On determinability of some classes of medial quasigroups by their endomorphisms

This content has been downloaded from IOPscience. Please scroll down to see the full text.
(http://iopscience.iop.org/1742-6596/532/1/012014)

View the table of contents for this issue, or go to the journal homepage for more

Download details:

IP Address: 193.40.244.197
This content was downloaded on 15/09/2014 at 04:31

Please note that terms and conditions apply.
On determinability of some classes of medial quasigroups by their endomorphisms

A Leibak and P Puusemp
Matemaatikainstituut, Tallinna Tehnikaülikool, Ehitajate tee 5, Tallinn 19086, Estonia

Abstract. We study the endomorphisms of idempotent medial quasigroups and determinability of some classes of medial quasigroups by their endomorphisms. We introduce the endomorphism algebra of idempotent medial quasigroup and prove that if the endomorphism algebras of quasigroups are isomorphic, then the corresponding quasigroups are isomorphic as well. In addition, we present a counterexample to demonstrate that the endomorphism algebras can not be replaced by the endomorphism monoids.

1. Introduction
Idempotent medial quasigroups \cite{2} are distributive quasigroups with a transitive group of middle transformations. Recall that a middle transformation $\phi$ of a quasigroup $Q$ is a permutation of $Q$, if there exists a permutation $\phi^*$, such that $\phi(x) \cdot y = x \cdot \phi^*(y)$ for all $x, y \in Q$. The distributive quasigroups are related to the commutative Moufang loops \cite{2}. It is known that the core of an arbitrary Moufang loop is a left distributive quasigroup. Analytic Moufang loops are used to study continuous symmetries \cite{7}. The left distributive quasigroups with the identity $x(xy) = y$ are homogenous spaces, in the sense of Loos, see \cite{6}. Also, recently several applications of quasigroups to cryptography (block ciphers, secret sharing schemes etc) were proposed.

In \cite{4} the endomorphisms of commutative idempotent medial quasigroups were studied, therefore it was natural to study bigger class of quasigroups. Since Toyoda’s theorem establishes a connection between medial quasigroups and Abelian groups, we restricted ourselves to idempotent medial quasigroups. Moreover, it was natural to ask, what we can get, if we combine Toyoda’s theorem with the results known for the determinability of Abelian groups by their endomorphisms.

One can associate the endomorphism monoid $\text{End}(A)$ to every algebraic structure. Depending on the underlying algebraic structure, the endomorphism monoid can be replaced by endomorphism semilattice, ring etc. Therefore it is natural to ask, if $A$ and $A'$ are algebraic structures of same type and that their endomorphism monoids $\text{End}(A)$ and $\text{End}(A')$ (ring etc) are isomorphic, are then $A$ and $A'$ isomorphic? Several mathematicians have studied this problem for several algebraic structures such as semigroups, groups, Abelian groups etc.

Looking the problem of the determinability of groups by their endomorphism semigroups, we know quite much. Then we have especially diverse information on endomorphisms of Abelian groups, because the endomorphisms of an Abelian group form a ring under the composition and the sum, and, therefore, it is possible to use methods of the theory of rings. An excellent overview of the present situation in the theory of endomorphism rings of Abelian groups is given in \cite{3}. In general, for a given group $G$ there exist many groups $H$ such that the semigroups...
End(G) and End(H) are isomorphic, and, for a given Abelian group G there exist many Abelian groups H such that their endomorphism rings End(G) and End(H) are isomorphic.

The class of all quasigroups contains the class of all groups, and, therefore, it is hopeless to describe a quasigroup by its endomorphism monoid in the class of all quasigroups. Probably, it is possible in some subclasses of quasigroups. Although, some authors tried to study endomorphisms and endomorphism monoids of quasigroups. Some aspects of automorphisms of quasigroups were studied by Shcherbacov [10]. His work [9] contains many facts on endomorphisms of quasigroups. Several observations on endomorphisms of linear and alinear quasigroups are made by Tabarov [11]. Nagy and Plaumann [5] characterized the quasigroups in which the left deviation, i.e, the map e(x) = x\backslash x is an endomorphism.

We tried to characterize some classes of medial quasigroups by their endomorphism monoids. In [4], it was proved that if the endomorphism monoids of two finite idempotent medial commutative quasigroups are isomorphic, then these quasigroups are isomorphic. In this paper, we give some further results on endomorphism monoids of some classes of medial quasigroups.

2. Endomorphisms of medial quasigroups

Definition 2.1. A magma (groupoid) \( \langle Q; \cdot \rangle \) is called a quasigroup, if each of the equations \( ax = b \) and \( ya = b \) has a unique solution for any \( a, b \in Q \).

The solutions of these equations will be denoted by \( x = a \backslash b \) and \( y = b/a \), respectively. Since the solutions are unique, one can define the binary operations \( \backslash \) and \( / \) on \( Q \) as follows:

\[
x = a \backslash b \iff ax = b \quad \text{(left division)}, \quad y = b/a \iff ya = b \quad \text{(right division)}
\]

Proposition 2.2 ([2]). If \( Q \) is a quasigroup, then the following identities hold

\[
x \backslash (xy) = x \cdot (x \backslash y) = y = (yx)/x = (y/x) \cdot x
\]

where \( \backslash \) and \( / \) denote the left and right division, respectively.

It follows that the definition of quasigroup can be given in terms of binary operations and identities.

Definition 2.3. A set \( Q \) together with binary operations \( \cdot, \backslash, / \), is called a quasigroup if it satisfies the identities (2.2)

Definitions 2.1 and 2.3 are equivalent [2].

It follows from Proposition 2.2 that the mappings \( L_a, R_b: Q \to Q \), defined by \( L_a(x) = ax \), \( R_b(x) = xb \), are bijective. Therefore, to each quasigroup \( Q \) one can associate the subgroup \( \text{Mlt}(Q) \), generated by all mappings \( L_a \) and \( R_b \) \( a, b \in Q \) in the group of all bijections \( Q \to Q \).

The group \( \text{Mlt}(Q) \) is called a multiplication group of the quasigroup \( Q \).

Definition 2.4. The mapping \( \varphi: Q \to Q \) is called an endomorphism of a quasigroup \( Q \), if \( \varphi \) preserves the binary operation \( \cdot \), that is \( \varphi(x \cdot y) = \varphi(x) \cdot \varphi(y) \) for all \( x, y \in Q \).

Applying an endomorphism \( \varphi \) to \( y = x \cdot (x \backslash y) \), we obtain \( \varphi(y) = \varphi(x \cdot (x \backslash y)) = \varphi(x) \cdot \varphi(x \backslash y) \).

Dividing by \( \varphi(x) \) from the left, we have that \( \varphi(x \backslash y) = \varphi(x) \backslash \varphi(y) \) i.e \( \varphi \) preserves the left division. Similarly, one can show that \( \varphi \) preserves right division as well.

We denote by \( \text{End}(Q) \) and \( \text{Aut}(Q) \) the sets of all endomorphisms and all automorphisms (i.e, invertible endomorphisms) of a quasigroup \( Q \), respectively. Obviously, the set \( \text{End}(Q) \) is a monoid with respect to the composition of mappings and \( \text{Aut}(Q) \) is a subgroup of \( \text{End}(Q) \).

Definition 2.5. A quasigroup \( Q \) is called medial (or entropic) if it satisfies the identity \( (xy)(zw) = (xz)(yw) \).
Let $Q$ be a quasigroup and $\varphi, \psi \in \text{End}(Q)$. Let us define the map $\varphi \circ \psi : Q \to Q$ as follows:

$$(\varphi \circ \psi)(x) = \varphi(x)\psi(x), \quad x \in Q$$

Endomorphisms $\varphi$ and $\psi$ are called summable, if $\varphi \circ \psi$ is an endomorphism, too. It is easy to check that each two endomorphisms of a medial quasigroup are summable, i.e, the situation is similar to the Abelian groups (recall that, all endomorphisms of Abelian groups are summable).

We define left and right division on $\text{End}(Q)$ elementwise, i.e,

$$(\varphi \circ \psi)(x) = \varphi(x)/\psi(x), \quad (\varphi \circ \psi)(x) = \varphi(x) \setminus \psi(x), \quad \forall \varphi, \psi \in \text{End}(Q), \quad x \in Q$$

Proposition 2.6. If $Q$ is a medial quasigroup, then for all $\varphi, \psi \in \text{End}(Q)$ the mappings $\varphi \circ \psi$ and $\varphi \circ \psi$ are endomorphisms of $Q$.

Proof. Really, if $x, y \in Q$ and $\varphi, \psi \in \text{End}(Q)$, we have, by (2.2) and mediality,

$$(\varphi \circ \psi)(xy) = \varphi(x)/\psi(x) = (\varphi(x)\varphi(y))/((\psi(x)\psi(y))$$

$$= [(\varphi(x)/\psi(x)) \cdot (\varphi(y)/\psi(y))]/(\psi(x)\psi(y))$$

$$= [(\varphi(x)/\psi(x)) \cdot (\varphi(y)/\psi(y))]/(\psi(x)\psi(y))$$

$$= \varphi(x)/\psi(x) \cdot (\varphi(y)/\psi(y)) = (\varphi \circ \psi)(x) \cdot (\varphi \circ \psi)(y), \quad \varphi \circ \psi \in \text{End}(Q)$$

Similarly, $\varphi \circ \psi \in \text{End}(Q)$.

The connection between Abelian groups and medial quasigroups is given by Toyoda’s theorem ([2], Theorem 2.10): If $Q$ is a medial quasigroup, then there exist an Abelian group $\langle Q; +, -, 0 \rangle$, its commuting automorphisms $\varphi$ and $\psi$, and an element $c \in Q$ such that

$$x \cdot y = \varphi(x) + \psi(y) + c$$

This Abelian group $\langle Q; +, -, 0 \rangle$ is called an underlying Abelian group of the medial quasigroup $Q$.

It is well-known that, if $G$ is an Abelian group, then $\text{End}(G)$ is a ring with respect to the addition and composition $\circ$ of endomorphisms. Next we demonstrate that the situation is somehow similar in the case of medial quasigroups.

Proposition 2.7. Let $Q$ be a medial quasigroup. Then

(i) $\langle \text{End}(Q); \circ, \oplus, \circ \rangle$ is a medial quasigroup,

(ii) the following (distributivity) identities hold:

$$\varphi \circ (\psi \circ \eta) = (\varphi \circ \psi) \circ (\varphi \circ \eta), \quad (\psi \circ \eta) \circ \varphi = (\psi \circ \varphi) \circ (\eta \circ \varphi)$$

$$\varphi \circ (\psi \circ \eta) = (\varphi \circ \psi) \circ (\varphi \circ \eta), \quad (\psi \circ \eta) \circ \varphi = (\psi \circ \varphi) \circ (\eta \circ \varphi)$$

Proof. To prove the first part, use Definition 2.3. Thus, it is sufficient to prove identities (2.2). Let $\varphi, \psi \in \text{End}(Q)$ and $x \in Q$. Then

$$[(\varphi \circ \psi)(x) \cdot \psi(x) = \varphi(x)/\psi(x) \cdot \psi(x) = \varphi(x)$$

i.e we have $(\varphi \circ \psi) \circ \psi = \varphi$. The rest of the identities can be proved analogously. Hence $\langle \text{End}(Q); \circ, \oplus, \circ \rangle$ is a quasigroup. Mediality follows from the immediate calculations:

$$[(\varphi \circ \psi) \circ (\chi \circ \pi)](x) = (\varphi \circ \psi)(x) \cdot (\chi \circ \pi)(x) = [\varphi(x)\psi(x)](\chi(x)\pi(x)$$
To prove the second part, check the distributivity identities. Let \( \varphi, \psi, \chi, \pi \in \text{End}(Q) \) and \( x \in Q \). Then we have

\[
[\varphi \circ (\psi \odot \eta)](x) = \varphi(\psi(x) \cdot \eta(x)) = \varphi(\psi(x)) \cdot \eta(x) = [(\varphi \circ \psi) \odot (\varphi \circ \eta)](x)
\]

i.e, \( \varphi \circ (\psi \odot \eta) = (\varphi \circ \psi) \odot (\varphi \circ \eta) \). The remaining five distributivity identities can be verified similarly.

3. **Endomorphisms of idempotent medial quasigroups**

Let \( Q \) be a quasigroup. To each \( x \in Q \) we associate the constant mapping \( \pi_x : Q \rightarrow \{ x \} \). The map \( \pi_x \) is an endomorphism of \( Q \). Let us denote by \( 0_Q \) the set of all constant mappings \( \pi_x : Q \rightarrow \{ x \} \), i.e, \( 0_Q = \{ \pi_x | x \in Q \} \). Since \( \pi_x \pi_y = \pi_x (x, y \in Q) \), the set \( 0_Q \) is a subsemigroup of the monoid \( \text{End}(Q) \).

**Definition 3.1.** A quasigroup \( Q \) is called idempotent if the identity \( xx = x \) holds in \( Q \).

**Proposition 3.2.** If \( Q \) is an idempotent quasigroup, then the subsemigroup \((0_Q; \odot)\) coincides with the semigroup of left-zeroes in \( \text{End}(Q) \).

**Proof.** Let \( \varphi \in \text{End}(Q) \) and \( \pi_x \in 0_Q \). Then, for each \( y \in Q \), we have

\[
(\pi_x \circ \varphi)(y) = \pi_x(\varphi(y)) = x = \pi_x(y)
\]

i.e, \( \pi_x \) is a left-zero. Therefore \((0_Q; \odot)\) is a subsemigroup of left-zeroes.

Conversely, suppose that an endomorphism \( \psi \) is left-zero in \( \text{End}(Q) \). Thus \( \psi \circ \pi_x = \psi \) for each \( x \in Q \). Let \( x \in Q \) be fixed. If \( y \in Q \), then we have

\[
\psi(y) = (\psi \circ \pi_x)(y) = \psi(x)
\]

i.e, \( \psi \) is a constant mapping. Therefore, each left-zero in \( \text{End}(Q) \) is a constant mapping.

Proposition 3.2 implies that the mapping \( \Psi : Q \rightarrow 0_Q, \Psi(x) = \pi_x \), is bijective. Hence, we have the following corollary.

**Corollary 3.3.** If the endomorphism monoid of an idempotent quasigroup \( Q \) is finite, then \( Q \) is finite, too.

Recall that, for groups we have the similar result [1]: If the endomorphism monoid of a group \( G \) is finite, then \( G \) is finite, too.

**Proposition 3.4.** Let \( Q \) be a medial idempotent quasigroup. Then

(i) the quasigroup \( Q \) is distributive, i.e, the following identities hold in \( Q \):

\[
x(yz) = (xy)(xz), \quad (xy)z = (xz)(yz)
\]

(ii) the multiplication group \( \text{Mlt}(Q) \) is a subgroup in \( \text{Aut}(Q) \),

(iii) the quasigroup \((0_Q; \odot)\) is isomorphic to \((Q; \cdot)\).
Proof. Assume that $Q$ is a medial idempotent quasigroup. Since
\[ x(yz) = (xx)(yz) = (xy)(xz), \quad (xy)z = (xy)(zz) = (xz)(yz), \quad \forall x, y, z \in Q \]
the quasigroup $Q$ is distributive.

The identities $x(yz) = (xy)(xz)$ and $(xy)z = (xz)(yz)$ imply that the mappings $L_a(x) = ax$ and $R_b(x) = xb$ are endomorphisms of $Q$. Since $a/(ax) = x$ and $(xb)/b = x$, we have that $L_a$ and $R_b$ are invertible, i.e., $L_a$ and $R_b$ are automorphisms. Therefore, Mlt($Q$) is an isomorphic group of $\operatorname{Aut}(Q)$, because the generators of Mlt($Q$) are automorphisms of $Q$.

To prove that $(0_Q; \circ)$ is isomorphic to $(Q; \cdot)$, consider a map $\Psi: Q \to 0_Q$ defined by $\Psi(x) = \pi_x$. Clearly, $\Psi$ is injective. By Proposition 3.2, $\Psi$ is surjective. Hence $\Psi$ is bijective. If we show that $\Psi$ is a homomorphism, then the proof is complete. Let $x, y \in Q$. Then
\[(\Psi(x) \circ \Psi(y))(z) = (\pi_x \circ \pi_y)(z) = \pi_x(z) \cdot \pi_y(z) = x \cdot y = \pi_{x \cdot y}(z) = (\Psi(x \cdot y))(z), \quad \forall z \in 0_Q \]

Corollary 3.5. If $Q$ is an idempotent medial quasigroup, then $(\operatorname{End}(Q); \circ)$ is also an idempotent medial quasigroup.

Proof. Let $\varphi \in \operatorname{End}(Q)$ and $x \in Q$. Then
\[(\varphi \circ \varphi)(x) = \varphi(x) \cdot \varphi(x) = \varphi(x) \quad \Rightarrow \quad \varphi \circ \varphi = \varphi \quad \forall \varphi \in \operatorname{End}(Q)\]
Mediality of $(\operatorname{End}(Q); \circ)$ follows from Proposition 2.7. \hfill \Box

Theorem 3.6. Suppose that $Q$ and $Q'$ are idempotent medial quasigroups. If $(\operatorname{End}(Q); \circ, \circ, \circ, \circ)$ and $(\operatorname{End}(Q'); \circ, \circ', \circ', \circ)$ are isomorphic, then $Q$ and $Q'$ are isomorphic, too.

Proof. Let
\[ \Phi: (\operatorname{End}(Q); \circ, \circ, \circ, \circ) \to (\operatorname{End}(Q'); \circ, \circ', \circ', \circ') \]
be an isomorphism. The isomorphism $\Phi$ induces an isomorphism $\Phi_{|0_Q}$ of the subsemigroups $(0_Q; \circ)$ and $(0_Q'; \circ)$ of left-zeroes of End($Q$) and End($Q'$), respectively. By Proposition 3.4, we have isomorphisms of quasigroups $\Psi: Q \to 0_Q$ and $\Psi': Q' \to 0_{Q'}$. Hence $\Psi'^{-1} \circ \Phi_{|0_Q} \circ \Psi$ is the isomorphism $Q \to Q'$. \hfill \Box

4. Endomorphisms of commutative idempotent medial quasigroups

In this section we restrict ourselves to the commutative idempotent medial quasigroups (IMC-quasigroups for short).

Proposition 4.1. A quasigroup $Q$ is an IMC-quasigroup iff there exists an Abelian group $(Q, +)$ such that the mapping $2: Q \to Q$, where $2(x) = x + x$, $x \in Q$, is an automorphism of $(Q, +)$ and $x \cdot y = 2^{-1}(x + y)$.

Proof. Let $Q$ be an IMC-quasigroup. By Toyoda’s theorem, there exist an Abelian group $(Q; +)$, its commuting automorphisms $\phi$ and $\psi$, and an element $c \in Q$ such that
\[ x \cdot y = \phi(x) + \psi(y) + c, \quad x, y \in Q \]
Since the group $Q$ is commutative, we have
\[ \phi(x) + c = \phi(x) + \psi(0) + c = x \cdot 0 = 0 \cdot x = \phi(0) + \psi(x) + c = \psi(x) + c \]
i.e., $\phi = \psi$. The idempotency implies
\[ x = x \cdot x = \phi(x) + \phi(x) + c = (2 \circ \phi)(x) + c \]
Therefore,
\[ 0 = (2 \circ \phi)(0) + c = c, \quad 1_Q(x) = x = (2 \circ \phi)(x), \quad 2 \circ \phi = 1_Q \]
Since $\phi$ is an automorphism of the group $Q$, the map $2$ is an automorphism, too, and, we have $\phi = 2^{-1}$. Finally,
\[ x \cdot y = \phi(x) + \psi(y) + c = \phi(x) + \phi(y) = \phi(x + y) = 2^{-1}(x + y) \]
Conversely, if $x \cdot y = 2^{-1}(x + y)$, then it is straightforward to check that $Q$ is an IMC-quasigroup.

Hence, any IMC-quasigroup is uniquely determined by its underlying Abelian group. Next corollary gives a complete description of finite Abelian groups which are the underlying Abelian groups of IMC-quasigroups.

It is well-known that the mapping $2$ is an automorphism of a finite Abelian group $(Q, +)$ if and only if $(Q, +)$ is of odd order. Hence, there does not exist finite IMC-quasigroups of even order. Combining the Proposition 4.1 with the properties of automorphism $2$, we get the following corollary.

**Corollary 4.2.** Let $Q$ be an IMC-quasigroup and $Q^+$ the underlying Abelian group. Then each endomorphism of the group $Q^+$ is an endomorphism of the quasigroup $Q$.

**Proof.** Really, if $\eta$ is an endomorphism of the underlying Abelian group, then
\[ (2 \circ \eta)(x) = \eta(x) + \eta(x) = \eta(x + x) = (\eta \circ 2)(x), \quad \forall x \in Q \]
and, therefore, $2 \circ \eta = \eta \circ 2$. Since $2$ is invertible, we obtain $\eta \circ 2^{-1} = 2^{-1} \circ \eta$. Hence
\[ \eta(x) \cdot \eta(y) = 2^{-1}(\eta(x)) + 2^{-1}(\eta(y)) = \eta(2^{-1}(x)) + \eta(2^{-1}(y)) = \eta(x \cdot y) \]
for each $x, y \in Q$, i.e. $\eta \in \text{End}Q$.

Let $Q$ and $Q'$ be finite IMC-quasigroups such that their endomorphism monoids are isomorphic. By Corollary 3.3, the corresponding underlying Abelian groups $Q^+$ and $Q'^+$ are finite, too. P. Puusemp proved (see [8, Theorem 4.2]) that if two finite Abelian groups have the isomorphic endomorphism monoids, then these groups are also isomorphic. Therefore, if we can show that the isomorphism between monoids $\text{End}(Q^+)$ and $\text{End}(Q'^+)$ follows from the isomorphism $\text{End}(Q) \cong \text{End}(Q')$, then the underlying Abelian groups are isomorphic and the quasigroups are isomorphic, too. The rest of the section is dedicated to prove that from $\text{End}(Q) \cong \text{End}(Q')$ implies $\text{End}(Q^+) \cong \text{End}(Q'^+)$.

Assume that $Q$ is an IMC-quasigroup and $Q^+$ its underlying Abelian group. Let us consider the following binary operation $\oplus_k$ on $Q$:
\[ x \oplus_k y = L_k^{-1}(x \cdot y) = k \setminus (xy), \quad \forall x, y \in Q, \quad k \in Q \]
Since $(Q, \cdot)$ is commutative, the magma $(Q, \oplus_k)$ is commutative, too.

**Proposition 4.3.** The magma $(Q, \oplus_k)$ is an Abelian group with the identity element $k$ and the inverse element of $x$ is $k/x$.
Let us define underlying Abelian group. Really, if

\[ L \]

Proposition 4.5. The Abelian groups

Corollary 4.4. We start the proof by showing that \( k \) is the identity element. Let \( x \in Q \). Then

\[ x \oplus_k k = k \oplus_k x = k \backslash (kx) = x \]

Next we prove the associativity of \( \oplus_k \). Let \( x, y, z \in Q \). Then

\[ x \oplus_k (y \oplus_k z) = (x \oplus_k k) \oplus_k (y \oplus_k z) = L_k^{-1}((x \oplus_k k) \cdot (y \oplus_k z)) = L_k^{-1}\left(L_k^{-1}(x \cdot k) \cdot (y \cdot z)\right) = L_k^{-1}(L_k^{-1}(x \cdot y) \cdot (k \cdot z)) = L_k^{-1}(L_k^{-1}(x \cdot y) \cdot L_k^{-1}(k \cdot z)) = L_k^{-1}((x \oplus_k y) \cdot (k \oplus_k z)) = (x \oplus_k y) \oplus_k (k \oplus_k z) = (x \oplus_k y) \oplus_k z \]

Finally, the inverse element of \( x \) is \( k/x \). Indeed, due to the commutativity of \((Q, \cdot)\), we have \( k/x = x \backslash k \) and

\[ x \oplus_k (k/x) = (k/x) \oplus_k x = k \backslash (k/x \cdot x) = k \backslash k = k \]

Corollary 4.4. For each \( k \in Q \), \( L_k \) is an automorphism of \((Q, \oplus_k)\) and \( L_k^{-1}(x) = 2_k(x) = x \oplus_k x \).

Proof. Really,

\[ L_k(x \oplus_k y) = x \cdot y = k \backslash (k \cdot xy) = k \backslash (k^2 \cdot xy) = k \backslash (kx \cdot ky) = L_k(x) \oplus_k L_k(y) \]

Therefore, \( L_k \) is an automorphism of \((Q, \oplus_k)\). Since \((Q, \cdot)\) is an idempotent quasigroup, we have

\[ x = x \cdot x = L_k(x \oplus_k x) = L_k(x) \oplus_k L_k(x) = (2_k \circ L_k)(x) \quad \Rightarrow \quad 2_k = L_k^{-1} \]

Proposition 4.5. The Abelian groups \((Q, \oplus_k)\) and \((Q, \oplus_l)\) are isomorphic for each \( k, l \in Q \).

Proof. First we observe that the binary operation \( \oplus_0 \) coincides with the addition in the underlying Abelian group. Really, if \( x, y \in Q \), then

\[ x \oplus_0 y = 0 \backslash (xy) = 2(xy) - 0 = 2\left(2^{-1}(x + y)\right) = x + y \]

Let us define \( \psi_k : Q \rightarrow Q \) by \( \psi_k(x) = x + k \). Clearly, \( \psi_k \) is bijective and

\[ \psi_k(x) \oplus_k \psi_k(y) = (x + k) + (y + k) - k = (x + y) + k = \psi_k(x + y), \quad \forall x, y \in Q \]

Hence \( \psi_k \) is an isomorphism from \((Q, +)\) to \((Q, \oplus_k)\).

Corollary 4.6. Let \( k \in Q \). Then each endomorphism of the group \((Q, \oplus_k)\) is an endomorphism of the quasigroup \( Q \).

The proof is similar to the proof of Corollary 4.2 and therefore is omitted.

We denote further the group \((Q, \oplus_k)\) by \( Q^{\oplus_k} \). The submonoid \( \text{End}(Q^{\oplus_k}) \) of \( \text{End}(Q) \) contains the identity mapping and only one constant map \( \pi_k \). For each \( k \in Q \), denote by \( M(k) \) the set of all submonoids \( M \) in \( \text{End}(Q) \) such that

\[ M \in M(k) \leftrightarrow (\{\pi_k, 1_Q\} \subseteq M) \wedge (M \cap 0_Q = \{\pi_k\}) \]

Thus \( M(k) \) is non-empty, because it contains \( \text{End}(Q^{\oplus_k}) \). By Zorn’s lemma, \( M(k) \) contains the maximal element, denoted by \( M_k \).

Proposition 4.7. The endomorphism monoid \( \text{End}(Q^{\oplus_k}) \) coincides with the submonoid \( M_k \) of \( \text{End}(Q) \).
Proof. Let $\varphi \in M_k$. Since $\varphi \circ \pi_k \in M_k$, we have

$$(\varphi \circ \pi_k)(x) = \varphi(k) = \pi_k(x), \quad x \in Q$$

Hence $\pi_k(x) \in M_k \cap Q$, i.e., $\pi_k(x) = \pi_k$ and $\varphi(k) = k$. Next show that $M_k \subseteq \text{End}(Q^\oplus_k)$. Let $\varphi \in M_k$ and $x, y \in Q$. Then

$$\varphi(x \oplus_k y) = \varphi(k \setminus xy) = \varphi(k) \setminus (\varphi(x) \varphi(y)) = k \setminus (\varphi(x) \varphi(y)) = \varphi(x) \oplus_k \varphi(y).$$

Therefore, $\varphi \in \text{End}(Q^\oplus_k)$ and $M_k \subseteq \text{End}(Q^\oplus_k) \subseteq \text{End} Q$. Since $\text{End}(Q^\oplus_k) \in \mathcal{M}(k)$, we have $M_k = \text{End}(Q^\oplus_k)$. \qed

**Theorem 4.8.** Let $Q$ and $Q'$ be IMC-quasigroups and $Q$ is finite. If the endomorphism monoids $\text{End}(Q)$ and $\text{End}(Q')$ are isomorphic, then the quasigroups $Q$ and $Q'$ are isomorphic as well.

**Proof.** Assume that $Q$ and $Q'$ are IMC-quasigroups and $Q$ is finite. Suppose that the monoids $\text{End}(Q)$ and $\text{End}(Q')$ are isomorphic, and let $\Gamma: \text{End}(Q) \rightarrow \text{End}(Q')$ be the corresponding isomorphism. By Corollary 3.3, $Q'$ is finite, too. We write $\boxtimes$ and $\boxplus$ for the multiplication in $Q'$ and addition in the underlying Abelian group of $Q'$, respectively. Since both $Q$ and $Q'$ are IMC-quasigroups, we have, by Proposition 4.1,

$$x \cdot y = 2^{-1}(x + y) \quad \text{and} \quad x' \cdot y' = 2^{-1}(x' \boxplus y'), \quad \forall x, y \in Q, \quad x', y' \in Q'$$

The monoids $\text{End}(Q^+)$ and $\text{End}(Q'^\boxtimes)$ are submonoids in $\text{End}(Q)$ and $\text{End}(Q')$, respectively.

Next we show that the monoids $\text{End}(Q^+)$ and $\text{End}(Q'^\boxtimes)$ are isomorphic. Propositions 4.5 and 4.7 imply that $\text{End}(Q^+) = M_0 \cong M_k$ for each $k \in Q$. Let $M$ be the maximal submonoid of $\text{End}(Q)$ such that $M \cap 0_Q = \{\pi_k\}$ for some $k \in Q$. Thus $M \cong \text{End}(Q^+)$. Therefore, the image of $M$ under $\Gamma$ is a maximal submonoid in $\text{End}(Q')$ containing only one constant endomorphism. Hence, by Propositions 4.5 and 4.7, $\Gamma(M) \cong \text{End}(Q'^\boxtimes)$, and, finally,

$$\text{End}(Q^+) \cong M \cong \Gamma(M) \cong \text{End}(Q'^\boxtimes) \quad \Rightarrow \quad \text{End}(Q^+) \cong \text{End}(Q'^\boxtimes)$$

Since $Q^+$ and $Q'^\boxtimes$ are finite Abelian groups, the isomorphism $\text{End}(Q^+) \cong \text{End}(Q'^\boxtimes)$ implies an isomorphism $Q^+ \cong Q'^\boxtimes$ ([8], Theorem 4.2). Let $\xi: Q \rightarrow Q'$ be the corresponding isomorphism. From immediate computations we obtain $2^{-1} \circ \xi = \xi \circ 2^{-1}$. Let $x, y \in Q$. Then

$$\xi(x) \boxtimes \xi(y) = 2^{-1}(\xi(x) \boxplus \xi(y)) = (2^{-1} \circ \xi)(x + y) = (\xi \circ 2^{-1})(x + y) = \xi(x \cdot y).$$ \qed

**5. An example of a quasigroup not determined by its endomorphism monoid.**

In this section we present an example of idempotent medial quasigroup that is not determined by its endomorphism monoid. Let the underlying abelian group be $C_5$ which we regard as an additive group of integers modulo 5. Define two additional binary operations $*$ and $\cdot$ on $C_5$:

$$x * y \equiv 2x + 4y \mod 5, \quad x \cdot y \equiv 3x + 3y \mod 5$$

Since the mappings $x \mapsto ax \mod 5$ are automorphisms of $C_5$ for each $a \in \{2, 3, 4\}$, $*$ and $\cdot$ are quasigroup operations on $C_5$. The quasigroups $(C_5, *)$ and $(C_5, \cdot)$ are non-isomorphic, because the quasigroup $(C_5, \cdot)$ is commutative but $(C_5, *)$ is not.

Next we show that $\text{End}(C_5, *) = \text{End}(C_5, \cdot)$. Let $\varphi \in \text{End}(C_5, \cdot)$. Since $\varphi(x \cdot 0) = \varphi(x) \cdot \varphi(0)$, we get

$$\varphi(3x) \equiv 3\varphi(x) + 3\varphi(0) \mod 5$$
Hence,
\[ \varphi(x \ast y) = \varphi(2x + 4y \pmod{5}) = \varphi(3(4x + 3y) \pmod{5}) = \varphi(4x \cdot 3y) \]
\[ = \varphi(4x) \cdot \varphi(3y) = 3[\varphi(4x) + \varphi(3y)] \pmod{5} \]
\[ = 3[\varphi(3 \cdot 3x) + 3\varphi(y) + 3\varphi(0)] \pmod{5} \]
\[ = 4\varphi(3x) + 4\varphi(y) + 3\varphi(0) \pmod{5} \]
\[ = 4[3\varphi(x) + 3\varphi(0)] + 4\varphi(y) + 3\varphi(0) \pmod{5} \]
\[ = 2\varphi(x) + 4\varphi(y) \pmod{5} \]
\[ \equiv \varphi(x) \ast \varphi(y) \]

i.e., \( \text{End}(C_5, \bullet) \subseteq \text{End}(C_5, \ast) \). Let us suppose now \( \tau \in \text{End}(C_5, \ast) \). After expanding the equalities \( \tau(x \ast 0) = \tau(x) \ast \tau(0) \) and \( \tau(0 \ast x) = \tau(0) \ast \tau(x) \), we have

\[ \tau(2x) \equiv 2\tau(x) + 4\tau(0) \pmod{5} \quad \text{and} \quad \tau(4x) \equiv 4\tau(x) + 2\tau(0) \pmod{5} \]

Compute

\[ \tau(x \bullet y) = \tau(3x + 3y \pmod{5}) = \tau(2 \cdot 4x + 4 \cdot 2y \pmod{5}) = \tau(4x \ast 2y) \]
\[ = \tau(4x) \ast \tau(2y) = 2\tau(4x) + 4\tau(2y) \pmod{5} \]
\[ = 2 \cdot 4\tau(x) + 2 \cdot 2\tau(0) + 4 \cdot 2\tau(y) + 4 \cdot 4\tau(0) \pmod{5} \]
\[ = 3\tau(x) + 3\tau(y) \pmod{5} \]

Hence \( \tau \in \text{End}(C_5, \bullet) \) and, therefore, \( \text{End}(C_5, \ast) \subseteq \text{End}(C_5, \bullet) \). We have proved that \( \text{End}(C_5, \ast) = \text{End}(C_5, \bullet) \). Therefore, the endomorphism monoids \( \text{End}(C_5, \ast) \) and \( \text{End}(C_5, \bullet) \) are isomorphic, but the quasigroups \( (C_5, \ast) \) and \( (C_5, \bullet) \) are not.

Therefore, the following quasigroups are not determined by their endomorphism monoid:

- the idempotent medial quasigroups in the class of idempotent medial quasigroups,
- medial quasigroups in the class of (medial) quasigroups,
- distributive quasigroups in the class of (distributive) quasigroups,
- left distributive quasigroups in the class of (left distributive) quasigroups,
- idempotent quasigroups in the class of (idempotent) quasigroups,
- commutative quasigroups in the class of quasigroups.

References

[9] Shechterbav V A 2009 J. Gen. Lie Theory Appl. 3 197
[10] Shechterbav V A 1991 Mat. Issled. 120 104 (Russian)