ROMAI J., v.13, no.2(2017), 55–58

# ON DEFINITION OF CI-QUASIGROUP

Natalia Didurik[1], Victor Shcherbacov[2]
[1] *University of the Academy of Sciences of Moldova, Chişinău, Moldova*
[2] *Institute of Mathematics and Computer Science, Academy of Sciences of Moldova, Chişinău, Moldova*
natnikkr83@mail.ru, scerb@math.md

**Abstract** Groupoid $(Q, \cdot)$ in which equality $(xy)Jx = y$ is true for all $x, y \in Q$, where $J$ is a map of the set $Q$, is a CI-quasigroup.

**Keywords:** quasigroup, loop, CI-quasigroup, CI-groupoid, left CI-groupoid.
**2010 MSC:** 20N05.

## 1. INTRODUCTION

Necessary definitions and concepts can be found in [4, 2, 9, 10].

**Definition 1.1.** *Binary groupoid $(Q, \circ)$ is called a left quasigroup if for any ordered pair $(a, b) \in Q^2$ there exists the unique solution $y \in Q$ to the equation $a \circ y = b$ [2, 10].*

**Definition 1.2.** *Binary groupoid $(Q, \circ)$ is called a right quasigroup if for any ordered pair $(a, b) \in Q^2$ there exists the unique solution $x \in Q$ to the equations $x \circ a = b$ [2, 10].*

**Definition 1.3.** *Binary groupoid $(Q, \circ)$ is called a quasigroup if for any ordered pair $(a, b) \in Q^2$ there exist the unique solutions $x, y \in Q$ to the equations $x \circ a = b$ and $a \circ y = b$ [2, 10].*

**Definition 1.4.** *A quasigroup $(Q, \cdot)$ with an element $1 \in Q$, such that $1 \cdot x = x \cdot 1 = x$ for all $x \in Q$, is called a loop.*

**Definition 1.5.** *Loop $(Q, \cdot)$ satisfying one of the equivalent identities $x \cdot yJx = y$, $xy \cdot Jx = y$, where $J$ is a bijection of the set $Q$ such that $x \cdot Jx = 1$, is called a CI-loop.*

CI-loops are classical objects of quasigroup theory. This loop class was defined by Rafael Artzy [1]. In [1] it is proved that $J$ is an automorphism of loop $(Q, \cdot)$.

V.D. Belousov and B.V. Tsurkan defined CI-quasigroups in [3]. Some applications of CI-quasigroups in cryptology are presented in [7, 5].

**Definition 1.6.** *Quasigroup $(Q, \cdot)$ with the identity $xy \cdot Jx = y$, where $J$ is a map of the set $Q$, is called a CI-quasigroup [3].*

Notice, in this case the map $J$ is a permutation of the set $Q$ [3]. In any CI-quasigroup the permutation $J$ is unique [10, Lemma 2.25].

**Definition 1.7.** *Groupoid* $(Q, \cdot)$ *with the identity*

$$xy \cdot J_r x = y, \tag{1}$$

*where* $J_r$ *is a map of the set* $Q$ *into itself, is called a left CI-groupoid.*

*Groupoid* $(Q, \cdot)$ *with the identity*

$$J_l x \cdot yx = y, \tag{2}$$

*where* $J_l$ *is a map of the set* $Q$ *into itself, is called a right CI-groupoid.*

*Groupoid* $(Q, \cdot)$ *with both identities (1) and (2) is called a CI-groupoid.*

Definition 1.7 is given in [3]. A groupoid with the equations (1) and (2) is called a CI-groupoid in [6].

In fundamental article [3] the following facts are proved: any CI-groupoid is a quasigroup; in CI-quasigroup the identities (1) and (2) are equivalent; any left CI-groupoid is a left quasigroup.

From the results of Keedwell and Shcherbacov (see, for example, [10, Proposition 3.28]) it follows that the left CI-groupoid in which the map $J_r$ is bijective, is a CI-quasigroup.

Any finite left CI-groupoid is a CI-quasigroup [6].

**Example 1.1.** *The following example of CI-quasigroup is constructed using Mace 4 [8].*

| * | 0 | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 0 | 3 | 4 | 5 | 1 | 0 | 2 |
| 1 | 5 | 3 | 4 | 2 | 1 | 0 |
| 2 | 4 | 5 | 3 | 0 | 2 | 1 |
| 3 | 2 | 0 | 1 | 3 | 5 | 4 |
| 4 | 0 | 1 | 2 | 5 | 4 | 3 |
| 5 | 1 | 2 | 0 | 4 | 3 | 5 |

Constructions of sufficiently large classes of CI-quasigroups are given in [7], [10, Theorem 3.48].

In this note we prove that any right (left) CI-groupoid is a CI-quasigroup.

## 2. RESULT

**Lemma 2.1.** *Any left CI-groupoid is a left quasigroup [3].*

*Proof.* We prove that in the left CI-groupoid $(Q, \cdot)$ the equation

$$a \cdot x = b \tag{3}$$

has the unique solution. From the equation (3) we have $ax \cdot J_r a = b \cdot J_r a$, $x = b \cdot J_r a$. If we substitute the last expression in (3), then we obtain the following equality:

$$a \cdot bJ_r a = b. \tag{4}$$

Uniqueness. Suppose that there exist two solutions of equation (3), say, $x_1$ and $x_2$. Then $ax_1 = ax_2$, $ax_1 \cdot J_r a = ax_2 \cdot J_r a$ and from the equality (1) we obtain that $x_1 = x_2$.

Therefore any left translation $L_x$ of groupoid $(Q, \cdot)$ is a bijective map. ∎

We denote by the letter $\mathcal{L}$ set of all left translations of a CI-groupoid $(Q, \cdot)$ and by the letter $\mathcal{R}$ we denote set of all translations of the form $R_{J_r x}$ of a CI-groupoid $(Q, \cdot)$.

**Lemma 2.2.** *There exists a bijection between the set $Q$ and the set $\mathcal{R}$, the map $J_r$ is bijective and $J_r Q = Q$.*

*Proof.* We can rewrite the identity (1) in the following translation form:

$$R_{J_r x} L_x = \varepsilon. \tag{5}$$

From the equality (5) and Lemma 2.1 it follows that the map $R_{J_r d}$ is a bijection of the set $Q$ for any fixed element $d \in Q$.

There exists a bijection between the set $Q$ and the set $\mathcal{L}$ of all left translations of groupoid $(Q, \cdot)$. Namely $x \leftrightarrow L_x$, $Q \leftrightarrow \mathcal{L}$.

From the equality (5) we have that there exists a bijection between the set $\mathcal{L}$ and the set $\mathcal{R}$ of all translations (bijections) of the form $R_{J_r x}$, namely, $L_x \leftrightarrow R_{J_r x}$, $\mathcal{L} \leftrightarrow \mathcal{R}$.

Therefore there exists a bijection between the set $Q$ and the set $\mathcal{R}$, the map $J_r$ is bijective and $J_r Q = Q$. ∎

**Theorem 2.1.** *Any left CI-groupoid $(Q, \cdot)$ is a CI-quasigroup.*

*Proof.* Taking into consideration Lemma 2.1 we must only prove that in the left CI-groupoid $(Q, \cdot)$ the equation

$$y \cdot a = b \tag{6}$$

has the unique solution for any fixed elements $a, b \in Q$. Using the language of translations we re-write the equation (6) in the following form: $R_a y = b$. Thus right translation $R_a$ exists for any $a \in Q$. By Lemma 2.2 the map $R_a$ is a bijection. Then $y = R_a^{-1} b$.

Therefore any left CI-groupoid $(Q, \cdot)$ is a CI-quasigroup. ∎

It is clear that the similar theorem is true for any right CI-groupoid.

Notice, Theorem 2.1 can be proved using Lemmas 2.1, 2.2 and Proposition 3.28 from [10].

## 3. CONCLUSION

The main result of this paper is Theorem 2.1 in which it is proved that any left CI-groupoid $(Q, \cdot)$ is a CI-quasigroup.

**Acknowledgement.** The authors thank Referee for valuable suggestions.

## References

[1] R. Artzy, *On loops with a special property*, Proc. Amer. Math. Soc., 6(1955), 448–453.

[2] V.D. Belousov, *Foundations of the Theory of Quasigroups and Loops*, Nauka, Moscow, 1967. (in Russian).

[3] V.D. Belousov, B.V. Tsurkan, *Crossed-inverse quasigroups (CI-quasigroups)*, Izv. Vyssh. Uchebn. Zaved. Mat., 82(3):21–27, 1969. (in Russian).

[4] R.H. Bruck, *A Survey of Binary Systems*, Springer Verlag, New York, third printing, corrected edition, 1971.

[5] J. Dénes, A. D. Keedwell, *Some applications of non-associative algebraic systems in cryptology*, P.U.M.A., 12(2)(2002), 147–195.

[6] V. Izbash, N. Labo. *Crossed-inverse-property groupoids*, Bul. Acad. tiine Repub. Mold. Mat., (2)(2007), 101–106.

[7] A.D. Keedwell, *Crossed-inverse quasigroups with long inverse cycles and applications to cryptography*, Australas. J. Combin., 20(1999), 241–250.

[8] W. McCune, *Mace 4*, University of New Mexico, www.cs.unm.edu/mccune/prover9/, 2007.

[9] H.O. Pflugfelder, *Quasigroups and Loops: Introduction*, Heldermann Verlag, Berlin, 1990.

[10] Victor Shcherbacov, *Elements of Quasigroup Theory and Applications*, CRC Press, Boca Raton, 2017.