi} \in M * M$. Since b_{uv} independent of x, we get that

$$x^{\phi\cdot\zeta[b_{uv}]} = b_{sd}$$

for a suitable element $b_{sd} \in M * M$ independent of x (element b_{sd} is determined by ϕ on b_{uv}). Thus, the equality $\phi \cdot \zeta[b_{uv}] = \zeta[b_{sd}]$. We have shown that $E_2(\mathfrak{S}(k,q)) \setminus \{I\}$ is left ideal.

Semigroup $E_2(\mathfrak{S}(k,q)) \setminus \{I\}$ is a right ideal. In fact, equality

$$x^{\zeta[b_{uv}]\cdot\phi} = (x^{\phi})^{\zeta[b_{uv}]} = b_{uv}$$

show that $\zeta[b_{uv}] \cdot \phi = \zeta[b_{uv}]$.

3. Let us prove the third statement. Let $\rho[a_i, M']$ and $\rho[a_j, M'']$ are two arbitrary endomorphisms from $E_3(\mathfrak{S}(k,q))$, a_m is an arbitrary element

from M and b_{uv} is an arbitrary element of $M * M$. We carry out the calculations

$$a_m^{\rho[a_i,M']\cdot\rho[a_j,M'']} = (a_m^{\rho[a_j,M'']})^{\rho[a_i,M']} = \begin{cases} a_i, & a_j \in M' \text{ and } a_m \in M'', \\ b_{ii}, & a_j \notin M' \text{ or } a_m \notin M'', \end{cases}$$

$$b_{uv}^{\rho[a_i,M']\cdot\rho[a_j,M'']} = (b_{jj})^{\rho[a_i,M']} = b_{ii}.$$

Hence, the equality

$$\rho[a_i, M'] \cdot \rho[a_j, M''] = \begin{cases} \rho[a_i, M''], & a_j \in M', \\ \zeta[b_{ii}], & a_j \notin M', \end{cases}$$

which gives inclusion $\rho[a_i, M'] \cdot \rho[a_j, M''] \in E_3(\mathfrak{S}(k,q)) \cdot E_2(\mathfrak{S}(k,q))$ is fulfield. Since $E_2(\mathfrak{S}(k,q)) \setminus \{I\}$ is two-sided ideal in $\mathrm{End}(\mathfrak{S}(k,q))$, then folows

$$(E_3(\mathfrak{S}(k,q)) \cdot E_2(\mathfrak{S}(k,q))) \cdot E_3(\mathfrak{S}(k,q)) \subseteq E_3(\mathfrak{S}(k,q)) \cdot E_2(\mathfrak{S}(k,q)),$$

$$E_3(\mathfrak{S}(k,q)) \cdot (E_3(\mathfrak{S}(k,q)) \cdot E_2(\mathfrak{S}(k,q))) \subseteq E_3(\mathfrak{S}(k,q)) \cdot E_2(\mathfrak{S}(k,q)),$$

therefore (3.2) is true.

Next let $\phi_\gamma \in E_1(\mathfrak{S}(k,q))$ and $\rho[a_i, M'] \in E_3(\mathfrak{S}(k,q))$. Then the equalities

$$a_m^{\phi_\gamma\cdot\rho[a_i,M']} = \begin{cases} a_i^{\phi_\gamma}, & a_m \in M' \\ b_{ii}^{\phi_\gamma}, & a_m \notin M' \end{cases} = \begin{cases} a_{\gamma(i)}, & a_m \in M' \\ b_{\gamma(i),\gamma(i)}, & a_m \notin M' \end{cases}, \tag{3.4}$$

$$b_{uv}^{\phi_\gamma\cdot\rho[a_i,M']} = b_{\gamma(i),\gamma(i)}$$

are fulfield.

Since $\rho[a_i, M'] \in E_3(\mathfrak{S}(k,q))$ and $\phi_\gamma \in E_1(\mathfrak{S}(k,q))$, then $\gamma \in A_e(q)$ and $\beta_i(i) = \beta_i(i) = i$. Then the equalities

$$\beta_{\gamma(i)}(\gamma(i)) = \gamma(\beta_i(i)) = \gamma(i), \quad \beta'_{\gamma(i)}(\gamma(i)) = \gamma(\beta'_i(i)) = \gamma(i)$$

are fulfield. Hence, the inclusion $\rho[a_{\gamma(i)}, M'] \in E_3(\mathfrak{S}(k,q))$ is fulfield. And by (3.4) equality $\phi_\gamma \cdot \rho[a_i, M'] = \rho[a_{\gamma(i)}, M']$ is true.

Thus, we have shown that the inclusion (3.3) is fulfield. The lemma is proved. $\square$

Remark 1. In general case, the inclusion

$$E_3(\mathfrak{S}(k,q)) \cdot E_1(\mathfrak{S}(k,q)) \subseteq E_3(\mathfrak{S}(k,q))$$

not fulfield. Next, we give a simple example illustrating Remark 1. Let q_0 is a tuple of permutations from $S_{k_0}^{2k_0}$, made up of identical permutations.

Let M' is a subset of the set M and γ is mapping of the set $\{1, ..., k_0\}$ in element j_0, which satisfies the condition $a_{j_0} \notin M'$. Then in the monoid $\mathrm{End}(\mathfrak{S}(k_0, q_0))$ equality will be fulfilled $\rho[a_i, M'] \cdot \phi_\gamma = \zeta[b_{ii}]$, for any $a_i \in M$. The last equality proves the statement from Remark 1.

Proof of the theorem 1. 1. Let ϕ is arbitrary endomorphism of a groupoid $\mathfrak{S}(k, q)$. Consider the case when $k = 1$. The monoid of endomorphisms consists of the identity transformation of the set V and $\zeta[b_{11}]$ endomorphism. The last statement can easily be verified by simply enumerating the mappings of V into itself.

2. We suppose that $k > 1$. In this case $M^\phi \cap (M * M) \neq \varnothing$ or $M^\phi \cap (M * M) = \varnothing$. By the Lemma 1, 5 and 6, we obtain the inclusion

$$E_1(\mathfrak{S}(k, q)) \cup E_2(\mathfrak{S}(k, q)) \cup E_3(\mathfrak{S}(k, q)) \subseteq \mathrm{End}(\mathfrak{S}(k, q)). \tag{3.5}$$

We assume that the intersection M^ϕ and $M * M$ empty. So $M^\phi \subseteq M$, hence, ϕ defines some mapping of the set $\{1, ..., k\}$ into itself. Denote this mapping by γ. Equality holds $a_i^\phi = a_{\gamma(i)}$. Lemma 2 gives inclusion $\gamma \in A_e(q)$. Next, restoring the steps ϕ on whole set V, we get that ϕ is a mapping ϕ_γ specified by rule (2.3).

We assume that the intersection M^ϕ and $M * M$ not empty. Then by the lemma 7 we get that ϕ is an endomorphism $\zeta[b_{uv}]$ either endomorphism $\rho[a_s, M']$. Thus, due to randomness ϕ we get the inclusion

$$\mathrm{End}(\mathfrak{S}(k, q)) \subseteq E_1(\mathfrak{S}(k, q)) \cup E_2(\mathfrak{S}(k, q)) \cup E_3(\mathfrak{S}(k, q)). \tag{3.6}$$

Since the sets $E_i(\mathfrak{S}(k, q))$, at $i = 1, 2, 3$, contain the identical endomorphism and the inclusions are valid (3.5) and (3.6), then helds the equality

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

3. We prove the second statement of Theorem. In [5] among the permutations from S_k stood out a lot of permutations $A(q)$ (see (1.3) in [5]). It is not difficult to verify the equality $S_k \cap A_e(q) = A(q)$. Theorem 2 from [5], in particular, parametrizes automorphisms $\mathrm{Aut}(\mathfrak{S}(k, q))$ permutations from $A(q)$ and gives a general view of automorphism. At γ from $A(q)$ mapping $\phi_\gamma \in E_1(\mathfrak{S}(k, q))$ is an automorphism. Thus, we obtain the inclusion

$$\mathrm{Aut}(\mathfrak{S}(k, q)) \subseteq E_1(\mathfrak{S}(k, q)).$$

4. The third and fourth points of the theorem follow from the lemma 8. Theorem 1 is proved. $\square$

Proof of the theorem 2. 1. Let G is an arbitrary finite monoid, $|G| = m$, $t \geq 0$ is some integer and $k = m + t$. Next, for the monoid

G build a groupoid $\mathfrak{S}(k,q)$ such that G is isomorphically embedded in a monoid $\mathrm{End}(\mathfrak{S}(k,q))$.

Choose a tuple $q \in S_k^{2k}$ such that the following conditions are fulfield:

A. for any $i \in \{1,...,m\}$ equalities are fulfield $\beta_i = \beta_i' = I$ is identity transformation of the set $\{1,...,k\}$;

B. for any $i \in \{m+1,...,k\}$ permutations β_i and β_i' operate on set $\{1,...,m\}$ as the identity permutation, and the set mapping of $\{m+1,...,k\}$ into itself.

2. Let γ is arbitrary mapping from $\mathcal{I}_m$ and γ' is mapping from $\mathcal{I}_k$,which acts on $\{1,...,m\}$ like mapping γ, on set $\{m+1,...,k\}$ acts as an identity map. Note that for each fixed γ mapping γ' defined uniquely. We show that $\phi_{\gamma'}$ is endomorphism of a groupoid $\mathfrak{S}(k,q)$ from monoid $E_1(\mathfrak{S}(k,q))$.

Let $s \in \{1,...,m\}$. Then $\beta_s = \beta_s' = I$, $\gamma'(s) = \gamma(s) \in \{1,..,m\}$, therefore $\beta_{\gamma'(s)} = \beta'_{\gamma'(s)} = I$ and equalities

$$\beta_{\gamma'(s)}(\gamma'(i)) = \gamma'(i),\ \gamma'(\beta_s(i)) = \gamma'(i),\ \beta'_{\gamma'(s)}(\gamma'(i)) = \gamma'(i),\ \gamma'(\beta_s'(i)) = \gamma'(i)$$

for any $i \in \{1,...,k\}$ are true.

Let $s \in \{m+1,...,k\}$. Then the equalities

$$\beta_{\gamma'(s)}(\gamma'(i)) = \beta_s(\gamma'(i)) = \begin{cases} \gamma(i), & i \in \{1,...,m\} \\ \beta_s(i), & i \in \{m+1,...,k\}, \end{cases}$$

$$\gamma'(\beta_s(i)) = \begin{cases} \gamma(i), & i \in \{1,...,m\} \\ \beta_s(i), & i \in \{m+1,...,k\} \end{cases}$$

are true. Hence and from similar equalities for β_s' we get that γ' satisfies the conditions (2.2), hence, $\phi_{\gamma'} \in E_1(\mathfrak{S}(k,q))$.

3. Theorem $1'$ from [4, p. 419] states: *every finite semigroup with unity G embeds isomorphically into a symmetric semigroup on the set G.*

By this theorem $G \cong H$, where H is a submonoid of a symmetric semigroup $\mathcal{I}_m$ (a-priory $|G| = m$). As proved in paragraph 2, any mapping $\gamma \in \mathcal{I}_m$ endomorphism will correspond $\phi_{\gamma'} \in E_1(\mathfrak{S}(k,q))$. Denote by $E(H)$ - a set of all kinds of endomorphisms $\phi_{\gamma'}$, where $\gamma \in H$.

It can be shown that for any mappings $\gamma_1, \gamma_2 \in \mathcal{I}_m$ equalities

$$\phi_{(\gamma_1 \circ \gamma_2)'} = \phi_{\gamma_1' \circ \gamma_2'}, \quad \phi_{\gamma_1' \circ \gamma_2'} = \phi_{\gamma_1'} \cdot \phi_{\gamma_2'} \tag{3.7}$$

are fulfield. In fact, the first equality (3.7) follows from equality of permutations $(\gamma_1 \circ \gamma_2)' = \gamma_1' \circ \gamma_2'$, which give equality

$$(\gamma_1 \circ \gamma_2)'(s_1) = (\gamma_1 \circ \gamma_2)(s_1) = \gamma_1(\gamma_2(s_1)) = \gamma_1'(\gamma_2'(s_1)) = (\gamma_1' \circ \gamma_2')(s_1);$$

$$(\gamma_1 \circ \gamma_2)'(s_2) = s_2 = \gamma_1'(\gamma_2'(s_2)) = (\gamma_1' \circ \gamma_2')(s_2) \quad (s_1 \le m;\ m+1 \le s_2).$$

Second equality from (3.7) follows from the equalities

$$(a_s)^{\phi_{\gamma'_1 \circ \gamma'_2}} = a_{(\gamma'_1 \circ \gamma'_2)(s)} = a_{\gamma'_1(\gamma'_2(s))} = (a_{\gamma'_2(s)})^{\phi_{\gamma'_1}} = ((a_s)^{\phi_{\gamma'_2}})^{\phi_{\gamma'_1}} = a_s^{\phi_{\gamma'_1} \cdot \phi_{\gamma'_2}}$$

$$(s \in \{1, ..., k\}).$$

So $E(H)$ is closed relative to the composition of endomorphisms and $G \cong H \cong E(H),\ E(H) \subseteq E_1(\mathfrak{S}(k,q))$. Theorem 2 is proved. □

4. Conclusion

It is important to study the automorphisms of groupoids that are not semigroups and quasigroups because of potential applications in the cryptography. Problems of application of some non-associative groupoids in cryptography were considered in [3] and other publications.

The results of this paper (Theorem 2) allow us to represent arbitrary finite monoids as some submonoids of a monoid of endomorphisms of a groupoid $\mathfrak{S}(k,q)$. In addition, the solution of Problem 1, formulated as Theorem 1, gives an example of the study of the monoid of endomorphisms of a groupoid, which is not a semigroup or quasigroup.

Moreover, it should be noted that studies of endomorphisms of semigroups and quasigroups are of interest to modern researchers. The $G_n(K)$ semigroups' endomorphisms of invertible non-negative matrices over ordered rings with invertible 2 were studied in [9]. Earlier, in [1; 7] automorphisms $G_n(K)$ over various ordered rings were studied. An example of the study of endomorphisms of linear and alinear quasigroups can be found in [10].

References

1. Bunina E.I., Semenov P.P. Automorphisms of the semigroup of invertible matrices with nonnegative elements over commutative partially ordered rings. *J. Math. Sci.*, 2009, vol. 162, no. 5, pp. 633-–655. https://doi.org/10.1007/s10958-009-9650-5
2. Birkgof G.O. On groups of automorphisms. *Revista de la Union Math. Argentina*, 1946, no. 4, pp. 155–157.
3. 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 https://doi.org/10.4213/dm1289
4. Kurosh A.G. *Lectures on General Algebra.* St. Petersburg, Lan Publ., 2007, 560 p. (in Russian)
5. Litavrin A.V. Automorphisms of some magmas of order $k + k^2$. *The Bulletin of Irkutsk State University. Series Mathematics,* 2018, vol. 26, pp. 47–61. (In Russian). https://doi.org/10.26516/1997-7670.2018.26.47

6. Litavrin A.V. Automorphisms of some finite magmas with order strictly less than the number N (N +1) and a generating set of N elements. *Vestnik TvGU. Series Prikladnaya matematika,* 2018, no. 2, pp. 70–87. (In Russian). https://doi.org/10.26456/vtpmk533
7. Mikhalev A.V., Shatalova M.A. Automorphisms and anti-automorphisms, semigroups of invertible matrices with nonnegative elements. *Math. sbornik*, 1970, vol. 81, no. 4, pp. 600–609. (In Russian).
8. Plotkin B.I. *Groups of automorphisms of algebraic systems.* Moscow, Nauka Publ., 1966.
9. Semenov P.P. Endomorphisms of semigroups of invertible nonnegative matrices over ordered rings. *J. Math. Sci.*, 2013, vol. 193, no. 4, pp. 591-–600. https://doi.org/10.1007/s10958-013-1486-3
10. Tabarov A. Kh. Homomorphisms and endomorphisms of linear and alinear quasigroups. *Discrete Math. Appl.*, 2007, vol. 17, no. 3, pp. 253–260. https://doi.org/10.4213/dm21
11. Timofeyenko G. V., Glukhov M. M. Automorphism group of finitely defined quasigroups. *Matem. zametki* vol. 37, no. 5 (1985), pp. 617–626. (In Russian).
12. Groot J. Automorphism groups of rings. *Int. Congr. of Mathematicians, Edinburgh.*, 1958, p. 18.

Andrey Litavrin, Candidate of Sciences (Physics and Mathematics), Siberian Federal University, 79, Svobodny avenue, Krasnoyarsk, 660041, Russian Federation, email: anm11@rambler.ru,
ORCID iD: https://orcid.org/0000-0001-6285-0201.

Received 10.12.19

Эндоморфизмы некоторых группоидов порядка $k + k^2$

А. В. Литаврин

Сибирский федеральный университет, Красноярск, Российская Федерация

Аннотация. Автоморфизмы и эндоморфизмы активно используются в различных теоретических исследованиях. В частности, теоретический интерес к изучению автоморфизмов обусловлен возможностью представления элементов фиксированной группы автоморфизмами некоторой подходящей алгебраической системы. Например, в 1946 году Г. Биркгоф показал, что каждая группа является группой всех автоморфизмов некоторой алгебры. В 1958 году Д. Гроот опубликовал работу, в которой было установлено, что всякая группа есть группа всех автоморфизмов некоторого кольца. М. М. Глуховым и Г. В. Тимофеенко было установлено: всякая конечная группа изоморфна группе автоморфизмов подходящей конечно-определенной квазигруппы.

Исследуются эндоморфизмы некоторых конечных группоидов с порождающим множеством из k элементов и порядком $k + k^2$, не являющихся квазигруппами и полугруппами при $k > 1$. Приводится описание всех эндоморфизмов этих группоидов как отображений носителя и устанавливаются некоторые структурные свойства моноида всех эндоморфизмов. Ранее было установлено, что всякая конечная группа изоморфно вкладывается в группу всех автоморфизмов некоторого подходящего группоида порядка $k + k^2$ и порождающим множеством из k элементов.

Показано, что для любого конечного моноида G и любого натурального числа $k \geq |G|$ будет существовать группоид S с порождающим множеством из k элементов и порядком $k+k^2$ такой, что G изоморфен некоторому подмоноиду моноида всех эндоморфизмов группоида S.

Ключевые слова: эндоморфизм группоида, эндоморфизмы, группоиды, магмы, моноиды.

Список литературы

1. 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.
2. Биркгоф Г. О. группах автоморфизмов // Revista de la Union Math. Argentina 11. 1946. № 4. С. 155-157.
3. Катышев С. Ю., Марков В. Т., Нечаев А. А. Использование неассоциативных группоидов для реализации процедуры открытого распределения ключей // Дискретная математика. 2014. Т. 26, № 3. С. 45–64. https://doi.org/10.4213/dm1289
4. Курош А. Г. Лекции по общей алгебре. М. : Лань, 2007. 560 с.
5. Литаврин А. В. Автоморфизмы некоторых магм порядка $k+k^2$ // Известия Иркутского государственного университета. Серия Математика. 2018. Т. 26. С. 47–61. https://doi.org/10.26516/1997-7670.2018.26.47
6. 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. 2018. № 2. С. 70–87. https://doi.org/10.26456/vtpmk533
7. Михалев А. В., Шаталова М. А. Автоморфизмы и антиавтоморфизмы, полугруппы обратимых матриц с неотрицательными элементами // Математический сборник. 1970. Т. 81, № 4. С. 600–609.
8. Плоткин Б. И. Группы автоморфизмов алгебраических систем. М. : Наука, 1966.
9. Семёнов П. П. Эндоморфизмы полугрупп обратимых неотрицательных матриц над упорядоченными кольцами // Фундаментальная и прикладная математика. 2012. Т. 17, №. 5. С. 165–178.
10. Табаров А. Х. Гомоморфизмы и эндоморфизмы линейных и алинейных квазигрупп // Дискретная математика. 2007. Т. 19, № 2. С. 67–73. https://doi.org/10.4213/dm21
11. Тимофеенко Г. В., Глухов М. М. Группа автоморфизмов конечноопределенных квазигрупп // Математические заметки. 1985. Т. 37, № 5. С. 617–626.
12. Groot J. Automorphism groups of rings // Int. Congr. of Mathematicians, Edinburgh. 1958. P. 18.

Андрей Викторович Литаврин, кандидат физико-математических наук, доцент кафедры высшей математики № 2, Институт математики и фундаментальной информатики, Сибирский федеральный университет, Россия, 660041, г. Красноярск, пр. Свободный 79,
email: anm11@rambler.ru,
ORCID iD: https://orcid.org/0000-0001-6285-0201.

Поступила в редакцию 10.12.19