Quasigroups and Related Systems, **4** (1997), 9–13

Quadratical quasigroups

Wiesław A. Dudek

Abstract

Quadratical quasigroups, which have a beautiful geometrical interpretation, are characterized by commutative groups and some of their automorphisms.

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

$$xy \cdot x = zx \cdot yz \tag{1}$$

holds and the equation $ax = b$ has a unique solution $x \in G$ for all $a, b \in G$.

Quadratical groupoids arose originally from the geometrical situation described by the field of complex numbers $\mathbf{C}$ and the operation $*$ on $\mathbf{C}$ defined by

$$x * y = (1 - q)x + qy\,,$$

where $q = \frac{1}{2}(1 + i)$ (cf. [3] or [4]). The geometrical interpretation of $(G, *)$ motivates us to the further study of quadratical groupoids.

Quadratical groupoids are idempotent quasigroups (cf. [4]). Such quasigroups are also medial and distributive (cf. [4]). This means (cf. Theorem 8.3 from [2]) that such quasigroups are transitive. Hence (cf. Theorem 8.1 from [2]) every quadratical groupoid is isotopic to some commutative Moufang loop.

The above results together with the above example suggest that every quadratical groupoid may be described by some commutative group and some of its automorphisms.

1991 Mathematics Subject Classification: 20N05
Keywords: quadratical groupoid, quasigroup, isotopy

Theorem. *A groupoid $(G,\cdot)$ is a quadratical quasigroup if and only if there exists a commutative group $(G,+)$ in which for every $a \in G$ the equation $z+z=a$ has a unique solution $z=\frac{1}{2}a \in G$ and φ, ψ are automorphisms of $(G,+)$ such that for all $x,y \in G$*

$$xy = \varphi(x) + \psi(y), \tag{2}$$

$$\varphi(x) + \psi(x) = x, \tag{3}$$

$$2\psi\varphi(x) = x. \tag{4}$$

Proof. Since a quadratical groupoid $(G,\cdot)$ is a transitive distributive quasigroup, then from results obtained in [1] it follows that there exists a commutative group $(G,+)$ and its automorphisms φ, ψ such that (2) and (3) hold.

Replacing in (1) an element x by 0 (i.e. by the neutral element of $(G,+)$) and applying (2) we obtain

$$\varphi\psi(y) = \varphi^2(z) + \psi\varphi(y) + \psi^2(z),$$

which for $y=0$ gives

$$\varphi^2(z) + \psi^2(z) = 0. \tag{5}$$

Hence

$$\varphi\psi(y) = \psi\varphi(y) \tag{6}$$

for every $y \in G$.

Since from (3) immediately follows $\varphi^2(x) + \varphi\psi(x) = \varphi(x)$ and $\psi^2(x) + \psi\varphi(x) = \psi(x)$, then

$$\varphi^2(x) + \psi^2(x) + \varphi\psi(x) + \psi\varphi(x) = \varphi(x) + \psi(x) = x,$$

which together with (5) and (6) implies (4).

Now applying (2) and (6) to the identity $y = xy \cdot yx$, which holds in all quadratical groupoids (cf. [4] Theorem 1) we obtain

$$y = \varphi^2(x) + \varphi\psi(y) + \psi\varphi(y) + \psi^2(x) = \varphi\psi(y) + \varphi\psi(y)\,.$$

Hence

$$\varphi^{-1}(y) = \psi(y) + \psi(y)$$

for all $y \in G$. This proves that every $a \in G$ $(a = \varphi^{-1}(y))$ may be written as $a = z + z$.

If also $a = u + u$ for some $u \in G$, then there exists $v \in G$ such that $u = \psi(v)$. Hence

$$a = \psi(v) + \psi(v) = \varphi^{-1}(v)\,,$$

which gives $\varphi^{-1}(y) = \varphi^{-1}(v)$. Thus $y = v$ and, in the consequence, $z = u$. This proves that the equation $a = z + z$ has a unique solution for every $a \in G$.

Conversely, assume that $(G, +)$ is a commutative group in which for every $a \in G$ there is only one $x = \frac{1}{2}a$ such that $x + x = a$. If φ and ψ are automorphisms of $(G, +)$ satisfying (3) and (4), then a groupoid $(G, \cdot)$ defined by (2) is a quasigroup and its quasigroup operation may be written in the form

$$xy = x + \psi(y - x). \tag{7}$$

From (3) and (4) we obtain also

$$\psi^2(x) - \psi(x) = \frac{1}{2}\,x$$

for all $x \in G$.

This together with (7) (after some simplifications) gives

$$xy \cdot x = x - \psi(x) + \psi^2(x) + \psi(y) - \psi^2(y) = \tfrac{1}{2}\,x + \tfrac{1}{2}\,y\,,$$

$$zx \cdot yz = \psi(x) - \psi^2(x) + \psi(y) - \psi^2(y) + z - 2\psi(z) + 2\psi^2(z) = \tfrac{1}{2}\,x + \tfrac{1}{2}\,y,$$

which proves (1). Hence this groupoid is a quadratical quasigroup. □

Corollary 1. *A finite quadratical quasigroup has odd order.*

Proof. Indeed, by Cauchy's theorem, in a group of even order there are at least two elements x satisfying $x + x = 0$. □

Corollary 2. *A quadratical groupoid defined by the additive group of a field* $(F, +, \cdot)$ *with char* $F \neq 2$ *has the form*

$$x * y = ax + (1 - a)y\,,$$

where $a \in F$ *is a solution of the equation*

$$2a^2 - 2a + 1 = 0\,. \tag{8}$$

Proof. All automorphisms of the additive group of F have the form $\varphi(x) = ax$, where $a \in F$. Moreover, (3) and (4) are equivalent to (8). Hence a quasigroup defined by $\varphi(x) = ax$ and $\psi(x) = (1 - a)x$ is quadratical if and only if a satisfies (8). □

Now we compute all quadratical quasigroups of order $n \leq 24$. As it is well known commutative groups of odd order $n \leq 24$ are (up to isomorphism) either Z_n or $Z_3 \times Z_3$. In the first case all automorphisms have the form $\varphi(x) = ax$, where $a \in \{1, 2, ..., n - 1\}$. Hence, by the Theorem, all quadratical quasigroups defined on Z_n have the form $xy = ax + by$, where $a + b \equiv 1 (mod\ n)$, $2ab \equiv 1 (mod\ n)$ and n is odd. Direct computations show that for odd $n \leq 24$ the last two equations have solutions (listed bellow) only for $n = 5, 13, 17$.

n	5		13		17	
a	2	4	3	11	7	11
b	4	2	11	3	11	7

This means that a quadratical quasigroup defined on the group Z_n, $n \leq 24$, has the form

$$\begin{aligned}
x * y &= 2x + 4y (mod\ 5),\\
x * y &= 4x + 2y (mod\ 5),\\
x * y &= 3x + 11y (mod\ 13),\\
x * y &= 11x + 3y (mod\ 13),\\
x * y &= 7x + 11y (mod\ 17),\\
x * y &= 11x + 7y (mod\ 17).
\end{aligned}$$

In the second case, all automorphisms are determined (as a linear transformations of the vector space $Z_3 \times Z_3$) by some matrices (in the basis $e_1 = (1,0)$, $e_2 = (0,1)$) such that $A + B \equiv I(mod\ 3)$ and $2AB \equiv I(mod\ 3)$. Direct calculations show that the matrix A has the forms:

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \quad \begin{bmatrix} 0 & 2 \\ 2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 \\ 2 & 0 \end{bmatrix}, \quad \begin{bmatrix} 2 & 1 \\ 2 & 2 \end{bmatrix}, \quad \begin{bmatrix} 2 & 2 \\ 1 & 2 \end{bmatrix}.$$

Computing B and replacing obtained matrices by corresponding linear transformations, we see that the quadratical quasigroup defined on the group $Z_3 \times Z_3$ has one of the following forms:

$$(x,y) * (z,u) = (y + z + 2u\,,\ x + y + 2z),$$
$$(x,y) * (z,u) = (2y + z + u\,,\ 2x + y + z),$$
$$(x,y) * (z,u) = (x + y + 2u\,,\ x + 2z + u),$$
$$(x,y) * (z,u) = (x + 2y + u\,,\ 2x + z + u),$$
$$(x,y) * (z,u) = (2x + y + 2z + 2u\,,\ 2x + 2y + z + 2u),$$
$$(x,y) * (z,u) = (2x + 2y + 2z + u\,,\ x + 2y + 2z + 2u).$$

References

[1] **V. D. Belousov**: *Transitive distributive quasigroups*, (Russian), Ukrain. Math. Zh. **10** (1958), 13 – 22.

[2] **V. D. Belousov**: *Fundations of the theory of quasigroups and loops*, (Russian), Nauka, Moscow 1967.

[3] **M. Osborn**; *New loops from old geometries*, Amer. Math. Monthly **68** (1961), 103 – 107.

[4] **V. Volenec**: *Quadratical groupoids*, Note di Mat. **13** (1993), 107 – 115.

Received December 15, 1997

Institute of Mathematics
Technical University
Wybrzeże Wyspiańskiego 27
50-370 Wrocław
Poland
e-mail: dudek@im.pwr.wroc.pl