Quasigroups and Related Systems **14** (2006), 157 – 162

Finite hexagonal quasigroups

Mea Bombardelli

Abstract

In this article some examples of finite hexagonal (idempotent, medial and semisymmetric) quasigroups are given. The main goal is to determine the set of possible orders of finite hexagonal quasigroups.

1. Introduction

Hexagonal quasigroups are defined by V. Volenec in [1] as follows:

Definition. A quasigroup $(Q, \cdot)$ is said to be *hexagonal* if it is idempotent, medial and semisymmetric, i.e., if the equalities

$$\begin{aligned} &a \cdot a = a, \\ &ab \cdot cd = ac \cdot bd, \\ &a \cdot ba = ab \cdot a = b \end{aligned}$$

hold for all its elements.

Study of hexagonal quasigroups in [1] and [2] is motivated by

Example 1. On the set $\mathbb{C}$ of complex numbers the operation $*$ is defined by:

$$a * b = \frac{1 - i\sqrt{3}}{2}\, a + \frac{1 + i\sqrt{3}}{2}\, b.$$

If we identify the complex numbers with the points of the Euclidean plane, the points a, b and $a * b$ are the vertices of a positively oriented equilateral triangle.

2000 Mathematics Subject Classification: 20N05
Keywords: hexagonal quasigroup, finite quasigroups, order, IM quasigroup

In this paper, we'll give some examples of finite hexagonal quasigroups, and answer the question: *for which positive integers n there exists a hexagonal quasigroup of order n?*

We'll need some elementary results.

Lemma 1. *Let $(Q_1, \cdot_1)$, $(Q_2, \cdot_2), \ldots, (Q_n, \cdot_n)$ be hexagonal quasigroups, and let $\circ$ be the operation defined on $Q = Q_1 \times Q_2 \times \ldots \times Q_n$ by:*

$$(x_1, x_2, \ldots, x_n) \circ (y_1, y_2, \ldots, y_n) = (x_1 \cdot_1 y_1, x_2 \cdot_2 y_2, \ldots, x_n \cdot_n y_n).$$

Then $(Q, \circ)$ is a hexagonal quasigroup.

Therefore, if a hexagonal quasigroup of order m exists, then there exists hexagonal quasigroup of order m^n, for each $n \in \mathbb{N}$. If hexagonal quasigroups of orders k_1, k_2,... k_n exist, then a hexagonal quasigroup of order $k_1 k_2 \cdots k_n$ exists.

A *subquasigroup* of the quasigroup $(Q, \cdot)$ is any subset $S \subset Q$ such that $(S, \cdot)$ is a quasigroup. Obviously, any subquasigroup of a hexagonal quasigroup is hexagonal.

For any quasigroup $(Q, \cdot)$ and its subset A, the smallest quasigroup that contains A is the intersection of all subquasigroups of Q that contain A.

Example 2. Let $(D, *)$ be the smallest subquasigroup of $(\mathbb{C}, *)$ (as in Example 1) that contains 0 and 1. D can be represent by triangular lattice with the same operation as in $(\mathbb{C}, *)$: the product of two points a and b is the third vertex of regular triangle with vertices a and b.

If $q = \frac{1}{2} + i\frac{\sqrt{3}}{2}$, then $D = \{x + qy : x, y \in \mathbb{Z}\}$, and it can be identified with the set $\{(x, y) : x, y \in \mathbb{Z}\}$. It's easy to verify:

$$\begin{aligned}(x_1, y_1) * (x_2, y_2) &= (1 - q)(x_1 + qy_1) + q(x_2 + qy_2) \\ &= (x_1 + y_1 - y_2, x_2 + y_2 - x_1).\end{aligned}$$

We obtained an important example of hexagonal quasigroup:

Theorem 1. *Let $(G, +)$ be a commutative group. The set $G \times G$ with the operation*

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 + y_1 - y_2, x_2 + y_2 - x_1)$$

is a hexagonal quasigroup.

Therefore, a hexagonal quasigroup of order n^2 exists for any $n \in \mathbb{N}$.

The following characterization of hexagonal quasigroups was given in [1].

Theorem 2. *A hexagonal quasigroup on the set Q exists if and only if on the same set exists commutative group with automorphism φ satisfying*

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

for all $a \in Q$.

Given such commutative group $(Q, +)$, the quasigroup is obtained by

$$a \cdot b = a + \varphi(b - a). \tag{2}$$

Note that from (1) it follows

$$\varphi^3(x) = \varphi(\varphi(x) - x) = \varphi \circ \varphi(x) - \varphi(x) = (\varphi(x) - x) - \varphi(x) = -x$$

and $\varphi^6(x) = x$ for all $x \in Q$.

2. Commutative hexagonal quasigroups

Let us use the Theorem 2 to study commutative hexagonal quasigroups. We wish to find all commutative groups Q which have an automorphism φ that satisfies (1), with additional condition that the operation $\cdot$ defined by (2) is commutative. In other words,

$$\begin{aligned} a + \varphi(b - a) &= b + \varphi(a - b), \\ \varphi(b - a) - \varphi(a - b) &= b - a \end{aligned}$$

for all $a, b \in Q$. Therefore

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

must hold for all $x \in Q$.

From (1) it follows $\varphi(\varphi(x)) + \varphi(\varphi(x)) + x + x = \varphi(x) + \varphi(x)$ and using (3) we obtain $\varphi(x) + x + x = \varphi(x) + \varphi(x) = x$. It follows

$$\varphi(x) + x = 0 \qquad \text{and} \qquad \varphi(x) = x + x.$$

Therefore, $x + x + x = 0$ for all $x \in Q$, i.e., each element of the group G is of order 3 or 1. The only finite groups which satisfy that condition are $(\mathbb{Z}_3)^n$, and the group of order 1.

On the other hand, if $x + x + x = 0$, $\forall x \in Q$, then $\varphi(x) = x + x = -x$ is an automorphism that satisfies (1), and the operation defined by (2) is commutative.

We have proved:

Theorem 3. *The only finite commutative hexagonal quasigroups with more than one element, are the quasigroups obtained in the way described in Theorem 2 from the group* $(\mathbb{Z}_3)^n$*, for some* $n \in \mathbb{N}$.

From each group $(\mathbb{Z}_3)^n$ we obtain unique hexagonal quasigroup of order 3^n.

Example 3. From $(\mathbb{Z}_3)^2$ we obtain hexagonal quasigroup of order 9:

$\cdot$	0	1	2	3	4	5	6	7	8
0	0	2	1	6	8	7	3	5	4
1	2	1	0	8	7	6	5	4	3
2	1	0	2	7	6	8	4	3	5
3	6	8	7	3	5	4	0	2	1
4	8	7	6	5	4	3	2	1	0
5	7	6	8	4	3	5	1	0	2
6	3	5	4	0	2	1	6	8	7
7	5	4	3	2	1	0	8	7	6
8	4	3	5	1	0	2	7	6	8

3. Cyclic groups

The automorphism $\varphi(x) = kx$ (k is relatively prime to n) of the group $\mathbb{Z}_n$ satisfies (1) if and only if $k^2 - k + 1 \equiv 0 (\mathrm{mod}\ n)$.

We need to determine for which $n \in \mathbb{N}$ the obtained quadratic congruence has solution k (in that case k and n are relatively prime), or to determine the possible factors of $k^2 - k + 1$ for $k \in \mathbb{Z}$.

Evidently, since $k^2 - k + 1$ is odd, n cannot be even.

Let us determine all odd primes p for which $p \mid k^2 - k + 1$, for some $k \in \mathbb{Z}$. If $p \mid k^2 - k + 1$, then so do p divides the number $4(k^2 - k + 1) = (2k-1)^2 + 3$, that is $p \mid a^2 + 3$ where $a = 2k - 1$ is an odd integer. It suffices to determine for which p exists $x \in \mathbb{Z}$ such that $x^2 \equiv -3 (\mathrm{mod}\ p)$ (if such an even integer x exists, then $x + p$ is odd integer that satisfies the condition).

It is equivalent to $\left(\frac{-3}{p}\right) = 1$, which (since p is an odd integer) is equivalent to $\left(\frac{p}{3}\right) = 1$, i.e., $p \equiv 0 (\mathrm{mod}\ 3)$ or $p \equiv 1 (\mathrm{mod}\ 3)$. The solutions are

$p = 3$ and all primes of the form $p = 6l + 1$, $l \in \mathbb{Z}$. Factors of $k^2 - k + 1$ cannot be primes of the form $6l - 1$.

This proves the following:

Theorem 4. *The cyclic group $\mathbb{Z}_n$ has an automorphism that satisfies* (1) *if and only if its order n is a product of primes from the set $\{3\} \cup \{6l + 1 : l \in \mathbb{Z}\}$, i.e., if and only if n is an odd integer without any prime factor that is congruent to -1 modulo* 6.

Example 4. Group $\mathbb{Z}_7$ has two such automorphisms, $\varphi(x) = 3x$ and $\varphi(x) = 5x$. So we obtain two hexagonal quasigroups of order 7.

·	0	1	2	3	4	5	6
0	0	3	6	2	5	1	4
1	5	1	4	0	3	6	2
2	3	6	2	5	1	4	0
3	1	4	0	3	6	2	5
4	6	2	5	1	4	0	3
5	4	0	3	6	2	5	1
6	2	5	1	4	0	3	6

·	0	1	2	3	4	5	6
0	0	5	3	1	6	4	2
1	3	1	6	4	2	0	5
2	6	4	2	0	5	3	1
3	2	0	5	3	1	6	4
4	5	3	1	6	4	2	0
5	1	6	4	2	0	5	3
6	4	2	0	5	3	1	6

4. Conclusion

The following theorem is well-known.

Theorem 5. *Let m_1 and m_2 be relatively prime positive integers, and G be commutative group of order m_1m_2, whose automorphism φ satisfies* (1). *Then there exist groups G_1 and G_2 such that $G = G_1 \times G_2$, $|G_1| = m_1$, $|G_2| = m_2$, with automorphisms that satisfy* (1).

Theorem 5 allows us to deal with groups of order p^k only, in order to determine which groups have "good" automorphism.

So far, we know that finite hexagonal quasigroup can have orders p^{2k} for any prime p, 3^k, and p^k where p is a prime of the form $6l + 1$.

Let G be finite commutative group with automorphism φ which satisfies (1). For $x \in G$ let us denote

$$S_x = \{x, \varphi(x), \varphi^2(x), \varphi^3(x), \varphi^4(x), \varphi^5(x), \ldots\}.$$

It is clear that $\{S_x : x \in G\}$ is a partition of the set G. Since $\varphi^6(x) = x$, for all $x \in G$, the set S_x has 6 elements at most, i.e., it may have 1, 2, 3 or 6 elements. The only x for which $\operatorname{Card} S_x = 1$ is $x = 0$.

Card $S_x = 2$ when $x = \varphi^2(x)$, that is when $x + x + x = 0$.
Card $S_x = 3$ when $x = \varphi^3(x)$, i.e., $x = -x$.
Let

$$a = \text{Card}\,\{S_x : x \in G, |S_x| = 2\},$$

$$b = \text{Card}\,\{S_x : x \in G, |S_x| = 3\},$$

$$c = \text{Card}\,\{S_x : x \in G, |S_x| = 6\}.$$

The number of elements of G equals $|G| = 1 + 2a + 3b + 6c$.

Now we can finally solve remaining problems: the existence of hexagonal quasigroup of order 2^{2m-1}, or of order p^{2m-1} for p prime of the form $6l-1$.

Suppose the group G of order 2^{2m-1} has an automorphism that satisfies (1). Since its order is not divisible by 3, $a = 0$, and $|G| = 1 + 3b + 6c \equiv 1 (\text{mod } 3)$. But, $2^{2m-1} \equiv 2 (\text{mod } 3)$, which is a contradiction.

Let now p be a prime number of the form $6l-1$, and let G be the group of order p^{2m-1}, with an automorphism which satisfies (1). That group has no element of order two, and no element of order three, so $a = 0$ and $b = 0$. It follows $p^{2m-1} = 1 + 6c$, which is impossible since $p^{2m-1} \equiv -1 (\text{mod } 6)$.

This finally proves:

Theorem 6. *A finite hexagonal quasigroup of order $n = m \cdot l^2$, where m is square-free, exists if and only if m is an odd integer with no prime factor congruent to -1 modulo 6.*

References

[1] **V. Volenec**: *Hexagonal quasigroups*, Arch. Math., Brno, **27a** (1991), 113 – 122.

[2] **V. Volenec**: *Regular triangles in hexagonal quasigroups*, Rad Hrvat. Akad. Znan. Umjet., Mat. Znan., **467(11)** (1994), 85 – 93.

Department of Mathematics
University of Zagreb
Bijenička 30
10000 Zagreb
Croatia
E-mail: Mea.Bombardelli@math.hr

Received May 2, 2006