Proceedings of the Third Conference of Mathematical Society of Moldova
IMCS-50, August 19-23, 2014, Chisinau, Republic of Moldova

On recursive differentiability of binary quasigroups

Inga Larionova-Cojocaru, Parascovia Syrbu

Abstract

A quasigroup is called recursively n-differentiable if its first n recursive derivatives are quasigroups. The class of recursively differential quasigroups is arisen in the theory of MDS codes, in early 2000. Connections between recursive derivatives of different order are found in the present work. It is shown that isomorphic quasigroups have isomorphic recursive derivatives of any order. Also, it is proved that, if the recursive derivative of order one of a finite quasigroup $(Q, \cdot)$ is commutative, then its group of inner mappings is a subgrup of the group of inner mappings of $(Q, \cdot)$, of the same index as their corresponding multiplication groups.

Keywords: recursively differential quasigroup, recursive derivative, the group of inner mappings.

If $(Q, \cdot)$ is a binary quasigroup, then the operations $(\overset{i}{\cdot})$, defined as follows:

$$x \overset{0}{\cdot} y = x \cdot y,\ x \overset{1}{\cdot} y = y \cdot (x \overset{0}{\cdot} y),\ x \overset{2}{\cdot} y = (x \overset{0}{\cdot} y) \cdot (x \overset{1}{\cdot} y),\ \ldots,$$
$$x \overset{n}{\cdot} y = (x \overset{n-2}{\cdot} y) \cdot (x \overset{n-1}{\cdot} y),$$

$\forall n \geq 2$, and $\forall x, y \in Q$, are called the recursive derivatives of the operation $(\cdot)$, or of the quasigroup $(Q, \cdot)$. A quasigroup $(Q, \cdot)$ is called recursively n-differentiable if its first n recursive derivatives are quasigroup operations. The notions of recursive derivative and recursively differentiable quasigroup arose in the theory of recursive MDS (maximum distance separable) codes [2]. The recursive derivatives of a quasigroup are not always quasigroups. A necessary and sufficient condition when a finite abelian group is recursively s-differentiable is given in [3],

for an arbitrary positive integer s. It is known that there exist recursively 1-differentiable finite quasigroups of order q, for every integer q, excepting $q = 6$ and possibly $q \neq 14, 18, 26$ (see [2,3]). Connections between recursive derivatives of different order are found in the present work. We show that isomorphic quasigroups have isomorphic recursive derivatives of any order and that the group of automorphisms of a quasigroup is a subgroup of the group of automorphisms of all its recursive derivatives. Also, it is proved that, if the recursive derivative $(Q, \circ)$ of order one of a finite quasigroup $(Q, \cdot)$ is commutative, then its group of inner mappings is a subgroup of the group of inner mappings of $(Q, \cdot)$ (with respect to the same element $h \in Q$) and $|M(Q, \cdot) : M(Q, \circ)| = |I_h^{(\cdot)} : I_h^{(\circ)}|$.

Proposition 1. *Let $(Q, \cdot)$ be a binary groupoid and $n \geq 2$ be a fixed positive integer. Then, for $\forall j = 1, \ldots, n-1$ and for $\forall x, y \in Q$, the following equality holds:*

$$x \overset{n}{\cdot} y = (x \overset{j-1}{\cdot} y) \overset{n-j-1}{\cdot} (x \overset{j}{\cdot} y). \tag{1}$$

Proof. We will use the mathematical induction. If $n = 2$, then $j = 1$ and: $x \overset{2}{\cdot} y = (x \overset{0}{\cdot} y) \overset{0}{\cdot} (x \overset{1}{\cdot} y)$, $\forall x, y \in Q$. Suppose that (1) is true for all natural numbers $2 \leq n \leq k$. Then, for $n = k + 1$, we get:

$$x \overset{k+1}{\cdot} y = (x \overset{k-1}{\cdot} y) \overset{0}{\cdot} (x \overset{k}{\cdot} y) =$$
$$[(x \overset{j-1}{\cdot} y) \overset{(k-1)-(j+1)}{\cdot} (x \overset{j}{\cdot} y)] \overset{0}{\cdot} [(x \overset{j-1}{\cdot} y) \overset{k-(j+1)}{\cdot} (x \overset{j}{\cdot} y)] =$$
$$(x \overset{j-1}{\cdot} y) \overset{(k+1)-(j+1)}{\cdot} (x \overset{j}{\cdot} y). \ \square$$

Proposition 2. *Let $(Q, \cdot)$ be a binary groupoid. Then, for every positive integer n and $\forall x, y \in Q$, the following equality holds:*

$$x \overset{n}{\cdot} y = y \overset{n-1}{\cdot} (x \overset{0}{\cdot} y) \tag{2}$$

Proof. We will use the mathematical induction. If $n = 1$, then $x \overset{1}{\cdot} y = y \overset{0}{\cdot} (x \overset{0}{\cdot} y)$. Suppose that the equality (2) is true for all positive integers $n \leq k$. Then, for $n = k + 1$, we get:

$$x \overset{k+1}{\cdot} y = (x \overset{k-1}{\cdot} y) \overset{0}{\cdot} (x \overset{k}{\cdot} y) =$$
$$= [y \overset{k-2}{\cdot} (x \overset{0}{\cdot} y)] \overset{0}{\cdot} [y \overset{k-1}{\cdot} (x \overset{0}{\cdot} y)] = y \overset{k}{\cdot} (x \overset{0}{\cdot} y),$$

for every $x, y \in Q$. $\square$

Proposition 3. *If two binary quasigroups $(Q, \cdot)$ and $(Q_1, \circ)$ are isomorphic, then their recursive derivatives $(Q, \overset{n}{\cdot})$ and $(Q_1, \overset{n}{\circ})$ are isomorphic, for every natural n.*

Proof. If φ is an isomorphism from $(Q, \cdot)$ to $(Q_1, \circ)$, then $\varphi(x \overset{1}{\cdot} y) = \varphi[y \cdot (x \cdot y)] = \varphi(y) \circ (\varphi(x) \circ \varphi(y)) = \varphi(x) \overset{1}{\circ} \varphi(y)$, $\varphi(x \overset{2}{\cdot} y) = \varphi[(x \cdot y) \cdot (x \overset{1}{\cdot} y)] = [(\varphi(x) \cdot \varphi(y)) \cdot (\varphi(x) \overset{1}{\cdot} \varphi(y))] = \varphi(x) \overset{2}{\circ} \varphi(y)$, ..., $\varphi(x \overset{n}{\cdot} y) = \varphi[(x \overset{n-2}{\cdot} y) \cdot (x \overset{n-1}{\cdot} y)] = (\varphi(x) \overset{n-2}{\circ} \varphi(y)) \circ (\varphi(x) \overset{n-1}{\circ} \varphi(y)) = \varphi(x) \overset{n}{\circ} \varphi(y)$, $\forall x, y \in Q$, i.e. φ is an isomorphism from $(Q, \overset{n}{\cdot})$ to $(Q_1, \overset{n}{\circ})$. $\square$

Proposition 4. *If $(Q, \cdot)$ is a quasigroup, then $Aut(Q, \cdot)$ is a subgroup of $Aut(Q, \overset{n}{\cdot})$, for every natural n.*

Proof. Let $\varphi \in Aut(Q, \cdot)$. Then $\varphi(x \overset{1}{\cdot} y) = \varphi(y \cdot (x \cdot y)) = \varphi(y) \cdot (\varphi(x) \cdot \varphi(y)) = \varphi(x) \overset{1}{\cdot} \varphi(y)$. So $Aut(Q, \cdot) \leq Aut(Q, \overset{1}{\cdot})$. Now, suppose that $Aut(Q, \cdot) \leq Aut(Q, \overset{i}{\cdot})$, $\forall i = 0, 1, ..., n-1$. Then,

$$\varphi(x \overset{n}{\cdot} y) = \varphi((x \overset{n-2}{\cdot} y) \cdot (x \overset{n-1}{\cdot} y)) = \varphi(x \overset{n-2}{\cdot} y) \cdot \varphi(x \overset{n-1}{\cdot} y) =$$
$$(\varphi(x) \overset{n-2}{\cdot} \varphi(y)) \cdot (\varphi(x) \overset{n-1}{\cdot} \varphi(y)) = \varphi(x) \overset{n}{\cdot} \varphi(y),$$

hence $Aut(Q, \cdot) \leq Aut(Q, \overset{n}{\cdot})$, for every natural number n. $\square$

Let $(Q, \cdot)$ be a quasigroup and let $M(Q, \cdot)$ be its multiplication group. Following [1], we will denote the group of inner mappings of $(Q, \cdot)$, with respect to an element $h \in Q$, by $I_h^{(\cdot)}$.

Proposition 5. *If $(Q, \cdot)$ is a quasigroup with a commutative recursive derivative $(Q, \circ)$ of order one, then $I_h^{(\cdot)}$ is a subgroup of $I_h^{(\circ)}$.*

Proof. So as $R_x^{(\circ)}(y) = y \circ x = x \cdot (y \cdot x) = L_x^{(\cdot)} R_x^{(\cdot)}(y)$, $\forall x, y \in Q$, we get that $RM(Q, \circ) \subseteq M(Q, \cdot)$. If the recursive derivative $(Q, \circ)$ is commutative, then $M(Q, \circ) = RM(Q, \circ) \subseteq M(Q, \cdot)$. So $I_h^{(\circ)} = M(Q, \circ)_h \leq M(Q, \cdot)_h = I_h^{(\cdot)}$, where $M(Q, \circ)_h$ (resp. $M(Q, \cdot)_h$) is the centralizer of h in $M(Q, \circ)$ (resp., in $M(Q, \cdot)$). $\square$

Corollary. *If $(Q,\cdot)$ is a finite quasigroup with a commutative recursive derivative $(Q,\circ)$ of order one, then*

$$|M(Q,\cdot):M(Q,\circ)| = |I_h^{(\cdot)} : I_h^{(\circ)}|.$$

Proof. According to the previous proposition, if the recursive derivative $(Q,\circ)$ of order one is commutative, then $I_h^{(\circ)}$ is a subgroup of $I_h^{(\cdot)}$ and $M(Q,\circ)$ is a subgroup of $M(Q,\cdot)$. Now, using the equality $|M(Q,\cdot)| = |Q| \cdot |I_h^{(\cdot)}|$, we have:

$$|Q| = \frac{|M(Q,\cdot)|}{|I_h^{(\cdot)}|} = \frac{|M(Q,\circ)|}{|I_h^{(\circ)}|} \Rightarrow \frac{|M(Q,\cdot)|}{|M(Q,\cdot)|} = \frac{|I_h^{(\circ)}|}{|I_h^{(\circ)}|},$$

which implies $|M(Q,\cdot):M(Q,\circ)| = |I_h^{(\cdot)} : I_h^{(\circ)}|$. □

References

[1] V. Belousov. *Foundations of the theory of quasigroups and loops*, Nauka, Moscow, 1967 (in Russian).

[2] S. Gonzalez, E. Couselo, V.T. Markov, A.A. Nechaev. *Recursive MDS-codes and recursively differentiable quasigroups*, Diskr. Mat., 10:2 (1998), pp. 3–29 (in Russian).

[3] Izbash V., Syrbu P. *Recursively differentiable quasigroups and complete recursive codes*. Commentat. Math. Univ. Carol. 45, No. 2 (2004), pp. 257–263.

[1]Larionova-Cojocaru Inga, [2]Syrbu Parascovia

Moldova State University
Email: [1]larionovainga@yahoo.com; [2]syrbuviv@yahoo.com