Schauffler-Like Theorems for Medial and Paramedial Algebras

Yu. M. Movsisyan & D.N. Harutyunyan

Yerevan State University

ABSTRACT

In [1], the endolinearity of regular division binary algebras satisfying second-order associativity identities was shown. Furthermore, schauffler-like theorems were proven for these algebras. This paper aims to establish similar results for regular division binary algebras satisfying second-order identities of mediality or paramediality.

Keywords: $\forall \exists (\forall)$-identities; division regular groupoids; schauffler theorem; quasiendomorphisms.

Classification: MSC 2010: 03C05, 03C85, 20N05

Language: English

Great Britain Journals Press

LJP Copyright ID: 925611
Print ISSN: 2631-8490
Online ISSN: 2631-8504

London Journal of Research in Science: Natural and Formal

Volume 23 | Issue 11 | Compilation 1.0

Schauffer-like Theorems for Medial and Paramedical Algebras

Yu. M. Movsisyan[α] & D.N. Harutyunyan[σ]

ABSTRACT

In [1], the endolinearity of regular division binary algebras satisfying second-order associativity identities was shown. Furthermore, schauffler-like theorems were proven for these algebras. This paper aims to establish similar results for regular division binary algebras satisfying second-order identities of mediality or paramediality.

Keywords: $\forall \exists (\forall)$-identities; division regular groupoids; schauffler theorem; quasiendomorphisms.

Author: Yerevan State University, Yerevan, Armenia.

I. INTRODUCTION

We call $Q(\cdot)$ the division(cancelation) groupoid if for any $a \in Q$ the left and right multiplications are surjections(injections), if the groupoid is both division and cancellation then it's called quasigroup. If $Q(\cdot)$ is a division(cancellation) groupoid, then its operation is called a divisible(cancellable) operation. A binary algebra $(Q;\Sigma)$ is called division(cancellation) if each operation $A \in \Sigma$ is a divisible operation and it's called invertible algebra if it's both division and cancellable algebra. We call a groupoid $(Q;\cdot)$ left-regular if $ca = cb \implies Ra = Rb$, where $a, b, c \in Q$. Similarly, we define the right-regular groupoid. We call a groupoid regular if it is simultaneously left-regular and right-regular. If $Q(\cdot)$ is a regular groupoid, then its operation is called regular. A binary algebra $(Q;\Sigma)$ is referred to as regular if each operation $A \in \Sigma$ is a regular operation. We say that a groupoid $(Q;A)$ is homotopic to a groupoid $(Q;B)$ if there exist such mappings $\alpha, \beta, \gamma : Q \implies Q$ that the equality $\gamma A(x,y) = B(\alpha x, \beta y)$ holds for any $x, y \in Q$ [2,3]. Then the triple (α, β, γ) is called a homotopy from $(Q;A)$ to $(Q;B)$. If $\gamma = id_Q$, then the groupoids are called principally homotopic. If α, β, γ are surjective mappings, then the groupoids are called epitopic or principally epitopic, respectively. We say that an algebra $(Q;\Sigma)$ is homotopic (epitopic) to a groupoid $(Q;\cdot)$ if for each $A \in \Sigma$ the groupoid $(Q;A)$

London Journal of Research in Science: Natural and Formal

is homotopic (epitopic) to the groupoid $(Q;\cdot)$. In the same manner we define the principal homotopy (epitopy) of an algebra $(Q;\Sigma)$ to a groupoid $(Q;\cdot)$. An algebra $(Q;\Sigma)$ is referred to as r-algebra if it is regular, division, and there exists at least one invertible operation $A \in \Sigma$. A binary algebra $(Q;\Sigma)$ is called left(right)-linear on a groupoid $(Q;\cdot)$ if each its operation is left (right) linear on the groupoid $(Q;\cdot)$, that is, for each operation $A \in \Sigma$ there exists an automorphism ϕ_A of the groupoid $(Q;\cdot)$ and a permutation α_A of the set Q such that:

$$A(x,y) = \phi x \cdot \alpha y,$$
$$(A(x,y) = \alpha x \cdot \phi y)$$

binary algebra $(Q;\Sigma)$ is called linear (endolinear) on a groupoid $(Q;\cdot)$ if each its operation is linear (endolinear) on the groupoid $(Q;\cdot)$, that is, for each operation $A \in \Sigma$ there exist automorphisms(endomorphisms) ϕ_A and $\quad_A$ of the groupoid $(Q;\cdot)$ and an element $t_A \in Q$ such that

$$A(x,y) = (\phi_A x \cdot t_A) \cdot \quad_A y$$

for any $x, y \in Q$.

During World War II, while working at the German cryptographic center, Schauffler obtained applications In Cryptography using invertible algebras that satisfy second-order identities, through proving the following theorem. [4–6]

Theorem 1.1 (Schauffler)**.** *Let Q be a non-empty set. The following propositions are equivalent:*

- *For all $(Q;X)$, $(Q;Y)$ quasigroups, there exist $(Q;X')$, $(Q;Y')$ quasigroups, such that following $\forall\exists(\forall)$-identity holds:*

$$\forall X, Y \exists X', Y' \forall x, y, z (X(Y(x,y),z) = X'(x, Y'(y,z))), \quad (1.1)$$

- *For all $(Q;X)$, $(Q;Y)$ quasigroups, there exist $(Q;X')$, $(Q;Y')$ quasigroups, such that following $\forall\exists(\forall)$-identity holds:*

London Journal of Research in Science: Natural and Formal

$$\forall X, Y \exists X', Y' \forall x, y, z (X(x, Y(y, z)) = X'(Y'(x, y), z)), \quad (1.2)$$

- $|Q| \leq 3$

In the [7] proved schauffler-like theorem for other second-order identities and hyperintensities (see [8–10]).

Theorem 1.2. *(Movsisyan) Let Q be non empty set. The following propositions are equivalent:*

- *for all $(Q; X)$, $(Q; Y)$ quasigroups, there exist $(Q; X')$, $(Q; Y')$ quasigroups, such that (1.1) identity holds,*
- *for all $(Q; X)$, $(Q; Y)$ quasigroups, there exist $(Q; X')$, $(Q; Y')$ quasigroups, such that (1.2) identity holds,*
- *for all $(Q; X)$, $(Q; Y)$ loops, there exist $(Q; X')$, $(Q; Y')$ quasigroups, such that (1.1) identity holds,*
- *for all $(Q; X)$, $(Q; Y)$ loops, there exist $(Q; X')$, $(Q; Y')$ quasigroups, such that (1.2) identity holds,*
- *for all $(Q; X)$, $(Q; Y)$ loops, there exist $(Q; X')$, $(Q; Y')$ loops, such that (1.1) identity holds,*
- *for all $(Q; X)$, $(Q; Y)$ loops, there exist $(Q; X')$, $(Q; Y')$ loops, such that (1.2) identity holds,*
- *following hyperidentity holds in the $(Q; L_Q)$ algebra:*

$$X(x, Y(y, z)) = X(Y(x, y), z),$$

- *following hyperidentity holds in the $(Q; L_Q)$ algebra:*

$$X(x, Y(y, z)) = X(Y(x, y), z),$$

- *For all $(Q; X)$ quasigroup, there exist $(Q; X')$, $(Q; Y')$ quasigroups, such that following $\forall\exists(\forall)$-identity holds:*

$$\forall X \exists X', Y' \forall x, y, z (X(X(x, y), z) = X'(x, Y'(y, z))), \quad (1.3)$$

London Journal of Research in Science: Natural and Formal

- *For all* $(Q;X)$ *quasigroup, there exist* $(Q;X')$, $(Q;Y')$ *quasigroups, such that following* $\forall\exists(\forall)$*-identity holds:*

$$\forall X\exists X',Y'\forall x,y,z(X(x,X(y,z))=X'(Y'(x,y),z)), \tag{1.4}$$

- $|Q|\leq 3$,

where L_Q *is the set of all loop-operations over the set* Q*.*

In [11] it was proved that an invertible algebra $(Q;\Sigma)$ with the formula (1.1) or (1.2) is linear on the group. In this paper, we will prove that r-algebras with second-order formulas of mediality and paramediality are endolinear on the group.

II. PRELIMANRY RESULTS

Definition 1. *A mapping* $\phi : Q \implies Q$ *is called quasiendomorphism of a group* $(Q;\cdot)$ *if* $\phi(x\cdot y)=\phi x\cdot(\phi 1)^{-1}\cdot\phi y$ *for all* $x,y\in Q$*,where* 1 *is the unity of the group* $(Q;\cdot)$*.If* ϕ *is also a bijection from* Q *to* Q*,then* ϕ *is called the quasi-automorphism of the group* $(Q;\cdot)$*.*

Lemma 2.1. *Each quasiendomorphism* ϕ *of a group* $(Q;\cdot)$ *has the form* $\phi=L_a\phi'$*,where* $L_ax=a\cdot x$, $a\in Q$, *and* ϕ' *is an endomorphism of the group* $(Q;\Delta)$*. The converse is valid: if* ϕ *is an endomorphism of a group* $(Q;\cdot)$*, then an arbitrary mapping* $\phi'=L_a\phi$ *from* Q *to* Q *is a quasiendomorphism of the group* $(Q;\cdot)$*.*

Proof. Suppose that $\phi 1=k$. We show that $\phi'=L_{k^{-1}}\phi$ is an endomorphism. We have

$$\phi'(ab)=L_{k^{-1}}\phi(ab)=k^{-1}\cdot\phi a\cdot(\phi 1)^{-1}\cdot\phi b=(k^{-1}\cdot\phi a)\cdot(k^{-1}\cdot\phi b)=\phi' a\cdot\phi' b.$$

Lemma 2.2. *Suppose that* $(Q;\cdot)$ *is a group and* α *is the principal epitopy of this group. Then* α *is a surjective quasiendomorphism of this group; moreover, if*

$$\alpha(x \cdot y) = \beta x \cdot \gamma y, \tag{2.5}$$

then β and γ are also quasiendomorphisms.

Proof. Making the successive replacements in the (2.5): (1) $x = 1$, (2) $y = 1$, and (3) $x = y = 1$, we obtain

$$\alpha y = \beta 1 \cdot \gamma y, \;\; x = \beta x \cdot \gamma 1, \;\; \alpha 1 = \beta 1 \cdot \gamma 1. \tag{2.6}$$

We transform equality (2.5), taking into account equalities (2.6):

$$\alpha(x \cdot y) = \alpha x \cdot (\gamma 1)^{-1} \cdot (\beta 1)^{-1} \cdot \alpha y = \alpha x \cdot (\beta 1 \cdot \gamma 1)^{-1} \cdot \alpha y = \alpha x \cdot (\alpha 1)^{-1} \cdot \alpha y,$$

that is, α is a quasiendomorphism.

From (2.5) we also have

$$\beta(x \cdot y) = \alpha(x \cdot y) \cdot (\gamma 1)^{-1} = \alpha x \cdot (\alpha 1)^{-1} \cdot (\alpha y \cdot (\gamma 1)^{-1}) =$$
$$(\alpha x \cdot (\gamma 1)^{-1}) \cdot (\beta 1)^{-1} \cdot \beta y = \beta x \cdot (\beta 1)^{-1} \cdot \beta y.$$

In the same manner, we prove that γ is a quasiendomorphism of the group $(Q; \cdot)$.

Lemma 2.3. *[12] If a loop $(Q; \circ)$ is principally homotopic to a group $(Q; \cdot)$, then they are isomorphic. If a group $(Q; \circ)$ is principally homotopic to a group $(Q; \cdot)$, then they are isomorphic.*

Theorem 2.3. *[12] Let the set Q form a division groupoid under the six operations $A_i(x; y)$ (for $i = 1, ..., 6$) and A_1 or A_4 is regular operation. If these operations satisfy the following equation:*

$$A_1(A_2(x, y), A_3(u, v)) = A_4(A_5(x, u), A_6(y, v)), \tag{2.7}$$

for all elements $x, y, u, v \in Q$, then there exists an operation $(\cdot)$ under which Q forms an abelian group and all these six division

groupoids are epitopic to the group $(Q;\cdot)$ *and there exist eight surjective mappings* $\alpha, \beta, \gamma, \delta, \lambda, \sigma, \phi, \psi$ *of* Q *onto itself such that:*

$$\begin{aligned} A_1(x,y) &= \alpha x \cdot \phi y, \\ \alpha A_2(x,y) &= \gamma x \cdot \delta y, \\ \phi A_3(x,y) &= \lambda x \cdot \beta y, \\ A_4(x,y) &= \psi x \cdot \sigma y, \\ \psi A_5(x,y) &= \gamma x \cdot \lambda y, \\ \sigma A_6(x,y) &= \delta x \cdot \beta y. \end{aligned}$$

The abelian group $(Q;\cdot)$ *is unique up to isomorphisms.*

Theorem 2.4. *[12] Let the set* Q *form a division groupoid under the six operations* $A_i(x;y)$ *(for* $i = 1, ..., 6$*) and* A_1 *or* A_4 *is regular operation. If these operations satisfy the following paramedial equation:*

$$A_1(A_2(x,y), A_3(u,v)) = A_4(A_5(v,y), A_6(u,x)) \tag{2.8}$$

for all elements $x, y, u, v \in Q$*, then there exists an operation* $(\cdot)$ *under which* Q *forms an abelian group, and all these six division groupoids are epitopic to the group* $(Q;\cdot)$ *and there exist eight surjective mappings* $\alpha, \beta, \gamma, \delta, \lambda, \sigma, \phi, \psi$ *of* Q *onto itself such that:*

$$\begin{aligned} A_1(x,y) &= \alpha x \cdot \phi y, \\ \alpha A_2(x,y) &= \gamma x \cdot \delta y, \\ \phi A_3(x,y) &= \lambda x \cdot \beta y, \\ A_4(x,y) &= \sigma x \cdot \psi y, \\ \sigma A_5(x,y) &= \beta x \cdot \delta y, \\ \psi A_6(x,y) &= \lambda x \cdot \gamma y. \end{aligned}$$

The abelian group $(Q;\cdot)$ *is unique up to isomorphisms.*

III. ENDO LINEAR REPRESENTATIONS

Theorem 3.5. *Suppose that $(Q;\Sigma)$ is an r-algebra. If for arbitrary $X,Y \in \Sigma$ there exist $X',Y',Z' \in \Sigma$ such that the following identity of mediality holds:*

$$X(Y(x,y),Y(u,v)) = X'(Y'(x,u),Z'(y,v)), \tag{3.9}$$

then there exist an abelian group $(Q;\cdot)$ such that an arbitrary operation $X \in \Sigma$ is endolinear over the group $(Q;\cdot)$. The group $(Q;\cdot)$ is determined uniquely up to isomorphism.

Proof. Let $X \in \Sigma$ be invertable operation, then from the theorem 2.3 we will have that exists operations $X_1, X_2, X_3 \in \Sigma$ and abelian group $(Q;\cdot)$ such that following identities hold:

$$\begin{aligned} X(x,y) &= \alpha x \cdot \phi y, \\ \alpha X(x,y) &= \gamma x \cdot \delta y, \\ \phi X(x,y) &= \lambda x \cdot \beta y, \\ X_1(x,y) &= \psi x \cdot \sigma y, \\ \psi X_2(x,y) &= \gamma x \cdot \lambda y, \\ \sigma X_3(x,y) &= \delta x \cdot \beta y. \end{aligned}$$

Since X is invertible operation, then we will have that α and β are bijections, moreover:

$$\alpha(\alpha x \cdot \phi y) = \gamma x \cdot \delta y,$$

from which we will obtain:

$$\alpha(x \cdot y) = \gamma\alpha^{-1}x \cdot \delta\phi^{-1}y,$$

This means that α is quasiautomorphism of the group $(Q;\cdot)$.

Lets fix operation X, for every operation Y exists operations $X',Y',Z' \in \Sigma$ such that(3.9) identity holds, and then from the theorem 2.3 we will have that exist abelian group $(Q;\cdot_Y)$ such that those identities hold:

$$
\begin{aligned}
X(x,y) &= \alpha_Y x \cdot_Y \phi_Y y,\\
\alpha_Y Y(x,y) &= \gamma_Y x \cdot_Y \delta_Y y,\\
\phi_Y Y(x,y) &= \lambda_Y x \cdot_Y \beta_Y y,\\
X'(x,y) &= \ {}_Y x \cdot_Y \sigma_Y y,\\
{}_Y Y'(x,y) &= \gamma_Y x \cdot_Y \lambda_Y y,\\
\sigma_Y Z'(x,y) &= \delta_Y x \cdot_Y \beta_Y y.
\end{aligned}
$$

From the proof of the theorem 2.3 we can construct the group $(Q;\cdot_Y)$ in such way that $\alpha_Y = \alpha$.

We have that: $X(x,y) = \alpha x \cdot_Y \phi_Y y = \alpha x \cdot \phi y$, which is the same as: $x \cdot_Y y = x \cdot \phi h_{\phi_Y} y$, where h_{ϕ_Y} is right inverse of ϕ_Y.

We have for every operation $Y \in \Sigma$ the following identity is true:

$$
\begin{aligned}
\alpha Y(x,y) = \gamma_Y x \cdot_Y \delta_Y y = \gamma_Y x \cdot \delta_Y \phi h_{\phi_Y} y \implies\\
Y(x,y) = \alpha^{-1}(\gamma_Y x \cdot \delta_Y \phi h_{\phi_Y} y).
\end{aligned}
$$

Since the set of all quasiautomorphisms of the group is also a group, then α^{-1} will also be quasiautomorphisms, which means:

$$
Y(x,y) = \alpha^{-1}\gamma_Y x \cdot (\alpha^{-1}e)^{-1} \cdot \alpha^{-1}\delta_Y \phi h_{\phi_Y} y = \alpha^{-1}\gamma_Y x \cdot L_{(\alpha^{-1}e)^{-1}}\alpha^{-1}\delta_Y \phi h_{\phi_Y} y,
$$

where $e \in Q$ is the identity element of the group $(Q;\cdot)$, $L_{(\alpha^{-1}e)^{-1}}$ is left translation of the group $(Q;\cdot)$ with the $(\alpha^{-1}e)^{-1}$ element.

We obtained that for every opreation $Y \in \Sigma$ there exists surjections ν_Y and μ_Y, such that $Y(x,y) = \nu_Y x \cdot \mu_Y y$. This means we can rewrite the representations of the operations X, Y, X', Y', Z' in the following way.

$$
\begin{cases}
X(x,y) = \alpha_X x \cdot \beta_X y,\\
Y(x,y) = \alpha_Y x \cdot \beta_Y y,\\
X'(x,y) = \alpha_{X'} x \cdot \beta_{X'} y,\\
Y'(x,y) = \alpha_{Y'} x \cdot \beta_{Y'} y,\\
Z'(x,y) = \alpha_{Z'} x \cdot \beta_{Z'} y,
\end{cases}
$$

where $\alpha_X, \alpha_Y, \alpha_{X'}, \alpha_{Y'}, \alpha_{Z'}, \beta_X, \beta_Y, \beta_{X'}, \beta_{Y'}, \beta_{Z'}$ are surjections.

By doing the replacements in the identity (3.9) we will obtain:

$$\alpha_X(\alpha_Y x \cdot \beta_Y y) \cdot \beta_X(\alpha_Y u \cdot \beta_Y v) = \alpha_{X'}(\alpha_{Y'} x \cdot \beta_{Y'} u) \cdot \beta_{X'}(\alpha_{Z'} y \cdot \beta_{Z'} v).$$

Replacing $x = h_{\alpha_Y} h_{\alpha_X} e$, $y = h_{\beta_Y} e$, $u = h_{\alpha_Y} u$ and $v = h_{\beta_Y} v$, where $h_{\alpha_X}, h_{\alpha_Y}, h_{\beta_Y}$ respectively are the right inverses of the α_X, α_Y, β_Y and e is the identity element of the group $(Q;\cdot)$, we will have:

$$\beta_X(u \cdot v) = \alpha_{X'}(\alpha_{Y'} h_{\alpha_Y} h_{\alpha_X} e \cdot \beta_{Y'} h_{\alpha_Y} u) \cdot \beta_{X'}(\alpha_{Z'} h_{\beta_Y} e \cdot \beta_{Z'} h_{\beta_Y} v) = \mu u \cdot \nu v,$$

where $\mu = \alpha_{X'} L_{\alpha_{Y'} h_{\alpha_Y} h_{\alpha_X} e} \beta_{Y'} h_{\alpha_Y}$ and $\nu = \beta_{X'} L_{\alpha_{Z'} h_{\beta_Y} e} \beta_{Z'} h_{\beta_Y}$. We showed that β_X is quasiendomorphism of the group $(Q;\cdot)$ and from lemma 2.1 we know that there exists ϕ_X endomorphism of the group $(Q;\cdot)$ such that $\beta_X = L_a \phi_X$, where L_a is left translation of the group $(Q;\cdot)$ with the element $a \in Q$. We will have following representation of the arbitrary operation $X \in \Sigma$: $X(x,y) = \alpha_X x \cdot L_a \phi_X y = R_a \alpha_X x \cdot \phi_X y = \sigma_X x \cdot \phi_X y$ where $\sigma_X = R_a \alpha_X$.

By doing following replacements in the identity $x = h_{\alpha_Y} x$, $y = h_{\beta_Y} y$, $u = h_{\alpha_Y} h_{\beta_X} e$ and $v = h_{\beta_Y} e$, we will obtain that $sigma_X$ is also a quasiendomorphism of the group $(Q;\cdot)$ and from lemma 2.1 we know that there exists $_X$ endomorphism of the group $(Q;\cdot)$ such that $\sigma_X = R_b \ _X$, where R_b is right translation of the group $(Q;\cdot)$ with the element $b \in Q$, so we will have:

$$X(x,y) = \phi_X x \cdot b \cdot \ _X y,$$

for every $x, y \in Q$.

Corollary 1. *Suppose that $(Q;\Sigma)$ is an r-algebra. If for arbitrary $X, Y, Z \in \Sigma$ there exist $X', Y', Z' \in \Sigma$ such that the following identity holds:*

$$X(Y(x,y), Z(u,v)) = X'(Y'(x,u), Z'(y,v)), \tag{3.10}$$

then there exist an abelian group $(Q;\cdot)$ such that an arbitrary operation $X \in \Sigma$ is endolinear over the group $(Q;\cdot)$. The group $(Q;\cdot)$ is determined uniquely up to isomorphism.

Corollary 2. *Suppose that $(Q;\Sigma)$ is an r-algebra. If for arbitrary $X, Y \in \Sigma$ there exist $X', Y' \in \Sigma$ such that the following identity holds:*

$$X(Y(x,y),Y(u,v)) = X'(Y'(x,u),Y'(y,v)), \tag{3.11}$$

then there exist an abelian group $(Q;\cdot)$ *such that an arbitrary operation* $X \in \Sigma$ *is endolinear over the group* $(Q;\cdot)$*. The group* $(Q;\cdot)$ *is determined uniquely up to isomorphism.*

Similarly, we can prove the following results.

Theorem 3.6. *Suppose that* $(Q;\Sigma)$ *is an r-algebra. If for arbitrary* $X,Y \in \Sigma$ *there exist* $X',Y',Z' \in \Sigma$ *such that the following identity of paramediality holds:*

$$X(Y(x,y),Y(u,v)) = X'(Y'(v,y),Z'(u,x)), \tag{3.12}$$

then there exists an abelian group $(Q;\cdot)$ *such that an arbitrary operation* $X \in \Sigma$ *is endolinear over the group* $(Q;\cdot)$*. The group* $(Q;\cdot)$ *is determined uniquely up to isomorphism.*

Corollary 3. *Suppose that* $(Q;\Sigma)$ *is an r-algebra. If for arbitrary* $X,Y,Z \in \Sigma$ *there exist* $X',Y',Z' \in \Sigma$ *such that the following identity holds:*

$$X(Y(x,y),Z(u,v)) = X'(Y'(v,y),Z'(u,x)), \tag{3.13}$$

then there exists an abelian group $(Q;\cdot)$ *such that an arbitrary operation* $X \in \Sigma$ *is endolinear over the group* $(Q;\cdot)$*. The group* $(Q;\cdot)$ *is determined uniquely up to isomorphism.*

Corollary 4. *Suppose that* $(Q;\Sigma)$ *is an r-algebra. If for arbitrary* $X,Y \in \Sigma$ *there exist* $X',Y' \in \Sigma$ *such that the following identity holds:*

$$X(Y(x,y),Y(u,v)) = X'(Y'(v,y),Y'(u,x)), \tag{3.14}$$

then there exists an abelian group $(Q;\cdot)$ *such that an arbitrary operation* $X \in \Sigma$ *is endolinear over the group* $(Q;\cdot)$*. The group* $(Q;\cdot)$ *is determined uniquely up to isomorphism.*

Theorem 3.7. *Suppose that* $(Q;\Sigma)$ *is an r-algebra. If for arbitrary* $X,X' \in \Sigma$ *there exist* $Y,Z,Y',Z' \in \Sigma$ *such that* (3.10) *identity of mediality satisfies, then there exists an abelian group* $(Q;\cdot)$ *such*

London Journal of Research in Science: Natural and Formal

that an arbitrary operation $X \in \Sigma$ is endolinear over the group $(Q;\cdot)$. The group $(Q;\cdot)$ is determined uniquely up to isomorphism.

Proof. Lets fix $X' = X$, from the theorem 2.3 we will have that there exists operations $Y_1, Z_1, Y_2, Z_2 \in \Sigma$ and abelian group $(Q;\cdot)$ such that following identities hold:

$$\begin{aligned} X(x,y) &= \alpha x \cdot \phi y, \\ \alpha Y_1(x,y) &= \gamma x \cdot \delta y, \\ \phi Z_1(x,y) &= \lambda x \cdot \beta y, \\ X(x,y) &= \psi x \cdot \sigma y, \\ \psi Y_2(x,y) &= \gamma x \cdot \lambda y, \\ \sigma Z_2(x,y) &= \delta x \cdot \beta y. \end{aligned}$$

Lets fix operation X, and for every opreation $X' \in \Sigma$ we have that there exists opreations $Y, Z, Y', Z' \in \Sigma$ such that identity (3.10) holds, and from the theore 2.3 we will have that there exists $\alpha_{X'}, \beta_{X'}, \gamma_{X'}, \delta_{X'}, \lambda_{X'}, \sigma_{X'}, \phi_{X'}, \psi_{X'} : Q \hookrightarrow Q$ surjections and abelian group $(Q;\cdot_{X'})$ such that following identities hold:

$$\begin{aligned} X(x,y) &= \alpha_{X'} x \cdot_{X'} \phi_{X'} y, \\ \alpha_{X'} Y(x,y) &= \gamma_{X'} x \cdot_{X'} \delta_{X'} y, \\ \phi_{X'} Z(x,y) &= \lambda_{X'} x \cdot_{X'} \beta_{X'} y, \\ X'(x,y) &= \ {}_{X'} x \cdot_{X'} \sigma_{X'} y, \\ {}_{X'} Y'(x,y) &= \gamma_{X'} x \cdot_{X'} \lambda_{X'} y, \\ \sigma_{X'} Z'(x,y) &= \delta_{X'} x \cdot_{X'} \beta_{X'} y. \end{aligned}$$

By doing following replacements $x = h_{\alpha_{X'}} x$ and $y = h_{\phi_{X'}} x$ we will obtain:

$$x \cdot_{X'} y = \alpha h_{\alpha_{X'}} x \cdot \phi h_{\phi_{X'}} y,$$

where $\alpha h_{\alpha_{X'}}$ and $\phi h_{\phi_{X'}}$ are surjections.

We showed that arbitary operations $X' \in \Sigma$ has following representation:

$$X'(x,y) = \ {}_{X'}x \cdot_{X'} \sigma_{X'}y = \alpha h_{\alpha_{X'}} \ {}_{X'}x \cdot \phi h_{\phi_{X'}} \sigma_{X'}y = \nu_{X'}x \cdot \mu_{X'}y,$$

where $\nu_{X'}$ and $\mu_{X'}$ are surjections.

From which we have that there exists abelian group $(Q;\cdot)$ that following identieis hold:

$$\begin{cases} X(x,y) = \nu_X x \cdot \mu_X y, \\ Y(x,y) = \nu_Y Y x \cdot \mu_Y y, \\ Z(x,y) = \nu_Z x \cdot \mu_Z y, \\ X'(x,y) = \nu_{X'} x \cdot \mu_{X'} y, \\ Y'(x,y) = \nu_{Y'} x \cdot \mu_{Y'} y, \\ Z'(x,y) = \nu_{Z'} x \cdot \mu_{Z'} y, \end{cases}$$

where $\nu_X, \mu_X, \nu_Y, \mu_Y, \nu_Z, \mu_Z, \nu_{X'}, \mu_{X'}, \nu_{Y'}, \mu_{Y'}, \nu_{Z'}, \mu_{Z'}$ are surjections.

By doing replacements in the identity (3.9) we will have:

$$\nu_X(\nu_Y x \cdot \mu_Y y) \cdot \mu_X(\nu_Z u \cdot \mu_Z v) = \nu_{X'}(\nu_{Y'} x \cdot \mu_{Y'} u) \cdot \mu_{X'}(\nu_{Z'} y \cdot \mu_{Z'} v).$$

Replacing $x = h_{\nu_Y} h_{\nu_X} e$, $y = h_{\mu_Y} e$, $u = h_{\nu_Z} u$ and $v = h_{\mu_Z} v$, where $h_{\nu_X}, h_{\nu_Y}, h_{\mu_Y}, h_{\nu_Z}, h_{\mu_Z}$ respectively are the right inverses of the ν_X, ν_Y, μ_Y, ν_Z, μ_Z and e is the identity element of the group $(Q;\cdot)$, we will have:

$$\mu_X(u \cdot v) = \nu_{X'}(\nu_{Y'} h_{\nu_Y} h_{\nu_X} e \cdot \mu_{Y'} h_{\nu_Z} u) \cdot \mu_{X'}(\nu_{Z'} h_{\mu_Y} e \cdot \mu_{Y'} h_{\mu_Z} v) = \theta u \cdot \gamma v,$$

where $\theta = \nu_{X'} L_{\nu_{Y'} h_{\nu_Y} h_{\nu_X} e} \mu_{Y'} h_{\nu_Z}$ and $\gamma = \mu_{X'} L_{\nu_{Z'} h_{\mu_Y} e} \mu_{Z'} h_{\mu_Z}$. We showed that μ_X is quasiendomorphism of the group $(Q;\cdot)$ and from lemma 2.1 we know that there exists ϕ_X endomorphism of the group $(Q;\cdot)$ such that $\mu_X = L_a \phi_X$, where L_a is left translation of the group $(Q;\cdot)$ with the element $a \in Q$. We will have following representation of the arbitrary operation $X \in \Sigma$: $X(x,y) = \nu_X x \cdot L_a \phi_X y = R_a \nu_X x \cdot \phi_X y = \sigma_X x \cdot \phi_X y$ where $\sigma_X = R_a \nu_X$.

By doing following replacements in the identity $x = h_{\nu_Y} x$, $y = h_{\mu_Y} y$, $u = h_{\nu_Z} h_{\mu_X} e$ and $v = h_{\mu_Z} e$, we will obtain that σ_X is also a quasiendomorphism of the group $(Q;\cdot)$ and from lemma 2.1 we know that there exists $\ _X$ endomorphism of the group $(Q;\cdot)$ such that $\sigma_X = R_b\ _X$, where R_b is right translation of the group $(Q;\cdot)$ with the element $b \in Q$, so we will have:

$$X(x,y) = \phi_X x \cdot b \cdot \ _X y,$$

Theorem 3.8. *Suppose that $(Q;\Sigma)$ is an r-algebra. If for arbitrary $X, X' \in \Sigma$ there exist $Y, Z, Y', Z' \in \Sigma$ such that (3.13) identity of paramediality satisfies, then there exists an abelian group $(Q;\cdot)$ such that an arbitrary operation $X \in \Sigma$ is endolinear over the group $(Q;\cdot)$. The group $(Q;\cdot)$ is determined uniquely up to isomorphism.*

Let denote by Ω_Q all the regular division operations of the set Q.

Theorem 3.9. *One of the following $\forall\exists(\forall)$-identities of mediality*

$$\forall X, Y \exists X', Y', Z' \forall x, y, u, v X(Y(x,y), Y(u,v)) = X'(Y'(x,u), Z'(y,v)),$$
$$\forall X, Y, Z \exists X', Y', Z' \forall x, y, u, v X(Y(x,y), Z(u,v)) = X'(Y'(x,u), Z'(y,v)),$$
$$\forall X, Y \exists X', Y' \forall x, y, u, v X(Y(x,y), Y(u,v)) = X'(Y'(x,u), Y'(y,v)),$$
$$\forall X, X' \exists Y, Y', Z, Z' \forall x, y, u, v X(Y'(x,y), Y'(u,v)) = Y(X'(x,u), X'(y,v)),$$

or paramediality

$$\forall X, Y \exists X', Y', Z' \forall x, y, u, v X(Y(x,y), Y(u,v)) = X'(Y'(v,y), Z'(u,x)),$$
$$\forall X, Y, Z \exists X', Y', Z' \forall x, y, u, v X(Y(x,y), Z(u,v)) = X'(Y'(v,y), Z'(u,x)),$$
$$\forall X, Y \exists X', Y' \forall x, y, u, v X(Y(x,y), Y(u,v)) = X'(Y'(v,y), Y'(u,x)),$$
$$\forall X, X' \exists Y, Y', Z, Z' \forall x, y, u, v X(Y(x,y), Z(u,v)) = X'(Y'(v,y), Z'(u,x)),$$

holds in the algebra $(Q;\Omega_Q)$, if and only if $|Q| \leq 3$.

Proof. Let us prove it for the first identity; the rest are proved similarly. It follows from Theorem 3.6 that there exists a group $(Q;\cdot)$ such that any operation $X \in \Omega_Q$ is endolinear over this group, which implies that all loops in Ω_Q are endolinear over this group; therefore,

they are principally homotopic to this group. From Lemma 2.1 it follows that they are isomorphic to this group; however, the Albert theorems ([[2], [3]]) imply that a nonassociative loop is not isomorphic to a group; therefore, $|Q| < 5$. It is well-known that on a finite set each surjecion is a bijection; so, each regular division operation is an invertible operation, that is, any operation in Ω_Q is invertible this means if we fix $u = a$ in the identity we will have:

$$X(Y(x, y), \alpha v) = X'(\beta x, Y'(y, v)),$$

which is same

$$X(Y(x, y), v) = X'(\beta x, Y'(y, \alpha^{-1} v)),$$

where α, β are bijections ad α^{-1} is inverse of the α.

This means $(Q; \Omega_Q)$ satisfies to the following second-order identity of associativity:

$$\forall X, Y \exists X'', Y'' \forall x, y, z X(Y(x, y), z) = X''(x, Y''(y, z)),$$

and from the Theorem 1.1 we have that $|Q| \leq 3$.

The sufficiency follows from the [7].

Funding

The first author was partially supported by the Science Committee of Funding of the Republic of Armenia, project nos. 10-3/1-41 and 21T-1A213.

REFERENCES

1. Y.M. Movsisyan, D.N. Harutyunyan, Schauffler-Type Theorems. J. Contemp. Mathemat. Anal. 58, 116–124, 2023. https://doi.org/10.3103/S1068362323020073
2. A. A. Albert, Quasigroup I. Trans. Amer. Math. Soc. 54, 507-519, 1943.
3. A. A. Albert, Quasigroup II. Trans. Amer. Math. Soc. 55, 401-419, 1944.
4. R. Schauffler, Eine Anwendung zyklischer Permutationen and ihreTheorie. Ph.D. Thesis, Marburg University, 1948.
5. R. Schauffler, Über die Bildung von Codewörtern. Arch. elekt. Übertragung, 10, 303-314, 1956.
6. R. Schauffler, Die Associativität im Ganzen, besonders bei Quasigruppen. Math. Z., 67, 428-435, 1957.
7. Yu. Movsisyan. On a theorem of Schauffler. Math. Notes, 53(2), 172–179, 1993.
8. Yu. Movsisyan. Introduction to the theory of algebras with hyperidentities(in Russian). Yerevan State University Press, 1986.

9. Yu. Movsisyan. Hyperidentities and hypervarieties in algebras(in Russian). Yerevan State University Press, 1990.
10. Yu. Movsisyan. Hyperidentities: Boolean And De Morgan Structures. World Scientific Publishing, 2022.
11. V. D. Belousov, “Globally associative systems of quasigroups,” Mat. Sb., N.S. 55 (2), 221–236, 1961.
12. S. Davidov, A. Krapež, Yu. Movsisyan, Functional equations with division and regular operations, Asian-European Journal of Mathematics, Vol. 11, No. 03, 1850033, 2018. https://doi.org/10.1142/S179355711850033X

This page is intentionally left blank