Quasigroups and Related Systems **5** (1998), 99 – 106

On automorphisms of the Cartesian square of a groupoid

Vladimir I. Izbash

Abstract

In this paper, we study the automorphisms of the Cartesian square of a groupoid and give a new approach to describe them. We introduce the notion of a medial pair of groupoids and find a relation between such orthogonal pairs and automorphisms of Cartesian square of the given groupoid. For a groupoid with the identity element this relation is concretized. Then we obtain some results about automorphisms of the Cartesian square of a nonabelian simple group. Also we formulate two problems about medial pairs which are necessary to solve to describe automorphisms of the Cartesian square of a groupoid.

1. Introduction

The present notice contains some results concerning automorphisms of systems with one operation which are various groupoids. Although the groupoids have a simple axiomatic definition, it is not so simple to describe their automorphisms, and the choice of terms for describing them is important. In the following we give an approach to determine automorphisms of the Cartesian square of a groupoid, namely, a relation between automorphisms of the Cartesian square of a groupoid and medial orthogonal pairs of groupoids defined on the basic set of the groupoid is given. It should be noted at once that automorphisms

1991 Mathematics Subject Classification: 20N15
Keywords: groupoid, automorphism

of the direct product of groupoids can be studied in a similar way, but this case is space consuming and will be reserved for later occasion.

The purpose of this paper is to introduce the notion of the medial pair of groupoids, to show the connection between these and automorphisms of the Cartesian square of a groupoid, and to formulate some problems needed to be solved to describe these automorphisms.

For fundamental concepts used in this paper, we refer to [3, 4, 5]. We consider systems (Q, A) consisting of a set Q of a finite or infinite order closed with respect to a binary operation A, called multiplication, i.e. to any two elements $a, b \in Q$ there corresponds a unique third element $c = A(a, b)$ which is called the product of a and b. Such a system is called a groupoid.

An operation A defined on a set Q is said to be *complete* if there exists a substitution θ on Q^2 : $\theta(x, y) = (x', y')$ such that $A = E\theta$, i.e.

$$A(x, y) = E\theta(x, y) = E(x', y') = y'$$

for all $x, y \in Q$, where $E(x, y) = y$.

Two operations L and R defined on a set Q are said to be *orthogonal* if the system of the equations

$$L(x, y) = a, \quad R(x, y) = b$$

has the unique solution for any $a, b \in Q$ [1]. As it is proved in [1], if the operations L and R are orthogonal then they are complete. Note that, in this case, for each $a \in Q$ there exist elements $x, y \in Q$ such that $a = A(x, y)$.

The element $e \in Q$ is the *identity* (or *unit*) of the groupoid (Q, A) if $A(e, x) = A(x, e) = x$ for every $x \in Q$. A groupoid (Q, A) is a quasigroup if for each ordered pair $a, b \in Q$, there is one and only one $x \in Q$ such that $A(a, x) = b$ and one and only one $y \in Q$ such that $A(y, a) = b$. An associative quasigroup is a group.

2. Medial pairs of groupoids

Suppose a set Q is finite or infinite. Each pair of groupoids (Q, L) and (Q, R) on Q uniquely determines a mapping θ on the set $Q \times Q = Q^2$, namely $\theta : (a, b) \longrightarrow (L(a, b), R(a, b))$, $a, b \in Q$ and conversely, each mapping θ on the set Q^2 uniquely determines a pair of groupoids (Q, L) and (Q, R): if $\theta(a, b) = (c, d)$, then we put $c = L(a, b)$ and $d = R(a, b)$.

If θ is a permutation of Q^2 (i.e. a one-to-one mapping of Q^2 onto itself), then the groupoids (Q, L) and (Q, R) determined by θ are orthogonal. Conversely, to each pair (Q, L) and (Q, R) of orthogonal groupoids there corresponds the permutation θ of the set Q^2, defined as above.

If (Q, C) is a groupoid and $\theta : (a, b) = (L(a, b), R(a, b))$, $a, b \in Q$, is an automorphism of (Q^2, C), then for any $a, b, c, d \in Q$ we have

$$\begin{gathered}
\theta(C((a,b),(c,d))) = C(\theta(a,b),\theta(c,d)) \Longleftrightarrow \\
\theta(C(a,c),C(b,d)) = C(\theta(a,b),\theta(c,d)) \Longleftrightarrow \\
(L(C(a,c),C(b,d)),R(C(a,c),C(b,d))) = \\
C((L(a,b),R(a,b)),(L(c,d),R(c,d))) \Longleftrightarrow \\
(L(C(a,c),C(b,d)),R(C(a,c),C(b,d))) = \\
(C(L(a,b),L(c,d)),C(R(a,b),R(c,d))) \Longleftrightarrow \\
\begin{cases} L(C(a,c),C(b,d)) = C(L(a,b),L(c,d)) \\ R(C(a,c),C(b,d)) = C(R(a,b),R(c,d)). \end{cases}
\end{gathered}$$

So we have proved the following theorem.

Theorem 1. *Let (Q, C) be a groupoid with a binary operation C defined on the set Q. A mapping $\theta : Q^2 \longrightarrow Q^2$ is an automorphism of the Cartesian square (Q^2, C) iff there exist two orthogonal groupoids (Q, L) and (Q, R) such that the equalities*

$$\begin{gathered}
C(L(x,y),L(u,v)) = L(C(x,u),C(y,v)), \\
C(R(x,y),R(u,v)) = R(C(x,u),C(y,v)), \\
(L(x,y),R(x,y)) = \theta(x,y)
\end{gathered}$$

hold for any $x, y, u, v \in Q$. □

Definition 1. A pair of groupoids (Q, A) and (Q, B) for which the equality

$$A(B(x,y),B(u,v)) = B(A(x,u),A(y,v)) \qquad (1)$$

holds for any $x, y, u, v \in Q$ will be called a *medial pair*.

By $M(Q,C)$ we denote the class of all groupoids (Q,D) such that the pair of (Q,C) and (Q,D) is a medial pair.

By $OrtM(Q,C)$ we denote the class of all orthogonal pairs of groupoids from $M(Q,C)$.

The above theorem shows that in describing automorphisms of the Cartesian square (Q^2,C) of a groupoid (Q,C), it is necessary and sufficient to solve the following two problems:

Problem 1. *Describe elements of* $M(Q,T)$.

Problem 2. *Describe elements of* $OrtM(Q,T)$.

3. Special cases

Now we use Theorem 1 in some special cases. At first we consider the case that a groupoid (Q,A) has the identity e.

Assume that groupoids (Q,B) and (Q,A) form a medial pair, i.e. the identity (1) holds. Since (1) for $x=u=e$ has the form

$$A(B(e,y),B(e,v)) = B(e,A(y,v)),$$

we have that $\alpha : Q \longrightarrow Q$ defined by $\alpha(x) = B(e,x)$ is an endomorphism of (Q,A). Analogously we prove that β defined by $\beta(x) = B(x,e)$ is an endomorphism of (Q,A).

From (1) for $u=y=e$ we obtain also

$$B(x,v) = A(\beta(x),\alpha(v)) \tag{2}$$

for every $x,v \in Q$ and, again, from (1) for $x=v=e$ we get

$$B(u,y) = A(\alpha(y),\beta(u)) \tag{3}$$

for every $u,y \in Q$.

Now, from (2) and (3) we have

$$B(x,y) = A(\beta(x),\alpha(y)) = A(\alpha(y),\beta(x)) \tag{4}$$

for $x,y \in Q$.

Hence, the identity (1) maybe replaced by

$$A(A(\beta(x),\alpha(y)),A(\beta(u),\alpha(v))) = A(\beta(A(x,u)),\alpha(A(y,v))). \tag{5}$$

From (4) and the definition of α and β we get

$$\alpha(e) = \beta(e), \tag{6}$$

$$\alpha(x) = A(\beta(e), \alpha(x)) = A(\alpha(x), \beta(e)), \tag{7}$$

$$\beta(x) = A(\beta(x), \alpha(e)) = A(\alpha(e), \beta(x)), \tag{8}$$

for $x \in Q$.

Putting $v = e$ in (5) and using (6), (7), (8), and (4), we obtain

$$A(A(\alpha(y), \beta(x)), \beta(u)) = A(\alpha(y), \beta(A(x, u))) \tag{9}$$

for any $y, u, x \in Q$.

Since (5) for $u = e$ has the form

$$A(A(\beta(x), \alpha(y)), \alpha(v)) = A(\beta(x), \alpha(A(y, v))), \tag{10}$$

then

$$\begin{aligned} A(A(\beta(x), \alpha(y)), A(\beta(u), \alpha(v))) &= A(\beta(A(x, u)), \alpha(A(y, v))) \\ &= A(\alpha A(y, v)), \beta(A(x, u))) = A(A(\alpha(A(y, v)), \beta(x)), \beta(u)) \\ &= A(A(\beta(x), \alpha(A(y, v))), \beta(u)) = A(A(A(\beta(x), \alpha(y)), \alpha(v)), \beta(u)) \end{aligned}$$

by (5), (4), (9) and (10). Thus

$$A(A(\beta(x), \alpha(y)), A(\beta(u), \alpha(v))) = A(A(A(\beta(x), \alpha(y)), \alpha(v)), \beta(u)) \tag{11}$$

holds for any $x, y, u, v \in Q$.

Conversely, let us have $\alpha, \beta \in End(Q, A)$ such that the relations (6), (9), (10), (11) and $A(\beta(x), \alpha(y)) = A(\alpha(y), \beta(x))$ hold in a groupoid (Q, A) for any $x, y, u, v \in Q$. Then the pair of groupoids (Q, A) and (Q, B), where $B(x, y) = A(\beta(x), \alpha(y))$ for all $x, y \in Q$, is a medial pair. Indeed, for every $x, y, u, v \in Q$ we have

$$\begin{aligned} A(B(x, y), B(u, v)) &= A(A(\beta(x), \alpha(y)), A(\beta(u), \alpha(v))) \\ &= A(A(A(\beta(x), \alpha(y)), \alpha(v)), \beta(u)) = A(A(\beta(x), \alpha(A(y, v))), \beta(u)) \\ &= A(A(\alpha(A(y, v)), \beta(x)), \beta(u)) = A(\alpha(A(y, v)), \beta(A(x, u))) \\ &= A(\beta(A(x, u)), \alpha(A(y, v))) = B(A(x, u), A(y, v)). \end{aligned}$$

So we have proved the following

Theorem 2. *Let (Q, A) and (Q, B) be groupoids and e be the unit of (Q, A). The pair (Q, A) and (Q, B) is a medial pair iff there exist endomorphisms α and β of (Q, A) such that* (4), (6), (9), (10) *and* (11) *hold.*

Suppose now that (Q, A) is a fixed nonabelian simple group. Then $\alpha \in End(Q, A)$ iff either $\alpha \in Aut(Q, A)$ or α is the zero endomorphism ω of (Q, A) defined by $\omega(x) = e$ for all $x \in Q$. Since (Q, A) is nonabelian the identity $A(\beta(x), \alpha(y)) = A(\alpha(y), \beta(x))$ is not fulfilled for all $\alpha, \beta \in Aut(Q, A)$. Clearly $A(\beta(x), \omega(y)) = A(\omega(y), \beta(x))$ and $A(\omega(x), \beta(y)) = A(\beta(y), \omega(x))$ for all $x, y \in Q$ and $\beta \in End(Q, A)$. Obviously the relations (9) – (11) hold in the group (Q, A) by the associativity. Therefore we have proved the following proposition.

Proposition 1. *The groupoid (Q, B) is contained in $M(Q, A)$ for a nonabelian simple group (Q, A) iff there exists $\beta \in End(Q, A)$ such that either $B(x, y) = \beta(x)$ or $B(x, y) = \beta(y)$ for all $x, y \in Q$.*

Proposition 2. *Let (Q, A) be a nonabelian simple group. Then the pair of groupoids $((Q, B), (Q, C))$ is contained in $OrtM(Q, A)$ iff there exist $\alpha, \beta \in Aut(Q, A)$ such that $B(x, y) = \alpha(x)$, $C(x, y) = \beta(y)$ for all $x, y \in Q$.*

Proof. Let $(Q, B), (Q, C) \in M(Q, A)$ be orthogonal groupoids. By Proposition 1, there exist $\alpha, \beta \in End(Q, A)$ such that either $B(x, y) = \alpha(x)$ or $B(x, y) = \alpha(y)$ and either $C(x, y) = \beta(x)$ or $C(x, y) = \beta(y)$ for all $x, y \in Q$.

The case "$B(x, y) = \alpha(x)$ and $C(x, y) = \beta(x)$ for all $x, y \in Q$" implies that the system of equations

$$B(x, y) = a, \quad C(x, y) = b \tag{12}$$

has more than one solution for any fixed $a, b \in Q$, thus the groupoids (Q, B) and (Q, C) are not orthogonal. The same is valid for the case when $B(x, y) = \alpha(y)$ and $C(x, y) = \beta(y)$ for all $x, y \in Q$.

Now suppose that we have $B(x, y) = \alpha(x)$ and $C(x, y) = \beta(y)$ for all $x, y \in Q$. If either $\alpha = \omega$ or $\beta = \omega$, then the system (12) has more than one solution for any fixed $a, b \in Q$.

Let $\alpha, \beta \in Aut(Q, A)$ and $B(x, y) = \alpha(x)$, $C(x, y) = \beta(y)$ for all

$x, y \in Q$. In this case the system (12) becomes $\alpha(x) = a, \quad \beta(y) = b$ which has a unique solution for any fixed $a, b \in Q$. Therefore the groupoids (Q, B) and (Q, C) are orthogonal. The same is valid for the case $B(x, y) = \alpha(y)$, $C(x, y) = \beta(x)$ and $\alpha, \beta \in End(Q, A)$.

Conversely, if $\alpha, \beta \in Aut(Q, A)$ and $B(x, y) = \alpha(x), \quad C(x, y) = \beta(y)$ for all $x, y \in Q$, then the groupoids (Q, B) and (Q, C) are orthogonal and (Q, B), $(Q, C) \in M(Q, A)$, by Proposition 1.

In the case $B(x, y) = \alpha(y)$, $C(x, y) = \beta(x)$ for all $x, y \in Q$, the proof is similar. □

Corollary 1. *Let (Q, A) be a nonabelian simple group. Then θ is an automorphism of (Q^2, A) iff there exist $\alpha, \beta \in Aut(Q, A)$ such that $\theta(x, y) = (\alpha(x), \beta(y))$ for every $x, y \in Q$.* □

Example. Let $(G, \cdot)$ be a groupoid, where $G = \{k, p, q, t, m, e, f, b, c, a\}$, and $(\cdot)$ is defined by the table

$\cdot$	k	p	q	t	m	e	f	b	c	a
k	k	p	q	t	m	e	f	b	c	a
p	p	q	t	p	p	p	p	b	c	a
q	q	q	t	q	q	q	q	b	c	a
t	t	t	t	t	t	t	t	b	c	a
m	m	p	q	t	m	e	f	b	c	a
e	e	p	q	t	e	e	f	b	c	a
f	f	p	q	t	f	f	f	b	c	a
b	b	b	b	b	b	b	b	a	a	a
c	c	c	c	c	c	c	c	a	a	a
a	a	a	a	a	a	a	a	a	a	a

It is easy to check that $(A, \cdot)$, $(B, \cdot)$, $(C, \cdot)$, $(D, \cdot)$, where $C = \{a, b, c\}$, $A = \{e, a, b, c\}$, $B = \{m, a, b, c\}$ and $D = \{e, m, a, b, c\}$, are commutative, associative subgroupoids of $(G, \cdot)$ such that $C = A \cap B$. The element k is the unit of $(G, \cdot)$ and $(G, \cdot)$ is not associative, since $p(pq) = p \neq t = (pp)q$.

Consider two mappings $\alpha, \beta : G \longrightarrow G$ defined by

$$\alpha(x) = \begin{cases} e, & \text{for } x \notin C \\ x, & \text{for } x \in C, \end{cases} \qquad \beta(x) = \begin{cases} m, & \text{for } x \notin C \\ x, & \text{for } x \in C. \end{cases}$$

It is easy to check that $\alpha, \beta \in End(G, \cdot)$ and $\alpha(x) = x$ for any $x \in A$, $\beta(x) = x$ for any $x \in B$ and $A \cdot B = D$. By the commutativity of

$(D, \cdot)$ and the definition of α and β we have $\beta(x) \cdot \alpha(y) = \alpha(y) \cdot \beta(x)$ for all $x, y \in G$. Now by the associativity of $(D, \cdot)$ we have

$$(\beta(x) \cdot \alpha(y)) \cdot (\beta(u) \cdot \alpha(v)) = ((\beta(x) \cdot \alpha(y) \cdot \alpha(v))\beta(u)$$

for all $x, y, u, v \in G$.

By Theorem 2, the groupoid $(G, *)$, where $x * y = \beta(x) \cdot \alpha(y)$, forms a medial pair with $(G, \cdot)$.

References

[1] **V. D. Belousov**: *On properties of binary operations*, (Russian), Uchenye Zapiski Beltskogo pedinstituta, Beltsy, **5** (1960), 9 – 28.

[2] **V. D. Belousov**: *Systems of orthogonal operations*, (Russian), Mat. Sbornik, **77 (119)** (1968), 38 – 58.

[3] **R. Bruck**: *A survey of binary systems*, Springer-Verlag, Berlin-Heidelberg-New York, 1966.

[4] **B. A. Hausman and O. Ore**: *Theory of quasigroups*, Amer. Math. J. **59** (1937), 1004.

[5] **A. R. Richardson**: *Groupoids and Their automorphisms*, Proc. London Math. Soc. **48** (1943), 83 – 111.

Department of Quasigroup Theory
Institute of Mathematics and Informatics
Academy of Sciences of Republic of Moldova
Academiei str. 5
MD-2028 Chishinau
Moldova

Received May 10, 1998