Note di Matematica Vol. XIII - n.1, 107-115 (1993)

QUADRATICAL GROUPOIDS (*)

VLADIMIR VOLENEC

A groupoid $(Q,\cdot)$ is said to be quadratical if the identity

$$ab\cdot a = ca\cdot bc \tag{1}$$

holds and if $(Q,\cdot)$ is a right quasigroup, i.e. for any $a,b\in Q$ the equation $ax=b$ has the unique solution x. Quadratical groupoids arose originally from the geometric situation described in Example 3 below. In this paper we study abstract quadratical groupoids and certain derived algebraic structures.

Example 1. Let $(G,+)$ be a commutative group with unique halving, i.e. for every $a\in G$ there is one and only one element $x\in G$ such that $x+x=a$. Denote this element by $\frac{1}{2}a$. Let use suppose that there is an automorphism φ of the group $(G,+)$ such that for any $a\in G$ the equality

$$(\varphi\circ\varphi)(a)-\varphi(a)+\frac{1}{2}a=0 \tag{2}$$

holds. If $\cdot$ is the binary operation on the set G defined by

$$ab=a+\varphi(b-a), \tag{3}$$

then $(G,\cdot)$ is a quadratical groupoid. Namely, for every $a,b\in G$ the equation $ax=b$ is equivalent to the equation

$$a+\varphi(x-a)=b$$

with the unique solution $x=a+\varphi^{-1}(b-a)$. By (3) we obtain after some simplifications

$$ab\cdot a=a-\varphi(a)+(\varphi\circ\varphi)(a)+\varphi(b)-(\varphi\circ\varphi)(b),$$

$$ca\cdot bc=\varphi(a)-(\varphi\circ\varphi)(a)+\varphi(b)-(\varphi\circ\varphi)(b)+c-2\varphi(c)+2(\varphi\circ\varphi)(c)$$

and by (2) we get

$$ab\cdot a=\frac{1}{2}a+\frac{1}{2}b=ca\cdot bc.$$

(*) Proofs not corrected by the author.

Example 2. Let $(F, +, \cdot)$ be a field with char $F \neq 2$ in which the equations

$$q^2 - q + \frac{1}{2} = 0$$

has a solution q and let $*$ the operation in the set F defined by

$$a * b = (1 - q)a + qb.$$

By (4) the identity (2) follows settings $\varphi(a) = qa$. Now, Example 1 implies that $(F, *)$ is a quadratical groupoid.

Example 3. Let $(C, +, \cdot)$ be the field of complex numbers and $*$ the operation on C defined by (5), where $q = \frac{1}{2}(1 + i)$. By Example 2 $(C, *)$ is a quadratical groupoid which we denote by $C\left(\frac{l+i}{2}\right)$. This groupoid has a beautiful geometrical interpretation which motivates the study of quadratical groupoids. Let us regard complex numbers as points of the Euclidean plane. For any point a we obviously have $a * a = a$ and for every two different points a, b the equality (5) can be written in the form

$$\frac{a * b - a}{b - a} = \frac{q - 0}{1 - 0},$$

which means that the points $a, b, a * b$ are the vertices of a triangle directly similar to the triangle with the vertices 0, 1, q, *i.e.* $a, b, a*b$ are the vertices of a positively oriented isosceles right triangle with the right angle at $a * b$. We can say that $a * b$ is the centre of the positively oriented square with the adjacent vertices a and b, which justifies the name «quadratical groupoid». Every identity in the quadratical groupoid $C\left(\frac{l+i}{2}\right)$ can be interpreted as a geometrical theorem which, of course, can be proved directly, but the theory of quadratical groupoids gives a better insight into the mutual relations of such theorems. For example, the left side of the identity

$$(a * b) * a = (c * a) * (b * c)$$

is obviously the midpoint of the points a and b and this identity is illustrated by Figure 1 (here and in the Figure 2 we omit the sign $*$). This identity and figure illustrate a famous problem about the buried treasure of captain Kidd which is attributed to G. Gamow.

From now on let $(Q, \cdot)$ be any quadratical groupoid. Let us prove some simple properties of this groupoid.

Theorem 1. *In a quadratical groupoid* $(Q,\cdot)$ *the following identities hold:*

(6) $\qquad aa = a \quad (\textit{idempotency}),$

(7) $\qquad a\cdot ba = ab\cdot a \quad (\textit{elasticity}),$

(8) $\qquad ab\cdot a = ba\cdot b,$

(9) $\qquad ba\cdot ab = a,$

(10) $\qquad a\cdot bc = ab\cdot ac \quad (\textit{left distributivity}).$

Proof. (6) follows from (1) with $b = c = a$ and (7) follows from (1) with $c = a$, using (6). Putting $c = b$ resp. $b = a$ in (1) and using (6), we obtain (8) resp. the identity $ca\cdot ac = a$, *i.e.* (9). Now, let $a, b, c \in Q$ be any elements. There is $d \in Q$ such that $cd = a$. Therefore, we obtain succesively

$$ab\cdot ac = ab\cdot(cd\cdot c) \overset{(8)}{=} ab\cdot(dc\cdot d) \overset{(7)}{=} ab\cdot(d\cdot cd)$$

$$= ab\cdot da \overset{(1)}{=} bd\cdot b \overset{(8)}{=} db\cdot d \overset{(1)}{=} cd\cdot bc = a\cdot bc.$$

Theorem 2. *In a quadratical groupoid* $(Q,\cdot)$ *we have the equivalence*

(11) $\qquad ab = cd \Longleftrightarrow bc = da$

and especially the equivalence

$$ab = c \Longleftrightarrow bc = ca.$$

Further, from $ab = ba$ *if follows* $a = b$.

Proof. Let $ab = cd$. We have

$$a\cdot bc \overset{(10)}{=} ab\cdot ac = cd\cdot ac \overset{(1)}{=} da\cdot d \overset{(8)}{=} ad\cdot a \overset{(7)}{=} a\cdot da,$$

wherefrom $bc = da$ follows? The converse follows by cyclic substitution of a, b, c, d. Further, from $ab = ba$ we obtain

$$aa \overset{(6)}{=} a \overset{(9)}{=} ba\cdot ab = ab\cdot ab \overset{(6)}{=} ab,$$

wherefrom $a = b$ follows.

Theorem 3. *In a quadratical groupoid* $(Q,\cdot)$ *we have the identity*

(12) $\qquad ab\cdot cd = ac\cdot bd \quad (\textit{mediality}).$

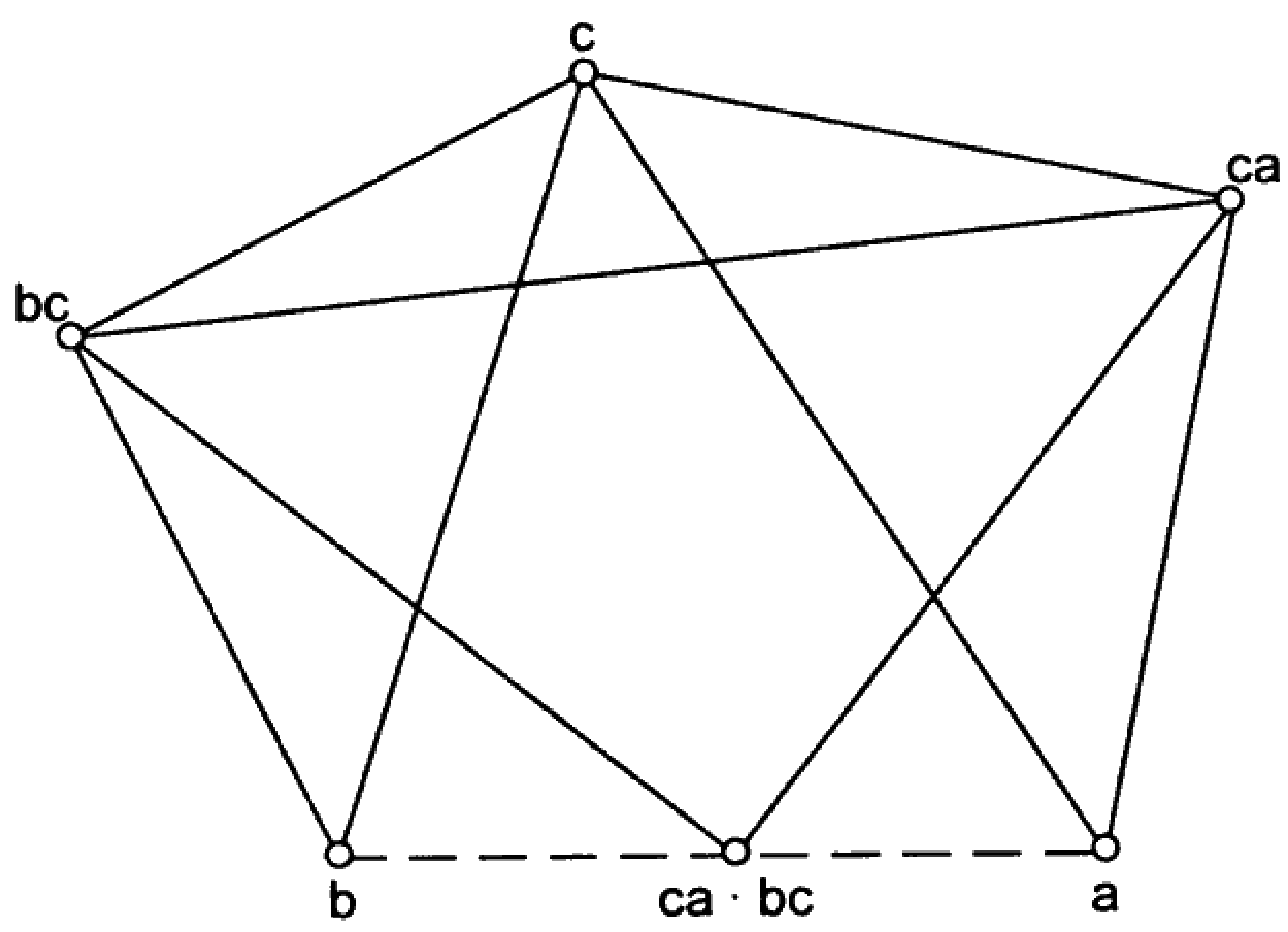

Figure 1

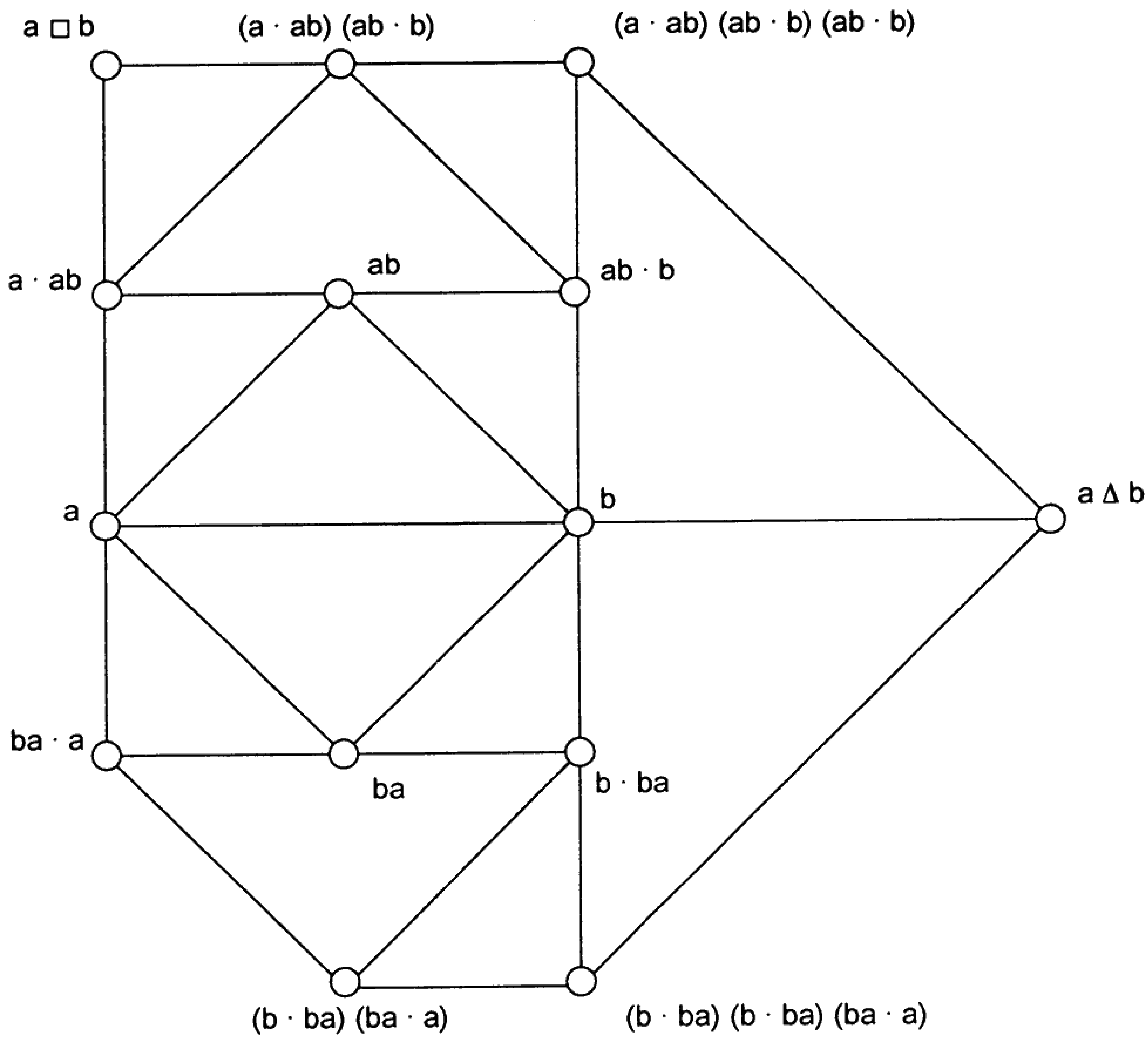

Figure 2

Proof. Let $a, b, c, d \in Q$ be any elements. There is $e \in Q$ such that $de = ab$, wherefrom by (11) it follows $bd = ea$. Therefore, we obtain

$$ab \cdot cd = de \cdot cd \overset{(1)}{=} ec \cdot e \overset{(8)}{=} ce \cdot c \overset{(1)}{=} ac \cdot ea = ac \cdot bd.$$

Theorem 4. *In a quadratical groupoid* $(Q, \cdot)$ *the following identities hold:*

$$ab \cdot c = ac \cdot bc \quad (\textit{right distributivity}), \tag{13}$$

$$a(b \cdot ba) = (ab \cdot a)b, \tag{14}$$

$$(ab \cdot b)a = b(a \cdot ba). \tag{15}$$

Proof. (13) follows from (12) with $d = c$, using (6). Further we obtain

$$a(b \cdot ba) \overset{(10)}{=} ab \cdot (a \cdot ba) \overset{(10)}{=} (ab \cdot a)(ab \cdot ba) \overset{(9)}{=} (ab \cdot a)b,$$

$$(ab \cdot b)a \overset{(13)}{=} 4ab \cdot a) \cdot ba \overset{(13)}{=} (ab \cdot ba)(a \cdot ba) \overset{(9)}{=} b(a \cdot ba).$$

Theorem 5. *Every quadratical groupoid* $(Q, \cdot)$ *is a quasigroup, i.e. for any* $a, b \in Q$ *the equation* $xa = b$ *has the unique solution* $x = (a \cdot ab)(ab \cdot b) \cdot (ab \cdot b)$.

Proof. With $x = (a \cdot ab)(ab \cdot b) \cdot (ab \cdot b)$ (Fig. 2) we have successively

$$xa = [(a \cdot ab)(ab \cdot b) \cdot (ab \cdot b)]a \overset{(13)}{=} [(a \cdot ab)a \cdot (ab \cdot b)a] \cdot (ab \cdot b)a =$$

$$\overset{(15)}{=} [(a \cdot ab)a \cdot b(a \cdot ba)] \cdot b(a \cdot ba) \overset{(7)}{=} [a(ab \cdot a) \cdot b(ab \cdot a)] \cdot b(ab \cdot a) =$$

$$\overset{(13)}{=} (ab \cdot b)(ab \cdot a) \overset{(10)}{=} ab \cdot ba \overset{(9)}{=} b.$$

Moreover, from $xa = b$ it follows

$$x \overset{(9)}{=} ax \cdot xa \overset{(10)}{=} (ax \cdot x)(ax \cdot a) \overset{(7)}{=} (ax \cdot x)(a \cdot xa) \overset{(13)}{=}$$

$$= [a(a \cdot xa) \cdot x(a \cdot xa)] \cdot x(a \cdot xa) \overset{(15)}{=} [a(a \cdot xa) \cdot (ax \cdot x)a] \cdot (ax \cdot x)a$$

$$\overset{(13)}{=} [a(a \cdot xa) \cdot (ax \cdot a)(xa)] \cdot (ax \cdot a)(xa) \overset{(7)}{=}$$

$$= [a(a \cdot xa) \cdot (a \cdot xa)(xa)] \cdot (a \cdot xa)(xa) = (a \cdot ab)(ab \cdot b) \cdot (ab \cdot b).$$

On the set Q we define a new operation $\square$ by

$$a \square b = c \Longleftrightarrow bc = a. \tag{16}$$

Theorem 6. $(Q,\square)$ *is a quasigroup with the identity*

$$a\square(a\square b)=c\square[(a\square c)\square b], \tag{17}$$

i.e. it is a rot-quasigroup in the terminology of J. Duplák [1].

Proof. The groupoid $(Q,\square)$ is conjugate (in the sense of S. K. Stein [6]) to the quasigroup $(Q,\cdot)$ and hence $(Q,\square)$ is a quasigroup. We must prove the identity (17), i.e. the implication

$$a\square b=d, a\square d=e, a\square c=f, f\square b=g\Rightarrow c\square g=e.$$

But, by (17) this implication is equivalent with the implication

$$bd=a, de=a, cf=a, bg=f,\Rightarrow ge=c,$$

which is to be proved. The hypotheses of this implication imply

$$ge\cdot bg\overset{(1)}{=}eb\cdot e\overset{(1)}{=}de\cdot bd=aa\overset{(6)}{=}a=cf=c\cdot bg$$

and it follows $ge=c$. Theorem 5 suggest that the operation $\square$ can be defined directly by the multiplication in the quasigroup $(Q,\cdot)$, i.e. we have:

Theorem 7. *For any* $a,b\in Q$ *the equality*

$$a\square b=(a\cdot ab)\cdot(a\cdot ab)(ab\cdot b)$$

holds (Fig. 2).

Proof. For any $a,b\in Q$ there is one and only element $c\in Q$ such that $bc=a$, i.e. $a\square b=c$ because of (16). But, we have successively

$$b[(a\cdot ab)\cdot(a\cdot ab)(ab\cdot b)]\overset{(10)}{=}b(a\cdot ab)\cdot([b(a\cdot ab)\cdot b(ab\cdot b)]=$$

$$\overset{(14)}{=}=(ba\cdot b)a\cdot[(ba\cdot b)a\cdot b(ab\cdot b)]\overset{(7)}{=}(b\cdot ab)a\cdot[(b\cdot ab)a\cdot(b\cdot ab)b]=$$

$$\overset{(10)}{=}=(b\cdot ab)(a\cdot ab)\overset{(13)}{=}ba\cdot ab\overset{(9)}{=}a.$$

Corollary. *Equation* $ax=b$ *has the unique solution* $x=(b\cdot ba)\cdot(b\cdot ba)(ba\cdot a)$ *(Fig. 2).*

On the set Q we define a new operation $\bullet$ by

$$a\bullet b=ab\cdot a. \tag{18}$$

Theorem 8. $(Q, \bullet)$ *is a indepotent medial commutative quasi group.*

Proof. Indepotency and commutativity are obvious because of (6) and (8). Owing to (18) and (12) we obtain successively

$$(a \bullet b) \bullet (c \bullet d) = (ab \cdot a)(cd \cdot c) \cdot (ab \cdot a) = (ab \cdot cd)(ac) \cdot (ab \cdot a) =$$

$$= (ac \cdot bd((ab) \cdot (ac \cdot a) = (ac \cdot a)(bd \cdot b) \cdot (ac \cdot a) = (a \bullet c) \bullet (b \bullet d).$$

For every $a, b \in Q$ there is $c \in Q$ such that $ca = b$ and then $x \in Q$ such that $ax = c$. Therefore

$$a \bullet x = ax \cdot a = ca = b.$$

Finally, from $a \bullet x = a \bullet y$, i.e. $ax \cdot a = ay \cdot a$, it follows at once $x = y$.

By Theorem 8, $(Q, \bullet)$ is a so called IMC-quasigroup, whose properties are studies in [2-5].

Theorem 9. *For any* $a, b, c, d \in Q$ *we have the identity*

$$(19) \qquad ab \bullet cd = (a \bullet c)(b \bullet d)$$

(mutual mediality of the operations $\cdot$ *and* $\bullet$*).*

Proof. By (18) and (12) we have successsively

$$ab \bullet cd = (ab \cdot cd) \cdot ab = (ac \cdot bd) \cdot ab = (ac \cdot a)(bd \cdot b) = (a \bullet c)(b \bullet d).$$

In the case of the quasigroup $C\left(\frac{l+1}{2}\right)$ Theorem 9 proves the following statement, which implies some rsults from [7].

Let p, q be the centres of positively oriented squares constructed on oriented segments (a, b) and (c, d), and let r, s be the midpoints of the segments $\{a, c\}$ and $\{b, d\}$. Then the midpoint of the segment $\{p, q\}$ is the centre of the positively oriented square constructed on the oriented segment (r, s).

By means of the quasigroup $(Q, \bullet)$ we can define a new operation $\triangle$ on the set Q by

$$(20) \qquad a \triangle b = c \Longleftrightarrow a \bullet c = b$$

Theorem 10. $(Q, \triangle)$ *is an idempotent quasigroup with the identity*

$$(21) \qquad [(a \triangle b) \triangle c] \triangle d = [(a \triangle d) \triangle c] \triangle b.$$

i.e. a quasigroup of the type that was studies in [8].

Proof. The groupoid $(Q, \triangle)$ and the quasigroup $(Q, \bullet)$ are conjugate and hence $(Q, \triangle)$ is a quasigroup, too. For every $a \in Q$ we have $a \bullet a = a$, wherefrom it follows by (20) that $a \triangle a = a$. We must prove the identity (21), i.e. the implication

$$a \triangle b = x, x \triangle c = y, y \triangle d = z, a \triangle d = u, u \triangle c = v \Rightarrow v \triangle b = z,$$

which is, because of (20), equivalent to the implication

$$a \bullet x = b, x \bullet y = c, y \bullet z = d, a \bullet u = d, u \bullet v = c \Rightarrow v \bullet z = b.$$

But, from the hypotheses of this implication we obtain by Theorem 8

$$(u \bullet y) \bullet (v \bullet z) = (u \bullet v) \bullet (y \bullet z) = c \bullet d = (x \bullet y) \bullet (a \bullet u) =$$

$$= (x \bullet a) \bullet y \bullet u) = (u \bullet y) \bullet (a \bullet x) = (u \bullet y) \bullet b,$$

wherefrom it follows $v \bullet z = b$.

The operation $\triangle$ can also be defined by means of the multiplication. We have

Theorem 11. *For every $a, b \in Q$ the equality*

$$a \triangle b = [(a \cdot ab)(ab \cdot b) \cdot (ab \cdot b)][(b \cdot ba) \cdot (b \cdot ba)(ba \cdot a)]$$

holds (Fig. 2).

Proof. For any $a, b \in Q$ there is one and only one element $c \in Q$ such that $a \bullet c = b$ (because of Theorem 8), i.e. $a \triangle b = c$ because of (20). But, we shall prove that

$$a \bullet [(a \cdot ab)(ab \cdot b) \cdot (ab \cdot b)][(b \cdot ba) \cdot (b \cdot ba)(ba \cdot a)] = b.$$

In the proofs of Theorems 5 and 7 we proved the identifies

$$[(a \cdot ab)(ab \cdot b) \cdot (ab \cdot b)]a = b, \tag{22}$$

$$b[(a \cdot ab) \cdot (a \cdot ab)(ab \cdot b)] = a \tag{23}$$

Now, we obtain successively

$$[(a \cdot ab)(ab \cdot b) \cdot (ab \cdot b)][(b \cdot ba) \cdot (b \cdot ba)(ba \cdot a)] \overset{(18)}{=}$$

$$= \{a \cdot [(a \cdot ab)(ab \cdot b) \cdot (ab \cdot b)][(b \cdot ba) \cdot (b \cdot ba)(ba \cdot a)]\}a \overset{(10)}{=}$$

$$= \{a[(a \cdot ab)(ab \cdot b) \cdot (ab \cdot b)] \cdot a[(b \cdot ba) \cdot (b \cdot ba)(ba \cdot a)]\}a \overset{(23)}{=}$$

$$= \{a[(a \cdot ab)(ab \cdot b) \cdot (ab \cdot b)] \cdot b\}a \overset{(13)}{=} \{a[(a \cdot ab)(ab \cdot b) \cdot (ab \cdot b)] \cdot a\} \cdot ba \overset{(7)}{=}$$

$$= \{a \cdot [(a \cdot ab)(ab \cdot b) \cdot (ab \cdot b)]a\} \cdot ba \overset{(22)}{=} ab \cdot ba \overset{(9)}{=} b.$$

REFERENCES

[1] J. DUPLÁK, *Rot quasigroups*, Mat. Čas. **23** (1973), 223-230.

[2] J. GATIAL, *Some geometrical examples of an IMC-quasigroup*, Mat.-Fyz. Čas **19**, 292-298.

[3] J. GATIAL, *Über die IMC-Quasigruppe und den Schwerpunkt eines Dreiecks*, Math. Nachr. **53** (1972), 119-123.

[4] J. GATIAL, *Die Schwerpunkte der Dreieckein einigen endlichen Quasigruppen*, Math. Slovaca **28** (1978), 169-172.

[5] E. NATALE, *n-quasigruppi mediali idempotenti commutativi*, Rend. Accad. Sci. Fis. Mat. Napoli (4) **46** (1980), 221-229.

[6] S.K. STEIN, *On the foundation of quasigroups*, Trans. Amer. Math. Soc. **85** (1957), 228-256.

[7] V. THÉBAULT, *Polygons de 2n cotés bordé de triangles isoscèles semblables*, Mathesis **54** (1940), 161-166.

[8] D. VAKARELOV, *Algebrični osnovi na centralnata simetrija, v'rteneto i homotetijata*, Godišnik Univ. Sofija Mat. Fak. **63** (1968/69), 121-166 (1970).

Received April 23, 1991 and in revised form October 21, 1991
V. Volenec
Department of Mathematics
University of Zagreb
41001 Zagreb, P.O. Box 187
Yugoslavia