Equational quasigroup definitions

V.A. Shcherbacov*, D.I. Pushkashu*, A.V. Shcherbacov**

March 17, 2010

Abstract

Quasigroup equational definitions are given.

2000 Mathematics Subject Classification: 20N05

Key words and phrases: quasigroup, equational quasigroup

Basic and standard definition of a binary quasigroup is the following

Definition 1. Binary groupoid \((Q, \circ)\) is called a quasigroup if for all ordered pairs \((a, b) \in Q^2\) there exist unique solutions \(x, y \in Q\) to the equations \(x \circ a = b\) and \(a \circ y = b\) [1].

T. Evans has given equational definition of a quasigroup [5] (see Definition 2). Evans’ definition usually used by the study of universal algebraic questions of quasigroup theory. The equivalence of Definitions 1 and 2 is well known fact [1, 8].

In this paper we give some new equational definitions of quasigroups. The subject of this paper is close with the subject of articles [9, 10].

We shall use basic terms and concepts from books [1, 2, 7].

Garrett Birkhoff in his famous book [3] defined equational quasigroup as a algebra with three binary operations \((Q, \cdot, /, \backslash)\) that fulfil the following six identities

\[
x \cdot (x \backslash y) = y \quad (1)
\]
\[
(y/x) \cdot x = y \quad (2)
\]
\[
x \cdot (x \cdot y) = y \quad (3)
\]
\[
(y \cdot x)/x = y \quad (4)
\]
\[
x/(y \backslash x) = y \quad (5)
\]
\[
(x/y) \backslash x = y \quad (6)
\]

Results of this paper are connected with the following
Problem 1. Research properties of algebra \((Q, \cdot, \backslash, /)\) with various combinations of identities \((1)\)–\((6)\) ([8], page 11).

It is well known the following

**Lemma 1.** In algebra \((Q, \cdot, \backslash, /)\) with identities \((1), (2), (3), \) and \((4)\) identities \((5)\) and \((6)\) are true [11, 8, 9].

**Proof.** We can re-write identity \((4)\) in the following form

\[
(x \cdot (x\backslash y)) / (x\backslash y) = x
\]

(7)

By identity \((1)\) \(x \cdot (x\backslash y) = y\). Thus from identity \((7)\) we obtain \(y / (x\backslash y) = x\), i.e. we obtain identity \((5)\).

We can re-write identity \((3)\) in the following form

\[
(x/y) \backslash ((x/y) \cdot y) = y
\]

(8)

By identity \((2)\) \((x/y) \cdot y = x\). Thus from identity \((8)\) we obtain \((x/y) \backslash x = y\), i.e. we obtain identity \((6)\).

Therefore it is used the following T. Evans’ equational definition of a quasigroup [5].

**Definition 2.** An algebra \((Q, \cdot, \backslash, /)\) with identities \((1), (2), (3)\) and \((4)\) is called a quasigroup [5, 3, 1, 2, 7, 4].

**Lemma 2.** In algebra \((Q, \cdot, \backslash, /)\) from identities \((2)\) and \((5)\) it follows identity \((1)\).

**Proof.** We can re-write identity \((2)\) in the following form

\[
(x / (y\backslash x)) \cdot (y\backslash x) = x
\]

(9)

But by identity \((5)\) \(x / (y\backslash x) = y\). Therefore we can rewrite identity \((9)\) in the following form

\[
y \cdot (y\backslash x) = x
\]

(10)

Then we obtain identity \((1)\).

**Lemma 3.** In algebra \((Q, \cdot, \backslash, /)\) from identities \((3)\) and \((5)\) it follows identity \((4)\).

**Proof.** We can re-write identity \((3)\) in the following form

\[
(x \cdot y) / (x\backslash (x \cdot y)) = x
\]

(11)

But by identity \((3)\) \(x\backslash (x \cdot y) = y\). Therefore identity \((11)\) takes the form \((x \cdot y) / y = x\) and it coincides with identity \((4)\).
**Lemma 4.** In algebra \((Q, \cdot, \backslash, /)\) from identities (4) and (6) it follows identity (3).

*Proof.* We can re-write identity (6) in the following form
\[
((x \cdot y)/y) \backslash (x \cdot y) = y \tag{12}
\]
But by identity (4) \((x \cdot y)/y) = x\). Therefore identity (12) takes the form \(x \backslash (x \cdot y) = y\) and it coincides with identity (3).

**Lemma 5.** In algebra \((Q, \cdot, \backslash, /)\) from identities (1) and (6) it follows identity (2).

*Proof.* We can re-write identity (1) in the following form
\[
(x/y) \cdot ((x/y) \backslash x) = x \tag{13}
\]
But by identity (6) \((x/y) \backslash x = y\). Therefore identity (13) takes the form \((x/y) \cdot y = x\) and it coincides with identity (2).

**Theorem 1.** An algebra \((Q, \cdot, \backslash, /)\) with identities (2), (3) and (5) is a quasigroup.

*Proof.* The proof follows from Lemmas 2 and 3.

**Theorem 2.** An algebra \((Q, \cdot, \backslash, /)\) with identities (1), (4) and (6) is a quasigroup.

*Proof.* The proof follows from Lemmas 4 and 5.

In the following corollary we give definitions of equational quasigroup using four identities from the identities (1)--(6).

**Corollary 1.**
1. An algebra \((Q, \cdot, \backslash, /)\) with identities (1), (2), (3) and (5) is a quasigroup.
2. An algebra \((Q, \cdot, \backslash, /)\) with identities (2), (3), (4) and (5) is a quasigroup.
3. An algebra \((Q, \cdot, \backslash, /)\) with identities (1), (2), (4) and (5) is a quasigroup.
4. An algebra \((Q, \cdot, \backslash, /)\) with identities (1), (3), (4) and (5) is a quasigroup.
5. An algebra \((Q, \cdot, \backslash, /)\) with identities (1), (2), (3) and (6) is a quasigroup.
6. An algebra \((Q, \cdot, \backslash, /)\) with identities (2), (3), (4) and (6) is a quasigroup.
7. An algebra \((Q, \cdot, \backslash, /)\) with identities (2), (4), (5) and (6) is a quasigroup.
8. An algebra \((Q, \cdot, \backslash, /)\) with identities (3), (4), (5) and (6) is a quasigroup.

*Proof.* The proof follows from Theorems 1 and 2, Lemmas 2, 3, 4 and 5.
The proofs of Lemmas 2, 3, 4 and 5 are obtained using Prover 9 [6].

Information on properties of algebras with 3-element sets of identities that are taken from identities (1)–(4) it is possible to deduce from results of the articles [9, 10]. For example, algebra $(Q, \cdot, /, \backslash)$ with identities (1), (2), (3) is a left quasigroup with right division.

**Example 1.** Let $x \circ y = \lfloor x/2 \rfloor - 1 \cdot y$ for all $x, y \in \mathbb{Z}$, where $(\mathbb{Z}, +, \cdot)$ is the ring of integers, $\lfloor x/2 \rfloor = a$, if $x = 2 \cdot a$; $\lfloor x/2 \rfloor = a$, if $x = 2 \cdot a + 1$. It is possible to check that $(\mathbb{Z}, \circ)$ is a left quasigroup with right division.

**References**

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

[2] V.D. Belousov. *Elements of Quasigroup Theory: a special course*. Kishinev State University Printing House, Kishinev, 1981. (in Russian).

[3] G. Birkhoff. *Lattice Theory*. Nauka, Moscow, 1984. (in Russian).

[4] S. Burris and H.P. Sankappanavar. *A Course in Universal Algebra*. Springer-Verlag, 1981.

[5] T. Evans. Abstract mean values. *Duke Math. J.*, 30:331–347, 1963.

[6] W. McCune. *Prover 9*. University of New Mexico, www.cs.unm.edu/mccune/prover9/, 2007.

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

[8] V.A. Shcherbacov. Elements of quasigroup theory and some its applications in code theory, 2003. www.karlin.mff.cuni.cz/ drapal/speccurs.pdf.

[9] V.A. Shcherbacov. On definitions of groupoids closely connected with quasigroups. *Bul. Acad. Stiinte Repub. Mold., Mat.*, (2):43–54, 2007.

[10] V.A. Shcherbacov, A.Kh. Tabarov, and D.I. Pushkashu. On congruences of groupoids closely connected with quasigroups. *Fundam. Prikl. Mat.*, 14(1):237–251, 2008.

[11] J.D.H. Smith. *An introduction to Quasigroups and Their Representation*. Studies in Advanced Mathematics. Chapman and Hall/CRC, London, 2007.

*Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
5 Academiei str., MD–2028, Chișinău
Moldova
E-mail: scerb@math.md
dmitry.pushkashu@gmail.com

**Moldova State University
A. Mateevici str. 60, MD-2009, Chișinău
Moldova
E-mail: admin@sibirsky.org*