DEMONSTRATIO MATHEMATICA
Vol. XLIV No 3 2011

10.1515/dema-2013-0328

E. Nazari, Yu. M. Movsisyan

TRANSITIVE MODES

Abstract. In this paper the connection between the right (left) invertible medial algebras and the right (left) group of binary operations is studied. As a consequence, we prove the structure results for transitive modes.

1. Introduction

The n-ary operation A on the set Q is called idempotent if it satisfies the identity $A(x, \ldots, x) = x$. An algebra $(Q; \Sigma)$ is called idempotent, if every operation $A \in \Sigma$ is idempotent.

Let A be n-ary and B be m-ary operations on the set Q. The pair (A, B) is called medial (possibly abelian, entropic, bisymmetric, bicommutative, etc.) if it satisfies the identity:

$$A\left(B(x_{11}, \ldots, x_{1m}), \ldots, B\left(x_{n1}, \ldots, x_{nm}\right)\right) = B(A(x_{11}, \ldots, x_{n1}), \ldots, A\left(x_{1m}, \ldots, x_{nm}\right)).$$

In the case of the binary operations A, B we have the identity:

$$A\left(B(x, y), B\left(u, v\right)\right) = B(A(x, u), A\left(y, v\right)).$$

An operation A on the set Q is called medial if the pair (A, A) is medial. In the case of one binary operation, we have [1, 7]:

$$A\left(A(x, y), A\left(u, v\right)\right) = A\left(A(x, u), A(y, v)\right).$$

An algebra $(Q; \Sigma)$ is called medial, if the pair (A, B) is medial for every $A, B \in \Sigma$ [6, 8] (for algebras without nullary operations). In other words, an algebra $(Q; \Sigma)$ is called medial if $(Q; \Sigma)$ satisfies the hyperidentity of mediality (abelity) [11]. An idempotent and medial algebra is called a mode [18].

The paper contains seven chapters. In chapter 2 some preliminary results are proved. In chapter 3 some preliminary concepts are introduced. In

2010 *Mathematics Subject Classification*: 20N05, 08A05, 03C05.
Key words and phrases: medial algebra, mode, right (left) invertible algebra, right (left) group of binary operation, transitive mode.

chapter 4 the connection between the right (left) invertible medial binary algebras and the right (left) group of binary operations is studied. In chapter 5 the concept of transitive mode is introduced and some auxiliary results are proved. In chapter 6 a structure theorem for transitive modes is proved. In the last chapter some open problems are formulated.

2. Preliminary results

The first well known result on medial algebras concerns medial quasigroups and is called Toyoda theorem [5, 21]: *For every medial quasigroup $Q(\cdot)$ there exists an abelian group $Q(+)$ such that the operation $(\cdot)$ is determined by the rule:*

$$x \cdot y = \varphi x + c + \psi y,$$

where $\varphi, \psi \in Aut\, Q(+)$ and $c \in Q$.

The next result is more general [12]:

Theorem 2.1. *If the pair (A, B) of binary quasigroup operations on the set Q is medial, then there is an abelian group $Q(+)$ such that the operations A, B are determined by the rules:*

$$A(x, y) = \varphi_1 x + c_1 + \psi_1 y,$$
$$B(x, y) = \varphi_2 x + c_2 + \psi_2 y,$$

where $c_1, c_2 \in Q$ and $\varphi_1, \varphi_2, \psi_1, \psi_2 \in Aut\, Q(+)$.

Proof. Indeed, if the quasigroup operations $A_1, A_2, A_3, A_4, A_5, A_6$ on the set Q satisfy the identity:

$$A_1(A_2(x, y), A_3(u, v)) = A_4(A_5(x, u), A_6(y, v)),$$

then there exists an abelian group $Q(+)$ such that:

$$A_1(x, y) = \alpha x + \tau y, \qquad A_4(x, y) = \mu x + \sigma y,$$
$$A_2(x, y) = \alpha^{-1}(\gamma x + \delta y), \quad A_5(x, y) = \mu^{-1}(\gamma x + \lambda y),$$
$$A_3(x, y) = \tau^{-1}(\lambda x + \beta y), \quad A_6(x, y) = \sigma^{-1}(\delta x + \beta y),$$

for every $x, y \in Q$ [2]. We have: $A_1 = A_5 = A_6 = A$ and $A_2 = A_3 = A_4 = B$. So $A_1(x, y) = A_5(x, y)$ and $A_1(x, y) = A_6(x, y)$, i.e.

$$\alpha x + \tau y = \mu^{-1}(\gamma x + \lambda y),$$
$$\alpha x + \tau y = \sigma^{-1}(\delta x + \beta y),$$

for every $x, y \in Q$. Thus:

$$\mu(\alpha x + \tau y) = \gamma x + \lambda y,$$
$$\sigma(\alpha x + \tau y) = \delta x + \beta y,$$

i.e.

$$\mu(x+y) = \gamma(\alpha^{-1}x) + \lambda(\tau^{-1}y),$$
$$\sigma(x+y) = \delta(\alpha^{-1}x) + \beta(\tau^{-1}y).$$

It follows from these equalities:

$$\gamma\left(\alpha^{-1}x\right) = \mu(x) + \left(-\lambda(\tau^{-1}0)\right),$$
$$\lambda\left(\tau^{-1}y\right) = \left(-\gamma(\alpha^{-1}0)\right) + \mu(y),$$
$$\delta\left(\alpha^{-1}x\right) = \sigma(x) + \left(-\beta(\tau^{-1}0)\right),$$
$$\beta(\tau^{-1}y) = \left(-\delta\left(\alpha^{-1}0\right)\right) + \sigma(y).$$

Hence,

$$\mu(x+y) = \mu(x) + (-\mu 0) + \mu(y)$$

and

$$\sigma(x+y) = \sigma(x) + (-\sigma 0) + \sigma(y),$$

for every $x, y \in Q$, where $0 \in Q$ is the identity element of the group $Q(+)$ i.e. the bijections $\mu, \sigma : Q \to Q$ are holomorphisms of the group $Q(+)$ ([9], Chapter IV, § 1; [11], Chapter 0, § 5). So the mappings $\varphi_2(x) = \mu(x)+(-\mu 0)$ and $\psi_2(x) = (-\sigma 0) + \sigma(x)$ are automorphisms of the group $Q(+)$. Hence, $\mu(x) = \varphi_2(x) + \mu 0$ and $\sigma(x) = \sigma 0 + \psi_2(x)$ where $\varphi_2, \psi_2 \in Aut\, Q(+)$. So

$$A_4(x,y) = \mu x + \sigma y = \varphi_2(x) + \mu 0 + \sigma 0 + \psi_2(y) =$$
$$= \varphi_2(x) + c_2 + \psi_2(y) = B(x,y),$$

where $c_2 = \mu 0 + \sigma 0$. For $A(x,y)$ we have the similar proof taking into account the equalities $A_2 = A_4$ and $A_3 = A_4$. ■

As a consequence, we get the following characterization (also see [20]):

Corollary 2.2. *If $(Q;\Sigma)$ is a binary medial algebra with quasigroup operations, then there exists an abelian group $Q(+)$ such that every operation $A_i \in \Sigma$ is determined by the rule:*

$$A_i(x,y) = \varphi_i x + c_i + \psi_i y,$$

where $c_i \in Q$ and $\varphi_i, \psi_i \in Aut\, Q(+)$. Moreover, if the algebra $(Q;\Sigma)$ also is idempotent (is a mode), then

$$A_i(x,y) = \varphi_i x + \psi_i y,$$

where $\varphi_i, \psi_i \in Aut\, Q(+)$ and $\varphi_i, \psi_i \in Aut\,(Q;\Sigma)$.

Proof. Namely, if $A_0 \in \Sigma$ is a fixed operation, then by Toyoda theorem A_0 is principally isotopic to the abelian group operation $+$ on Q. If $B \in \Sigma$ is any operation, then the pair (A_0, B) is medial, hence A_0 and B are principally isotopic to the abelian group operation $*$ on Q. Thus, any operation B is principally isotopic to the same abelian group operation + by transitivity of isotopy. So

$$A_0(x,y) = \alpha x + \tau y = A_1(x,y) = A_5(x,y) = A_6(x,y),$$

and for any operation $B \in \Sigma$ we have:

$$B(x,y) = \mu x + \sigma y = A_2(x,y) = A_3(x,y) = A_4(x,y).$$

Hence, for every $x, y \in Q$ we have:

$$B(x,y) = \varphi x + t + \psi y,$$

where $\varphi, \psi \in Aut\, Q(+)$ and $t \in Q$ according to the proof of the previous theorem. For the idempotent case we have: $t = 0$ and $\varphi x = B(x,0)$, $\psi y = B(0,y)$. Hence, $\varphi, \psi \in Aut\,(Q;\Sigma)$. For instance:

$$\begin{aligned}\varphi A(x,y) &= B(A(x,y),0) = B(A(x,y),A(0,0)\\ &= A(B(x,0),B(y,0)) = A(\varphi x,\varphi y).\end{aligned}$$ ■

Remark 2.3. From the proof of Theorem 2.1 also follows the result:

If the binary quasigroup operations A, B_1, B_2 and C on the set Q satisfy the identity:

$$A(B_1(x,y), B_2(u,v)) = C(A(x,u), A(y,v)),$$

then there exists an abelian group $Q(+)$ such that the operation C is determined by the rule:

$$C(x,y) = \varphi x + c + \psi y,$$

where $\varphi, \psi \in Aut\, Q(+)$ and $c \in Q$.

3. Preliminary concepts

The set of all binary operations defined on the set Q is denoted by $\mathcal{F}_Q^2$ and we consider the following two operations on this set:

$$\begin{aligned}A \cdot B(x,y) &= A(x, B(x,y)),\\ A \circ B(x,y) &= A(B(x,y),y),\end{aligned}$$

where $A, B \in \mathcal{F}_Q^2$, $x, y \in Q$. These operations $(\cdot)$ and $(\circ)$ are called the right and left multiplications of binary operations (functions), and they were studied in the works of various authors [3, 4, 13–16, 19, 22, 23].

The set $\mathcal{F}_Q^2$ forms a monoid under the right (and left) multiplication of binary operations. These two semigroups are isomorphic. The identity element of the semigroup $\mathcal{F}_Q^2(\cdot)$ is $E \in \mathcal{F}_Q^2$ and it is defined by the rule: $E(x,y) = y$; and the identity element of the semigroup $\mathcal{F}_Q^2(\circ)$ is $F \in \mathcal{F}_Q^2$ and it is defined by the rule: $F(x,y) = x$. The mapping $A \to A^*$ is the isomorphism of these two semigroups, where $A^*(x,y) = A(y,x)$.

The set of idempotent binary operations on Q is a subsemigroup in the semigroups $\mathcal{F}_Q^2(\cdot)$ and $\mathcal{F}_Q^2(\circ)$.

The binary operation $A \in \mathcal{F}_Q^2$ is the right (left) invertible one if the equation $A(a,x) = b$ ($A(y,a) = b$) has a unique solution $x \in Q$ ($y \in Q$) for every $a, b \in Q$. The unique solutions $x, y \in Q$ are usually denoted by $x = A^{-1}(a,b)$ and $y =^{-1} A(b,a)$. Hence,

$$A \cdot A^{-1} = A^{-1} \cdot A = E\,,$$

for the right invertible operation A and we have:

$$^{-1}A \circ A = A \circ^{-1} A = F,$$

for the left invertible operation A. The operation A^{-1} (or ^{-1}A) is the right (or left) inverse one for the right (left) invertible operation $A \in \mathcal{F}_Q^2$. It is evident that A^{-1} (or ^{-1}A) is right (or left) invertible, and:

$$(A^{-1})^{-1} = A =^{-1} (^{-1}A), \quad (A^{-1})^* =^{-1} (A^*), \quad (^{-1}A)^* = (A^*)^{-1}.$$

The binary operation $A \in \mathcal{F}_Q^2$ is invertible, if it is right and left invertible. In this case:

$$\left(^{-1}\left(A^{-1}\right)\right)^{-1} =^{-1} \left(\left(^{-1}A\right)^{-1}\right) = A^*\,.$$

For example:

$$\left(^{-1}\left(A^{-1}\right)\right)^{-1}(x,y) = z \;\leftrightarrow\; ^{-1}\left(A^{-1}\right)(x,z) = y \;\leftrightarrow\; A^{-1}(y,z) = x \;\leftrightarrow\; A(y,x) = z \leftrightarrow A^*(x,y) = z.$$

On the applications of right (left) invertible operations in axiomatic characterization of geometric structures and equivalency problem in knot theory see [10, 17].

The set of all right (left) binary invertible operations on the set Q is denoted by $\mathcal{F}_Q^r$ (and $\mathcal{F}_Q^\ell$).

The set $\mathcal{F}_Q^r$ is a group under the right multiplication of binary operations. The set $\mathcal{F}_Q^\ell$ is a group under the left multiplication of binary operations. These two groups are isomorphic.

The groups $\mathcal{F}_Q^r(\cdot)$ and $\mathcal{F}_Q^\ell(\circ)$ are called the right and left groups of binary operations, respectively.

The binary algebra $(Q;\Sigma)$ is called (right, left) invertible, if every operation $A \in \Sigma$ is (right, left) invertible.

For any right (left) invertible algebra $(Q;\Sigma)$ we define the algebra $(Q;\Sigma^{-1})$ ($(Q;\,^{-1}\Sigma)$), where

$$\Sigma^{-1} = \{A^{-1} |\, A \in \Sigma\}\,,$$
$$^{-1}\Sigma = \{^{-1}A |\, A \in \Sigma\}.$$

So, for any invertible algebra $(Q;\Sigma)$ we have the algebras: $(Q;\Sigma^{-1})$, $(Q;{}^{-1}\Sigma)$, $\left(Q;{}^{-1}(\Sigma^{-1})\right)$, $(Q;({}^{-1}\Sigma)^{-1})$ and $(Q;\Sigma^*)$, where

$$ {}^{-1}\left(\Sigma^{-1}\right) = \{{}^{-1}\left(A^{-1}\right) \mid A \in \Sigma\}, $$
$$ \left({}^{-1}\Sigma\right)^{-1} = \{\left({}^{-1}A\right)^{-1} \mid A \in \Sigma\}, $$
$$ \Sigma^* = \{A^* \mid A \in \Sigma\}. $$

However, the algebra $(Q;\Sigma^*)$ is meaningful for every algebra $(Q;\Sigma)$.

4. Modes and the right (left) group of binary operations

The subgroup of the group $\mathcal{F}_Q^r(\cdot)$ generated by the subset $\Sigma \subseteq \mathcal{F}_Q^r$ is denoted by $(\Sigma)_r$. Similarly, the subgroup of the group $\mathcal{F}_Q^\ell(\circ)$ generated by the subset $\Sigma \subseteq \mathcal{F}_Q^\ell$ is denoted by $(\Sigma)_\ell$.

Lemma 4.1. *If a right invertible algebra $(Q;\Sigma)$ is medial (mode), then the algebra $\left(Q;\Sigma \cup \Sigma^{-1}\right)$ also is medial (mode).*

Proof. For every $A, B \in \Sigma$ and $x, y, u, v \in Q$ there exists an element $v' \in Q$ such that

$$ A^{-1}\left(B(x,y), B(u,v')\right) = B(A^{-1}(x,u), A^{-1}(y,v)). $$

From this equality, we have:

$$ A\left(B(x,y), B\left(A^{-1}(x,u), A^{-1}(y,v)\right)\right) = B(u,v'), $$

and by the mediality:

$$ B\left(A(x, A^{-1}(x,u)), A\left(y, A^{-1}(y,v)\right)\right) = B(u,v'), $$

i.e. $B(u,v) = B(u,v')$ and $v = v'$. So,

$$ A^{-1}\left(B(x,y), B(u,v)\right) = B(A^{-1}(x,u), A^{-1}(y,v)). $$

Hence:

$$ A^{-1}\left(B^{-1}(x,y), B^{-1}(u,v)\right) = B^{-1}(A^{-1}(x,u), A^{-1}(y,v)). \qquad \blacksquare $$

Lemma 4.2. *If the left invertible algebra $(Q;\Sigma)$ is medial (is a mode), then the algebra $\left(Q;\Sigma \cup {}^{-1}\Sigma\right)$ also is medial (is a mode).*

Corollary 4.3. *If the invertible algebra $(Q;\Sigma)$ is medial (is a mode), then the algebra, $(Q;\Sigma \cup \Sigma^{-1} \cup {}^{-1}\Sigma \cup {}^{-1}\left(\Sigma^{-1}\right) \cup \left({}^{-1}\Sigma\right)^{-1} \cup \Sigma^*)$ also is medial (is a mode).*

Lemma 4.4. *If a right invertible algebra $(Q;\Sigma)$ is medial (is a mode), then the extended algebra $(Q;(\Sigma)_r)$ also is medial (is a mode).*

Lemma 4.5. *If a left invertible algebra $(Q;\Sigma)$ is medial (is a mode), then the extended algebra $(Q;(\Sigma)_\ell)$ also is medial (is a mode).*

Example 4.6. If $|Q| = 2$ then the right invertible algebra $(Q; \mathcal{F}^r_Q)$ is medial.

5. Auxiliary results

Following the papers: [13, 14], we call a binary algebra $(Q; \Sigma)$ with the property $E, F \in \Sigma$ transitive if

a) $|Q| \geqslant 2$;
b) for every $a, b, c \in Q$ where $b \neq a$ there exists an operation $A \in \Sigma$ such that $A(a, b) = c$;
c) the algebra $(Q; \Sigma \setminus \{F\})$ is right invertible.

Example 5.1. If $|Q| = 2$ and $\Sigma = \{E, F\}$, then $(Q; \Sigma)$ is a transitive mode.

Example 5.2. Let $Q(\cdot)$ be a nontrivial abelian group and

$$\Sigma^0 = \{A_q |\, A_q(x, y) = y \cdot q,\ q \in Q,\ x, y \in Q\}.$$

If $\Sigma = \Sigma^0 \cup \{F\}$ then $(Q; \Sigma)$ is a medial and transitive algebra. However $(Q; \Sigma)$ is not a mode.

Example 5.3. If $Q(+, \cdot)$ is a field with the identity $e \in Q$,

$$\Sigma = \{A_q |\, A_q(x, y) = qx + (e - q)y,\ q \in Q,\ x, y \in Q\},$$

then $(Q; \Sigma)$ is a transitive mode, where $(Q; \Sigma \setminus \{E, F\})$ is an invertible algebra.

If $Q = \{1, 2\}$ and $\Sigma^0 = \mathcal{F}^r_Q$, $\Sigma = \Sigma^0 \cup \{F\}$ then $(Q; \Sigma)$ is a transitive and medial algebra, and there exists the operation $A \neq E$ such that $A(2, 1) = 1$. However, the following result is valid for transitive modes.

Lemma 5.4. *Let $(Q; \Sigma)$ be a transitive mode and $A \in \Sigma$. If the equation $A(x, a) = a$ has a solution $x \neq a \in Q$ then $A = E$.*

Proof. If $|Q| = 2$ then the idempotent and right invertible operation A is unique: $A = E$. Let $|Q| \geqslant 3$ and the equation $A(x, a) = a$ has a solution $x_0 \neq a$. Let us choose an element $b \in Q$ where $b \neq a,\ x_0$. There exists an operation $B \in \Sigma \setminus \{F\}$, such that $B(a, b) = x_0$ according to the condition of transitivity b). So,

$$\begin{aligned} B(a, a) &= B\left(A(x_0, a), A(x_0, a)\right) = A\left(B(x_0, x_0), B(a, a)\right) \\ &= A\left(x_0, B(a, a)\right) = A\left(B(a, b), B(a, a)\right) = B\left(A(a, a), A(b, a)\right) \\ &= B(a, A(b, a)). \end{aligned}$$

Hence, $a = A(b, a)$ for every $b \neq x_0, a$. However, this equality is also valid for $b = a, x_0$ (because, $A(x_0, a) = a$ and $A(a, a) = a$). Let $c \in Q$ and fix the element $d \neq a, c$. Then there exists an operation $C \in \Sigma \setminus \{F\}$ such that $C(d,a) = c$. Thus:

$$\begin{aligned} c &= C(d,a) = C\left(d, A(b,a)\right) = C\left(A(d,d), A(b,a)\right) \\ &= A\left(C(d,b), C(d,a)\right) = A(C(d,b), c), \end{aligned}$$

for every element $b \in Q$. Hence, $A(u,c) = c$ for every $u, c \in Q$. ■

Corollary 5.5. *If $(Q;\Sigma)$ is a transitive mode, then for every $a,b,c \in Q$ where $b \neq a$ there exists a unique operation $A \in \Sigma$ such that $A(a,b) = c$.*

Proof. Let there exist the two operations $A, B \in \Sigma \setminus \{F\}$ such that $A(a,b) = c$ and $B(a,b) = c$. Consider the group $(\Sigma \setminus \{F\})_r$. The algebra $(Q; (\Sigma \setminus \{F\})_r)$ is medial (and idempotent) by Lemma 4.4. Hence, the algebra $(Q; (\Sigma \setminus \{F\})_r \cup \{F\})$ is a transitive mode and we can apply the previous Lemma 5.4. Thus, we have $A(a,b) = B(a,b)$ and

$$A^{-1}\left(a, A(a,b)\right) = A^{-1}(a, B(a,b)),$$

i.e. $A^{-1} \cdot A(a,b) = A^{-1} \cdot B(a,b)$ and $b = A^{-1} \cdot B(a,b)$. Hence, the equation $A^{-1} \cdot B(x,b) = b$ has a solution $x \neq b$ and it follows that $A^{-1} \cdot B = E$ and $B = A$ by the previous lemma.

If $A = F$ but $B \neq F$ then $B \neq E$ and $B(a,b) = F(a,b) = a$. Hence,

$$B^{-1}(a, B(a,b)) = B^{-1}(a,a) = a$$

and $B^{-1} \cdot B(a,b) = a$ i.e. $E(a,b) = a$ and $b = a$. Contradiction! ■

Corollary 5.6. *If $(Q;\Sigma)$ is a transitive mode and $A(a,b) = B(a,b)$, where $A, B \in \Sigma$, $a, b \in Q$ and $a \neq b$ then $A = B$.*

Corollary 5.7. *If $(Q;\Sigma)$ is a transitive mode, then $(Q;\Sigma)$ is maximal in the following sense: there does not exist a transitive mode $(Q;\Sigma')$ where $\Sigma \subseteq \Sigma'$, $\Sigma \neq \Sigma'$. Hence, $(\Sigma \setminus \{F\})^{-1} \subseteq \Sigma \setminus \{F\}$.*

Proof. If $|Q| = 2$ then $\Sigma = \{E, F\}$ and assertion is valid. Let $|Q| \geqslant 3$ and $(Q;\Sigma')$ also is a transitive mode, where $\Sigma \subseteq \Sigma$ and $\Sigma \neq \Sigma'$. So there exists an operation $A \in \Sigma'$ such that $A \notin \Sigma$. Hence, $A \neq E, F$. Let us prove that there exists a triple of pare-vise distinct elements $a, b, c \in Q$ such that $A(a,b) = c$. Indeed:

1) If for all pairs of distinct elements $a \neq b$ we have: $A(a,b) = a$ then $A = F$;
2) If for all pairs of distinct elements $a \neq b$ we have: $A(a,b) = b$ then $A = E$;
3) If for some pairs of distinct elements $a \neq b$ we have $A(a,b) = b$ and for other pairs of distinct elements $c \neq d$ we have $A(c,d) = c$ then $A = E$ by Lemma 5.4.

Besides, there exists an operation $B \in \Sigma$ such that $B(a,b) = c$ by transitivity of $(Q;\Sigma)$. The algebra $(Q; \Sigma \cup \{A\})$ is also a transitive mode.

Thus, there exists a pair of elements $a \neq b$ in Q and the pair of operations $A, B \in \Sigma_1 \cup \{A\}$ such that $A(a,b) = B(a,b)$ where $\Sigma_1 = \Sigma \setminus \{F\}$. Hence, $A = B$ by Corollary 5.6, and: $A \in \Sigma$. Contradiction! Now the second part of the assertion follows from Lemma 4.1. ∎

Corollary 5.8. *If $(Q;\Sigma)$ is a transitive mode, then $\Sigma \setminus \{F\}$ is an abelian group under the right multiplication of binary functions.*

Proof. The set $\Sigma \setminus \{F\}$ is a group under the right multiplication of binary functions, because $\Sigma\setminus\{F\} = (\Sigma\setminus\{F\})_r$ by maximality of $(Q;\Sigma)$. This group is abelian:

$$\begin{aligned} A \cdot B(x,y) &= A(x, B(x,y)) = A(B(x,x), B(x,y)) \\ &= B(A(x,x), A(x,y)) = B(x, A(x,y)) = B \cdot A(x,y), \end{aligned}$$

for every $A, B \in \Sigma \setminus \{F\}$. ∎

Theorem 5.9. *Let $|Q| \geqslant 3$ and $(Q;\Sigma)$ be a transitive mode. Then every operation $A \in \Sigma \setminus \{F\}$, $A \neq E$ is left invertible. Hence,*

$$^{-1}(\Sigma \setminus \{E\}) \subseteq \Sigma \setminus \{E\}, \quad \left(^{-1}(\Sigma \setminus \{E,F\})\right)^{-1} \subseteq \Sigma \setminus \{E,F\},$$

$$^{-1}((\Sigma \setminus \{E,F\})^{-1}) \subseteq \Sigma \setminus \{E,F\}, \quad (\Sigma \setminus \{E,F\})^{*} \subseteq \Sigma \setminus \{E,F\}.$$

The set $\Sigma \setminus \{E\}$ is closed under the left multiplication of binary functions.

Proof. Since $A \neq E, F$ then there are pair-wise distinct elements $a, b, c \in Q$ such that $A(a,b) = c$. Hence, the equation $A(x,b) = c$ has a solution $x = a$.

Consider the equation $A(x,b) = p$, where $p \neq c, b$ (since in the cases $p = c, b$ a solution exists). There is an operation $B \in \Sigma \setminus \{F\}$ such that $B(b,c) = p$. So,

$$B(b,c) = B\left(A(b,b), A(a,b)\right) = A\left(B(b,a), B(b,b)\right) = A\left(B(b,a), b\right) = p,$$

and the solution of the equation $A(x,b) = p$ is an element $B(b,a) \in Q$.

Consider the equation $A(x,q) = p$ where $q \neq b, p$. Let $d \in Q$ and $d \neq b, q$. There is an operation $C \in \Sigma \setminus \{F\}$ such that $C(d,b) = q$. Thus:

$$\begin{aligned} C(d,c) &= C\left(d, A(a,b)\right) = C\left(A(d,d), A(a,b)\right) \\ &= A\left(C(d,a), C(d,b)\right) = A(C(d,a), q). \end{aligned}$$

Thus, if $p = C(d,c)$ then the equation $A(x,q) = p$ has a solution $x = C(d,a)$. If $p \neq C(d,c)$ and since $q \neq C(d,c)$ there is an operation $D \in \Sigma\setminus\{F\}$ such that $D\left(q, C(d,c)\right) = p$. Hence,

$$\begin{aligned} p &= D\left(q, C(d,c)\right) = D\left(q, A(C(d,a), q)\right) = D\left(A(q,q), A(C(d,a), q)\right) \\ &= A\left(D(q, C(d,a)), D(q,q)\right) = A(D(q, C(d,a)), q), \end{aligned}$$

and the equation $A(x,q) = p$ also has a solution in the case $p \neq C(d,c)$.

From Lemma 5.4 it follows that the equation $A(x,q) = p$ has a unique solution, where $A \neq E$. Namely, if $q = p$ then the uniqueness of the solution $x = q = p$ follows from Lemma 5.4. If $p \neq q$ and the equation $A(x,q) = p$ has solutions $x_0 \neq y_0$ then $q \neq y_0, x_0$ and there is an operation $T \in \Sigma \setminus \{F\}$ such that $T(q, x_0) = y_0$. Hence, $T \neq E$ and

$$p = A(y_0, q) = A\left(T(q,x_0), T(q,q)\right) = T\left(A(q,q), A(x_0,q)\right) = \\ = T\left(q, A(x_0,q)\right) = T(q,p).$$

It follows from Lemma 5.4 that $T = E$. Contradiction!

The last part of the assertion is valid according to Corollary 4.3, Lemmas: 4.4, 4.5, and Corollary 5.7 about maximality of $(Q;\Sigma)$. ∎

6. The structure result

Let $(Q;\Sigma)$ be a transitive mode and let $|Q| \geqslant 3$. Then $\Sigma \setminus \{E,F\} \neq \emptyset$. Consider $B \in \Sigma \setminus \{E,F\}$ and $0 \in Q$. According to Theorem 5.9, the operation B is invertible, medial, idempotent and:

$$A\left(B(x,y), B(u,v)\right) = B(A(x,u), A(y,v)),$$

for every $A \in \Sigma$. According to Corollary 2.2, we have: $B(x,y) = \varphi x + \psi y$ where

$$x + y = B(^{-1}B(x,0), B^{-1}(0,y)), \quad \varphi x = B(x,0), \quad \psi y = B(0,y),$$

and

$$A(\varphi x + \psi y, \varphi u + \psi v) = \varphi A(x,u) + \psi A(y,v) = A(\varphi x, \varphi u) + A(\psi y, \psi v),$$

i.e.

$$A(x+y, u+v) = A(x,u) + A(y,v).$$

Theorem 6.1. *If $(Q;\Sigma)$ is a transitive mode, then there exists a field $Q(+,\cdot)$ such that every operation $A \in \Sigma$ is defined by the rule:*

$$A(x,y) = (e-a)x + ay,$$

where e is the identity element of the field and $a \in Q$ (and depends on A).

Proof. If $|Q| = 2$ then the assertion is evident, because in this case $\Sigma = \{E,F\}$. Let $|Q| \geqslant 3$. Let us define the addition as above, while we define the multiplication by the following way. Let e be a fixed element of Q and let $e \neq 0$. For every element $x \in Q$ there exists an operation $A_x \in \Sigma$ such that $x = A_x(0,e)$ (if $x = 0, e$ we have: $A_x = F, E$). The mapping $\Phi : x \to A_x$ is a bijection from Q to Σ by Corollary 5.6. We define: $x \cdot y = A_x(0,y)$ where $A_x = \Phi(x)$. Then we prove the field axioms. For example:

$$x \cdot y = A_{x\cdot y}(0,e), \quad x \cdot y = A_x(0,y) = A_x\left(0, A_y(0,e)\right) = A_x \cdot A_y(0,e),$$

and according to Corollary 5.6, we have: $A_x \cdot A_y = A_{x \cdot y}$; then $\Phi(x \cdot y) = \Phi(x) \cdot \Phi(y)$, hence $x \cdot y = A_x(0, y)$ is associative and commutative. For every operation $A = A_a \in \Sigma$ we have:

$$A(x, y) = A(x + 0, 0 + y) = A(x, 0) + A(0, y),$$
$$A(x, x) = A(x, 0) + A(0, x) = x.$$

So $A(x, 0) = x - A(0, x)$ hence:

$$\begin{aligned} A(x, y) &= A(x, 0) + A(0, y) = x - A(0, x) + A(0, y) = x - ax + ay \\ &= (e - a)x + ay, \end{aligned}$$

where $a = A(0, e)$. ∎

7. Open problems

An algebra $(Q; \Sigma)$ is called three-medial if the subalgebra of the algebra $(Q; \Sigma)$ generated by any three elements $a, b, c \in Q$ is medial.

Problem 7.1. *Characterize medial transitive algebras.*

Problem 7.2. *Characterize three-medial invertible algebras.*

Problem 7.3. *Characterize three-medial transitive algebras.*

Problem 7.4. *Characterize three-medial, idempotent and transitive algebras.*

Thanks to the referee for useful remarks.

References

[1] J. Aczel, J. Dhombres, *Functional Equations in Several Variables*, Cambridge University Press, Cambridge, New York, New Rochelle, Melburne, Sydney, 1991.

[2] J. Aczel, V. D. Belousov, M. Hosszu, *Generalized associativity and bisymmetry on quasigroups*, Acta Math. Acad. Sci. Hungar. 11 (1960), 127–136.

[3] V. D. Belousov, *Systems of quasigroups with generalized identities*, Uspekhi. Mat. Nauk 20 (1965), 75–146. [English transl. in Russian Math. Surveys 20 (1965), 73–143.]

[4] S. L. Bloom, Z. Esik, E. G. Manes, *A Cayley theorem for bolean algebras*, Amer. Math. Monthly 97 (1990), 831–833.

[5] R. H. Bruck, *Contributions to the theory of loops*, Trans. Amer. Math. Soc. 60 (1946), 245–354.

[6] T. Evans, *Properties of algebras almost equivalent to identities*, J. London Math. Soc. 35 (1962), 53–59.

[7] J. Ježek, T. Kepka, *Medial Groupoids*, Praha, 1983.

[8] A. G. Kurosh, *General Algebra*, Nauka, 1974 (Russian).

[9] S. Maclane, *Homology*, Die Grundlehren der Mathematischen Wissenschaften, Band 114, Springer-Verlag.

[10] S. V. Matveev, *Distributive groupoids in knot theory*, Mat. Sb. 119(1) 1982, 78–88. [English transl. in Mathematics of the USSR-Sbornik 47(1), 1984.]

[11] Yu. M. Movsisyan, *Introduction to the Theory of Algebras with Hyperidentities*, Yerevan State University Press, 1986 (Russian).

[12] Yu. M. Movsisyan, *Generalization of Toyoda theorem*, Loops'99, Praha, July 27-August 1, 1999, 26–27.

[13] Yu. M. Movsisyan, *The multiplicative group of field and hyperidentities*, Izv. Akad. Nauk SSSR Ser. Mat. 53 (1989), 1040–1055. [English transl. in Math. USSR Izvestiya 35 (1990), 337–391.]

[14] Yu. M. Movsisyan, *Hyperidentities in algebras and varieties*, Uspekhi Mat. Nauk 53(1) (1998), 61–114. English transl. in Russian Mathematical Surveys 53(1) (1998), 57–108.

[15] Yu. M. Movsisyan, *Binary representations of algebras with at most two binary operations. A Cayley theorem for distributive lattices*, Int. J. Algebr. Comput. 19(1) (2009), 97–106.

[16] R. Padmanabhan, P. Penner, *Lattice ordered polynomial algebras*, Order 15 (1998), 75–86.

[17] V. Pambuccian , *Euclidean geometry problems rephrased in terms of midpoints and point-reflections*, Elem. Math. 60 (2005), 19–24.

[18] A. B. Romanowska, J. D. H. Smith, *Modes*, Singapore: World Scientific, 2002.

[19] S. K. Stein, *On the foundation of quasigroups*, Trans. Amer. Math. Soc. 85 (1957), 228–256.

[20] M. M. Stronkowski, *Cancelation in entropic algebras*, Algebra Universalis 60 (2009), 439–468.

[21] K. Toyoda, *On axioms of linear functions*, Proc. Imp. Acad. Tokyo 17 (1941), 221–227.

[22] K. Urbanik, *On algebraic operations in idempotent algebras*, Colloquium Math. 13 (1965), 129–157.

[23] K. A. Zaretskii, *Abstract characteristics of bisemigroups of binary operations*, Matematicheskie Zametki 1(5) (1967), 525–530.

E. Nazari
PAYAME NOOR UNIVERSITY
GASERSHERIN, IRAN
E-mail: nazari_ibrahim2008@yahoo.com

Yu. M. Movsisyan
DEPARTMENT OF MATHEMATICS AND MECHANICS
YEREVAN STATE UNIVERSITY
0025, YEREVAN, ARMENIA

E-mail: yurimovsisyan@yahoo.com

Received October 3, 2010; revised version February 25, 2011.