DEMONSTRATIO MATHEMATICA
Vol. XLII No 2 2009

Grzegorz Bińczak*, Joanna Kaleta

CYCLIC ENTROPIC QUASIGROUPS

Abstract. In this paper we explain the relationship of some entropic quasigroups to abelian groups with involution. It is known that $(Z_n, -_n)$ are examples of cyclic entropic quasigroups which are not groups. We describe all cyclic entropic quasigroups with quasi-identity.

1. Introduction

In this paper we describe cyclic quasigroups in the variety $EQ1$. This variety contains abelian groups. The variety of abelian groups is generated by integers with the usual addition, whereas $EQ1$ is generated by two algebras: integers with the usual addition and integers with the usual subtraction.

The first section is devoted to the basic definitions. In the second section we show that the variety $EQ1$ is equivalent to the variety of abelian groups with involution. Thanks to this equivalence, dealing with quasigroups in $EQ1$ becomes simpler. The notion of rank of an element can be transfered from abelian groups to quasigroups in $EQ1$. In the third section we describe finite cyclic quasigroups in $EQ1$. One can also consider infinite cyclic quasigroups in $EQ1$. We deal with this case in the fourth section.

Basic information on quasigroups can be found in [2], [5]. In [3] entropic (in other words medial) quasigroups are considered. In [1] the tables of characters of some quasigroups in $EQ1$ are found.

Definition 1. $(Q, \cdot, /, \backslash, 1)$ is an entropic quasigroup with quasi-identity if:

1. $a \cdot (a \backslash b) = b$, $(b/a) \cdot a = b$,
2. $a \backslash (a \cdot b) = b$, $(b \cdot a)/a = b$,
3. $(a \cdot b) \cdot (c \cdot d) = (a \cdot c) \cdot (b \cdot d)$,
4. $a \cdot 1 = a$, $1 \cdot (1 \cdot a) = a$.

Key words and phrases: quasigroups, entropic quasigroups, abelian groups, involution.
2000 *Mathematics Subject Classification*: 20N05.
*The author was partially supported by the statutory grant of Warsaw University of Technology no. 504G 1120 0112 000.

The conditions 1, 2 and 3 define entropic quasigroup, whereas the condition 4 defines quasi-identity.

We denote the variety of all entropic quasigroups with quasi-identity by $EQ1$. Example. $(Z, -, +, -, 0)$ is an entropic quasigroup with quasi-identity.

Definition 2. $(G, +, -, 0,^*)$ is an abelian group with involution if:

1° $(G, +, -, 0)$ is an abelian group,
2° $0^* = 0$, $a^{**} = a$, $(a + b)^* = a^* + b^*$.

We denote the variety of all abelian groups with involution by AGI.

2. Equivalence of EQ1 and AGI

Toyoda's theorem presents the description of entropic quasigroups:

Theorem 1. (Toyoda's theorem, see [6] and [7]) *For every non-empty entropic quasigroup* $(Q, \cdot, /, \backslash)$ *there exists a commutative group* $(Q, +)$*, an element* $q \in Q$ *and a pair of commuting automorphisms* ϕ, ψ *of* $(Q, +)$ *such that*

$$x \cdot y = \phi(x) + \psi(y) + q \quad \textit{for all } x, y \in Q.$$

Theorem 2. (Murdoch's theorem, see [4]) *For every entropic quasigroup* $(Q, \cdot, /, \backslash)$ *with idempotent element there exists a commutative group* $(Q, +)$*, and a pair of commuting automorphisms* ϕ, ψ *of* $(Q, +)$ *such that*

$$x \cdot y = \phi(x) + \psi(y) \quad \textit{for all } x, y \in Q.$$

Theorem 3. *If* $\mathcal{G} = (G, +, -, 0,^*)$ *is an abelian group with involution then* $\Psi(\mathcal{G}) = (G, \cdot, /, \backslash, 1)$ *is an entropic quasigroup with quasi-identity, where* $a \cdot b := a + (b^*)$, $a \backslash b := b^* + (-a^*)$, $a/b := a + (-b^*)$, $1 := 0$.

Proof. $\Psi(\mathcal{G})$ is a quasigroup:

1. $a \cdot (a \backslash b) = a + (b^* + (-a^*))^* = a^{**} + (b^* + (-a^*))^* = (a^* + b^* + (-a^*))^* = b^{**} = b.$
2. $(b/a) \cdot a = b + (-a^*) + a^* = b,$
3. $a \backslash (a \cdot b) = (a + b^*)^* + (-a^*) = a^* + b + (-a^*) = b$,
4. $(b \cdot a)/a = b + a^* + (-a^*) = b$.

$\Psi(\mathcal{G})$ is entropic:

$$\begin{aligned}(a \cdot b) \cdot (c \cdot d) &= (a + b^*) + (c + d^*)^* = a + b^* + c^* + d \\ &= (a + c^*) + (b + d^*)^* = (a \cdot c) \cdot (b \cdot d).\end{aligned}$$

1 is a quasi-identity of $\Psi(\mathcal{G})$:

$a \cdot 1 = a + 0^* = a + 0 = a,$

$1 \cdot (1 \cdot a) = 0 + (0 + a^*)^* = a^{**} = a.$ ∎

THEOREM 4. *If* $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ *is an entropic quasigroup with quasi-identity then* $\Phi(\mathcal{Q}) = (Q, +, -, 0, ^*)$ *is an abelian group with involution, where* $a + b := a \cdot (1 \cdot b)$, $(-a) := 1/(1 \cdot a)$, $0 := 1$, $a^* := 1 \cdot a$.

Proof. The operation $+$ is associative: $a + (b + c) = a \cdot (1 \cdot (b \cdot (1 \cdot c))) = a \cdot ((1 \cdot 1) \cdot (b \cdot (1 \cdot c))) = a \cdot ((1 \cdot b) \cdot (1 \cdot (1 \cdot c))) = (a \cdot 1) \cdot ((1 \cdot b) \cdot c) = (a \cdot (1 \cdot b)) \cdot (1 \cdot c) = (a + b) \cdot (1 \cdot c) = (a + b) + c$.

Moreover, $+$ is commutative: $(b + a) = b \cdot (1 \cdot a) = (1 \cdot (1 \cdot b)) \cdot (1 \cdot a) = (1 \cdot (1 \cdot b)) \cdot ((1 \cdot a) \cdot 1) = (1 \cdot (1 \cdot a)) \cdot ((1 \cdot b) \cdot 1) = a \cdot (1 \cdot b) = a + b$.

0 is a unity because: $a + 0 = a \cdot (1 \cdot 1) = a \cdot 1 = a$,

$(-a)$ is the negative of $a : (-a) + a = (1/(1 \cdot a)) \cdot (1 \cdot a) = 1 = 0$.

Hence $\Phi(\mathcal{Q})$ is an abelian group.

* is an involution: $0^* = 1 \cdot 1 = 1 = 0$,

$(a^*)^* = 1 \cdot (1 \cdot a) = a$,

$(a + b)^* = 1 \cdot (a \cdot (1 \cdot b)) = (1 \cdot 1) \cdot (a \cdot (1 \cdot b)) = (1 \cdot a) \cdot (1 \cdot (1 \cdot b)) = (1 \cdot a) + b^* = a^* + b^*$. ∎

PROPOSITION 1. *If* $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ *is an entropic quasigroup with quasi-identity then*

a) $x \cdot (1/y) = x/(1 \cdot y)$,
b) $1 \cdot (y \cdot x) = x \cdot y$,
c) $x/y = y \backslash (1 \cdot x)$.

Proof.

Concerning a):

$$x \cdot (1/y) = (((x \cdot (1/y)) \cdot (1 \cdot y))/(1 \cdot y) = ((x \cdot 1) \cdot ((1/y) \cdot y))/(1 \cdot y)$$
$$= ((x \cdot 1) \cdot 1)/(1 \cdot y) = x/(1 \cdot y).$$

Concerning b):

$$1 \cdot (y \cdot x) = (1 \cdot 1) \cdot (y \cdot x) = (1 \cdot y) \cdot (1 \cdot x) = (1 \cdot y) \cdot ((1 \cdot x) \cdot 1)$$
$$= (1 \cdot (1 \cdot x)) \cdot (y \cdot 1) = x \cdot y.$$

Concerning c): $x/y = y \backslash (y \cdot (x/y)) = y \backslash (1 \cdot ((x/y) \cdot y) = y \backslash (1 \cdot x)$. ∎

Applying Theorem 2 one can prove Theorem 5 but one needs only to show that $\phi = id$ and $\psi = {}^*$. However we present a simpler proof which does not depend on the mentioned Theorem 2.

THEOREM 5. *If* $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ *is an entropic quasigroup with quasi-identity then* $\Psi(\Phi(\mathcal{Q})) = \mathcal{Q}$.

Proof. Let $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ be an entropic quasigroup with quasi-identity. Then $\Phi(\mathcal{Q}) = (Q, +, -, 0, ^*)$ and $\Psi(\Phi(\mathcal{Q})) = (Q, \cdot_1, /_1, \backslash_1, 1)$, where

$$a \cdot_1 b = a + b^* = a \cdot (1 \cdot (1 \cdot b)) = a \cdot b.$$

Using Proposition 1 we have:

$$a\backslash_1 b = b^* + (-a^*) = b^* \cdot (1 \cdot (-a^*)) = b^* \cdot (1 \cdot (1/(1 \cdot a^*))) \overset{\text{Prop. 1a}}{=}$$
$$b^* \cdot (1/(1 \cdot (1 \cdot a^*))) = b^* \cdot (1/a^*) \overset{\text{Prop. 1a}}{=} b^*/(1 \cdot a^*) =$$
$$(1 \cdot b)/(1 \cdot (1 \cdot a)) \overset{\text{Prop. 1c}}{=} a\backslash(1 \cdot (1 \cdot b) = a\backslash b$$

and

$$a/_1 b = a + (-b^*) = a \cdot (1 \cdot (-b^*)) = a \cdot (1 \cdot (1/(1 \cdot (b^*)))) =$$
$$a \cdot (1 \cdot (1/b)) \overset{\text{Prop. 1a}}{=} a \cdot (1/(1 \cdot b)) \overset{\text{Prop. 1a}}{=} a/(1 \cdot (1 \cdot b)) = a/b. \blacksquare$$

THEOREM 6. *If* $\mathcal{G} = (G, +, -, 0, ^*)$ *is an abelian group with involution then* $\Phi(\Psi(\mathcal{G})) = \mathcal{G}$.

Proof. Let $\mathcal{G} = (G, +, -, 0, ^*)$ be an abelian group with involution. Then $\Psi(\mathcal{G}) = (G, \cdot, /, \backslash, 1)$ and $\Phi(\Psi(\mathcal{G})) = (G, +_1, -_1, 0, ^{*_1})$, where

$$a +_1 b = a \cdot (1 \cdot b) = a + (1 \cdot b)^* = a + (0 + b^*)^* = a + b^{**} = a + b.$$

Moreover

$$-_1 a = 1/(1 \cdot a) = 0 + (-(1 \cdot a)^*) = -((0 + a^*)^*) = -(a^{**}) = -a$$

and $a^{*_1} = 1 \cdot a = 0 + a^* = a^*$. $\blacksquare$

EXAMPLE. Let $Z_+ = (Z, +, -, 0, ^*) = \Phi(Z, +, /, \backslash, 0)$, where $x^* = x$ and $Z_- = (Z, +, -, 0, ^*) = \Phi(Z, -, /, \backslash, 0)$, where $x^* = -x$. It is easy to check that Z_-, $Z_+ \in AGI$.

THEOREM 7. *The variety generated by* Z_- *and* Z_+ *is equal to* AGI.

Proof. Let us observe that if equality

$$a_1x_1 + a_1'x_1^* + \ldots + a_nx_n + a_n'x_n^* = b_1x_1 + b_1'x_1^* + \ldots + b_nx_n + b_n'x_n^*$$

(for some $a_i, a_i', b_i, b_i' \in Z$) is satisfied in Z_- and Z_+ then $a_i = b_i$ and $a_i' = b_i'$ for $i = 1, \ldots, n$ because if we put $x_i = 1$ and $x_j = 0$ for $j \neq i$ we obtain $a_i + a_i' = b_i + b_i'$ (for Z_+) and $a_i - a_i' = b_i - b_i'$ (for Z_-), hence $a_i = b_i$ and $a_i' = b_i'$.

For every term $t(x_1, \ldots, x_n)$ there exist $a_1, a_1', \ldots a_n, a_n' \in Z$ such that equality $t(x_1, \ldots, x_n) = a_1x_1 + a_1'x_1^* + \ldots + a_nx_n + a_n'x_n^*$ holds in AGI. If

$$t(x_1, \ldots, x_n) = s(x_1, \ldots, x_n)$$

is valid in Z_- and Z_+ then there exist $a_1, a_1', \ldots a_n, a_n' \in Z$ and $b_1, b_1', \ldots b_n, b_n' \in Z$ such that $t(x_1, \ldots, x_n) = a_1x_1 + a_1'x_1^* + \ldots + a_nx_n + a_n'x_n^*$ and $s(x_1, \ldots, x_n) = b_1x_1 + b_1'x_1^* + \ldots + b_nx_n + b_n'x_n^*$ holds in AGI, hence $a_1x_1 + a_1'x_1^* + \ldots + a_nx_n + a_n'x_n^* = b_1x_1 + b_1'x_1^* + \ldots + b_nx_n + b_n'x_n^*$ is true in Z_- and Z_+, so $a_i = b_i$ and $a_i' = b_i'$ for $i = 1, \ldots, n$ therefore $t(x_1, \ldots, x_n) = s(x_1, \ldots, x_n)$ is satisfied in AGI. Thus an equality is valid in Z_- and Z_+ if and only if it is valid in AGI. There is why the variety generated by Z_- and Z_+ is equal to AGI. ∎

3. Finite Cyclic quasigroups in EQ1

Definition 3. Let $\mathcal{Q} = (Q, \cdot, /.\backslash, 1)$ be an entropic quasigroup with quasi-identity, $a \in Q$ and $\Phi(\mathcal{Q}) = (Q, +, -, 0, ^*)$.

$$\text{If } n \in Z \text{ then } na = \begin{cases} \underbrace{a + \cdots + a}_{n-\text{times}} & \text{for } n \geq 1 \\ 0 & \text{for } n = 0 \\ \underbrace{(-a) + \cdots + (-a)}_{-n-\text{times}} & \text{for } n \leq -1. \end{cases}$$

In AGI every subalgebra generated by only one element has the form: $\langle a \rangle = \{na + ka^* \mid n, k \in Z\}$.

In $EQ1$ we can introduce three kinds of ranks:

$r_+(a) = \min\{n \in N \mid na = 0, n \geq 1\}$, (it is the usual rank of a in abelian groups),

$r_*(a) = \min\{n \in N \mid n \geq 1, \exists_{k \in Z}\ na^* = ka\}$,

$r_{*+}(a) = \min\{n \in N \mid r_*(a)a^* = (r_*(a) + n)a\}$.

The following proposition shows that the ranks mentioned above do not depend on the choice of generator.

Proposition 2. *Let $\mathcal{Q} = (Q, \cdot, /.\backslash, 1)$ be a finite entropic quasigroup with quasi-identity. If $Q = \langle a \rangle = \langle b \rangle$ then $r_+(a) = r_+(b)$, $r_*(a) = r_*(b)$, $r_{*+}(a) = r_{*+}(b)$.*

Proof. Since $b \in \langle a \rangle$ there exist $c, d \in Z$ such that $b = ca + da^*$. Let us note that if $na = 0$ then $na^* = 0$ and $nb = n(ca + da^*) = cna + dna^* = 0$. Similarly, if $nb = 0$ then $na = 0$. Hence $r_+(a) = r_+(b)$. Moreover, $na^* = ka \Leftrightarrow nb^* = kb$ therefore $r_*(a) = r_*(b)$ and $r_{*+}(a) = r_{*+}(b)$. ∎

Definition 4. Let $\mathcal{Q} = (Q, \cdot, /.\backslash, 1)$ be a cyclic entropic quasigroup with quasi-identity and $Q = \langle a \rangle$ for some $a \in Q$. Define $r_+(Q) = r_+(a)$, $r_*(Q) = r_*(a)$, $r_{*+}(Q) = r_{*+}(a)$.

From Proposition 2 this definition does not depend on the choice of the generator a.

Proposition 3. *Let $\mathcal{Q} = (Q, \cdot, /.\backslash, 1)$ be a finite cyclic entropic quasigroup with quasi-identity and $Q = \langle a \rangle$ for some $a \in Q$. If $c \in Z$ then $ca = 0 \Leftrightarrow r_+(Q) | c$.*

Now we show some properties of ranks.

Theorem 8. *If* $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ *is a finite cyclic entropic quasigroup with quasi-identity then* $r_*(Q)|r_+(Q)$, $r_*(Q)|r_{*+}(Q), 0 \le r_{*+}(Q) < r_+(Q)$ *and* $r_+(Q)|2r_{*+}(Q) + \frac{r_{*+}(Q)^2}{r_*(Q)}$.

Proof. Let $Q = \langle x \rangle$, $a = r_+(x)$, $b = r_*(x)$, $k = r_{*+}(x)$. Let $a = bb' + r$ and $0 \le r < b$. Then $0 = ax^* = b'bx^* + rx^* = b'(b+k)x + rx^*$.Hence

$$rx^* = -b'(b+k)x.$$

By definition of $r_*(x)$ we obtain $r = 0$. Hence $b|a$. Let $k = b''b + r'$ and $0 \le r' < b$. Then

$$bx = (b+k)x^* = (b + b''b + r')x^* = (1+b'')bx^* + r'x^*$$
$$= (1+b'')(b+k)x + r'x^*, \text{ so } r'x^* = (-b''b - b''k - k)x.$$

By definition of $r_*(x)$ we obtain $r' = 0$. Hence $b|k$.
Moreover, $(k+b)x^* = (b''b+b)x^* = b''(b+k)x + (b+k)x$. Thus, $bx = (k+b)x^* = (b''(b+k)+(b+k))x$ and $0 = (b''(b+k)+k)x = (\frac{k}{b}(b+k)+k)x = (k + \frac{k^2}{b} + k)x = (2k + \frac{k^2}{b})x$, by Proposition 3 we have $a|2k + \frac{k^2}{b}$. ∎

And now we preceed to the definition of maps $\gamma^k_{a,b}$ needed to define some canonical cyclic quasigroups in $EQ1$. We denote the integer part of a by $[a]$, whereas $(a)_b$ denotes the remainder after dividing a by b.

Definition 5. Let $a, b, k \in N$ and $a, b \ge 1$. Let $\gamma^k_{a,b} : Z \times Z \to Z \times Z$ be a mapping such that

$$\gamma^k_{a,b}(x,y) = ((x + \left[\frac{y}{b}\right](b+k))_a, (y)_b)$$

and let

$$(x,y) \oplus^k_{a,b} (z,t) = \gamma^k_{a,b}(x+z, y+t).$$

Let $T : Z \times Z \to Z \times Z$ be a function such that $T(x,y) = (y,x)$.

It is easy to check the following properties of the operation of taking the integer part.

Proposition 4. *Let* $b, t, y \in Z$ *and* $b \ge 1$. *Then*

$$\left[\frac{t}{b}\right] + \left[\frac{y+(t)_b}{b}\right] = \left[\frac{y+t}{b}\right] \qquad (y+(t)_b)_b = (y+t)_b.$$

The next proposition will be helpful in proving that $\oplus^k_{a,b}$ is associative.

Proposition 5. *Let* $a, b, k \in N$ *and* $a, b \ge 1$.

a) *If* $(x,y) \in Z_a \times Z_b$ *then* $\gamma^k_{a,b}(x,y) = (x,y)$.
b) $(x,y) \oplus^k_{a,b} \gamma^k_{a,b}(z,t) = \gamma^k_{a,b}(x+z, y+t)$.

Proof.

a) If $0 \le x < a$ and $0 \le y < b$ then $\left[\frac{y}{b}\right] = 0$, $(x)_a = x$ and $(y)_b = y$. Hence $\gamma^k_{a,b}(x,y) = ((x+0)_a, (y)_b) = (x,y)$. This ends the proof of a).

b)

$$\begin{aligned}
(x,y) \oplus^k_{a,b} \gamma^k_{a,b}(z,t) &= (x,y) \oplus^k_{a,b} \left((z + \left[\frac{t}{b}\right](b+k))_a, (t)_b\right) \\
&= \gamma^k_{a,b}\left(x + (z + \left[\frac{t}{b}\right](b+k))_a, y + (t)_b\right) \\
&= \left(\left(x + (z + \left[\frac{t}{b}\right](b+k))_a + \left[\frac{y+(t)_b}{b}\right](b+k)\right)_a, (y+(t)_b)_b\right) \\
&\overset{\text{Prop. 3}}{=} \left((x + z + \left[\frac{y+t}{b}\right](b+k))_a, (y+t)_b\right) \\
&= \gamma^k_{a,b}(x+z, y+t). \ \blacksquare
\end{aligned}$$

First we show that the set $Z_a \times Z_b$ with the operation $\oplus^k_{a,b}$ is an abelian group.

THEOREM 9. *Let $a,b,k \in Z$ and $a \ge 1, b \ge 1, k \ge 0$. Then the algebra $\left(Z_a \times Z_b, \oplus^k_{a,b}, -, (0,0)\right)$ is an abelian group, where $-(x,y) = \gamma^k_{a,b}(-x,-y)$.*

Proof. Obviously the operation $\oplus^k_{a,b}$ is commutative. We show that $\oplus^k_{a,b}$ is associative: $(x_1,y_1) \oplus^k_{a,b} \left((x_2,y_2) \oplus^k_{a,b} (x_3,y_3)\right) = (x_1,y_1) \oplus^k_{a,b} \gamma^k_{a,b}(x_2 + x_3, y_2 + y_3) \overset{\text{Prop. 5b}}{=} \gamma^k_{a,b}(x_1 + (x_2 + x_3), y_1 + (y_2 + y_3)) = \gamma^k_{a,b}(x_3 + (x_1 + x_2), y_3 + (y_1 + y_2)) \overset{\text{Prop. 5b}}{=} (x_3,y_3) \oplus^k_{a,b} \gamma^k_{a,b}(x_1 + x_2, y_1 + y_2) = \gamma^k_{a,b}(x_1 + x_2, y_1 + y_2) \oplus^k_{a,b} (x_3,y_3) = \left((x_1,y_1) \oplus^k_{a,b} (x_2,y_2)\right) \oplus^k_{a,b} (x_3,y_3)$.

If $(x,y) \in Z_a \times Z_b$ then by Proposition 5a we have $(x,y) \oplus^k_{a,b} (0,0) = \gamma^k_{a,b}(x,y) = (x,y)$. Finally

$$\begin{aligned}
(x,y) \oplus^k_{a,b} -(x,y) &= (x,y) \oplus^k_{a,b} \gamma^k_{a,b}(-x,-y) \\
&\overset{\text{Prop. 5b}}{=} \gamma^k_{a,b}(x + (-x), y + (-y)) = \gamma^k_{a,b}(0,0) = (0,0). \ \blacksquare
\end{aligned}$$

Next we show the following proposition (we use it to prove that * is an involution.)

PROPOSITION 6. *Let $a,b,k \in Z$ and $a \ge 1, b \ge 1, k \ge 0$ and $b|a, b|k, 0 \le k < a, a|2k + \frac{k^2}{b}$. Then $\gamma^k_{a,b} \circ T \circ \gamma^k_{a,b} = \gamma^k_{a,b} \circ T$.*

Proof. Let $(x,y) \in Z \times Z$. Then

$$\gamma^k_{a,b}(T(\gamma^k_{a,b}(x,y))) = \gamma^k_{a,b}((y)_b, (x + \left[\tfrac{y}{b}\right](b+k))_a)$$

$$= \left(\left((y)_b + \left[\frac{(x+\left[\frac{y}{b}\right](b+k))_a}{b}\right](b+k)\right)_a, \left(\left(x+\left[\frac{y}{b}\right](b+k)\right)_a\right)_b\right).$$

Moreover, $\gamma^k_{a,b}(T(x,y)) = \left(\left(y + \left[\frac{x}{b}\right](b+k)\right)_a, (x)_b\right)$.

Let

$$(*) \qquad x + \left[\frac{y}{b}\right](b+k) = aa' + r, \quad 0 \le r < a.$$

Notice that

$$x - \left(x + \left[\frac{y}{b}\right](b+k)\right)_a = x - \left(x + \left[\frac{y}{b}\right](b+k) - aa'\right) = -\left[\frac{y}{b}\right](b+k) + aa'$$

is divided by b since $b|a$ and $b|(b+k)$. Hence the second coordinates of $\gamma^k_{a,b}(T(\gamma^k_{a,b}(x,y)))$ and $\gamma^k_{a,b}(T(x,y))$ coincide. Let

$$(**) \qquad y = bb' + r', \quad 0 \le r' < b.$$

Then

$$(y)_b + \left[\frac{(x+\left[\frac{y}{b}\right](b+k))_a}{b}\right](b+k) - \left(y + \left[\frac{x}{b}\right](b+k)\right)$$

$$\overset{(*),(**)}{=} -bb' + (b+k)\left(\left[\frac{x + b'(b+k) - aa'}{b}\right] - \left[\frac{x}{b}\right]\right)$$

$$\overset{\text{Prop. 3}}{=} -bb' + (b+k)\left(\left[\frac{x}{b}\right] + \frac{b'(b+k) - aa'}{b} - \left[\frac{x}{b}\right]\right)$$

$$= -bb' + (b+k)\left(\frac{b'(b+k) - aa'}{b}\right)$$

$$= \frac{-b^2b' + b^2b' + 2kbb' + k^2b' - aa'(b+k)}{b}$$

$$= b'\frac{2kb + k^2}{b} - a\frac{a'(b+k)}{b} = (2k + \frac{k^2}{b})b' - aa'\frac{b+k}{b}$$

is divided by a, because $a|(2k + \frac{k^2}{b})$ and $b|(b+k)$. Hence the first coordinates of $\gamma^k_{a,b}(T(\gamma^k_{a,b}(x,y)))$ and $\gamma^k_{a,b}(T(x,y))$ coincide. ∎

Definition 6. Let $a, b, k \in Z$ and $a \ge 1, b \ge 1, k \ge 0$. Define

$$Q^k_{a,b} = \left(Z_a \times Z_b, \oplus^k_{a,b}, -, (0,0), ^*\right),$$

where $-(x,y) = \gamma^k_{a,b}(-x,-y)$ and $(x,y)^* = \gamma^k_{a,b}(y,x)$.

The following theorem shows that $Q^k_{a,b}$ belongs to AGI if some conditions concerning a, b, k are satisfied. Moreover $Q^k_{a,b}$ is cyclic because it is generated by $(1, 0)$.

THEOREM 10. *Let $a, b, k \in Z$ with $a \geq 1, b \geq 1, k \geq 0$ and $b|a, b|k, 0 \leq k < a, a|2k + \frac{k^2}{b}$. Then $Q^k_{a,b}$ is an abelian group with involution.*

Proof. From Theorem 9 we know that $Q^k_{a,b}$ is an abelian group. Moreover $(0,0)^* = \gamma^k_{a,b}(0,0) \overset{\text{Prop. 5a}}{=} (0.0)$. Let $(x, y) \in Z_a \times Z_b$. Then $(x, y)^{**} = \gamma^k_{a,b}(T(\gamma^k_{a,b}(T(x,y)))) \overset{\text{Prop. 6}}{=} \gamma^k_{a,b}(T(T(x,y)) = \gamma^k_{a,b}(x,y) \overset{\text{Prop. 5}}{=} (x,y)$. Now we prove that $\left((x,y) \oplus^k_{a,b} (z,t)\right)^* = (x,y)^* \oplus^k_{a,b} (z,t)^*$. Notice that

$$\begin{aligned}\left((x,y) \oplus^k_{a,b} (z,t)\right)^* &= \gamma^k_{a,b}(T(\gamma^k_{a,b}(x+z, y+t))) \overset{\text{Prop. 6}}{=} \gamma^k_{a,b}(T(x+z, y+t)) \\ &= \gamma^k_{a,b}(y+t, x+z) \\ &= \left(\left(y + t + \left[\frac{x+z}{b}\right](b+k)\right)_a, (x+z)_b\right) \\ &= \left((L_1)_a, (L_2)_b\right)\end{aligned}$$

and

$$\begin{aligned}&(x,y)^* \oplus^k_{a,b} (z,t) \\ &\quad= \left(\left(y + \left[\frac{x}{b}\right](b+k)\right)_a, (x)_b\right) \oplus^k_{a,b} \left(\left(t + \left[\frac{z}{b}\right](b+k)\right)_a, (z)_b\right) \\ &\quad= \gamma^k_{a,b}\left(\left(y + \left[\frac{x}{b}\right](b+k)\right)_a + \left(t + \left[\frac{z}{b}\right](b+k)\right)_a, (x)_b + (z)_b\right) \\ &\quad= \Bigg(\left(\left(y + \left[\frac{x}{b}\right](b+k)\right)_a + \left(t + \left[\frac{z}{b}\right](b+k)\right)_a \right.\\ &\qquad\left. + \left[\frac{(x)_b + (z)_b}{b}\right](b+k)\right)_a, (x)_b + (z)_b\Bigg) = \left((R_1)_a, (R_2)_b\right).\end{aligned}$$

Hence $L_2 - R_2 = x + z - (x)_b - (z)_b = b\left[\frac{x}{b}\right] + b\left[\frac{z}{b}\right]$ and $b|L_2 - R_2$ so $(L_2)_b = (R_2)_b$. By Proposition 4 we have

$$(*) \qquad \left[\frac{x}{b}\right] + \left[\frac{z}{b}\right] + \left[\frac{(x)_b + (z)_b}{b}\right] = \left[\frac{x+z}{b}\right].$$

There exists $a' \in Z$ such that $R_1 = \left(y + \left[\frac{x}{b}\right](b+k)\right)_a + \left(t + \left[\frac{z}{b}\right](b+k)\right)_a + \left[\frac{(x)_b+(z)_b}{b}\right](b+k) = y + \left[\frac{x}{b}\right](b+k) + t + \left[\frac{z}{b}\right](b+k) + \left[\frac{(x)_b+(z)_b}{b}\right](b+k) + aa' \overset{(*)}{=} y + t + (b+k)\left[\frac{x+z}{b}\right] + aa' = L_1 + aa'$ hence $(L_1)_b = (R_1)_b$. ■

Proposition 7. *Let* $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ *be finite cyclic entropic quasigroup with quasi-identity and* $Q = \langle x \rangle$ *for some* $x \in Q$. *Let* $a = r_+(Q)$, $b = r_*(Q)$, $k = r_{*+}(Q)$. *If* $\alpha : Z \times Z \to Q$ *is a function such that* $\alpha(n, l) = nx + lx^*$ *then* $\alpha \circ \gamma^k_{a,b} = \alpha$.

Proof. Let $n, l \in Z$ and $l = bb' + r$, $0 \le r < b$. Then $\alpha(n, l) = nx + lx^* = nx + b'bx^* + rx^* = nx + b'(b + k)x + rx^* = \left(n + \left[\frac{l}{b}\right](b + k)\right)x + rx^* = \left(n + \left[\frac{l}{b}\right](b + k)\right)_a x + (l)_b x = \alpha(\gamma^k_{a,b}(n, l))$. ■

It turns out that every cyclic algebra in AGI is isomorphic to some $Q^k_{a,b}$. It follows that every cyclic quasigroup in $EQ1$ is isomorphic to some $\Psi(Q^k_{a,b})$.

Theorem 11. *Let* $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ *be a finite cyclic entropic quasigroup with quasi-identity and* $a = r_+(Q)$, $b = r_*(Q)$, $k = r_{*+}(Q)$. *Then* $\Phi(\mathcal{Q}) \cong \mathcal{Q}^k_{a,b}$.

Proof. Let $Q = \langle x \rangle$ for some $x \in Q$ and $\alpha : Z_a \times Z_b \to Q$ be a function such that $\alpha(n, l) = nx + lx^*$ for each $(n, l) \in Z_a \times Z_b$. We show that α is an isomorphism. If $y \in Q$ then there exist $n, l \in Z$ such that $y = nx + lx^* \overset{\text{Prop. 7}}{=} \alpha(\gamma^k_{a,b}(n, l))$. Hence α is onto Q. Let $(n, l), (n', l') \in Z_a \times Z_b$ and $\alpha(n, l) = \alpha(n', l')$. Hence $nx + lx^* = n'x + l'x^*$ and $(l - l')x^* = (n' - n)x$ so by defintion of b we have $l - l' = 0$. Therefore $nx = n'x$, so $(n - n')x = 0$ and $a | n - n'$ thus $n - n' = 0$ and α is injective. Let $(n, l), (n', l') \in Z_a \times Z_b$. Then $\alpha((n, l) \oplus^k_{a,b} (n', l')) = \alpha(\gamma^k_{a,b}(n + n', l + l')) \overset{\text{Prop. 7}}{=} \alpha(n + n', l + l') = (n + n')x + (l + l')x^* = nx + lx^* + n'x + l'x^* = \alpha(n, l) + \alpha(n', l')$. Moreover $\alpha((n, l)^*) = \alpha(\gamma^k_{a,b}(l, n)) \overset{\text{Prop. 7}}{=} \alpha(l, n) = lx + nx^* = (nx + lx^*)^* = (\alpha(n, l))^*$. Hence α is a homomorphism. ■

Corollary. *Let* $\mathcal{Q}_1, \mathcal{Q}_2$ *be a finite cyclic entropic quasigroups with quasi-unities. Then* $\mathcal{Q}_1 \cong \mathcal{Q}_2$ *if and only if* $r_+(\mathcal{Q}_1) = r_+(\mathcal{Q}_2)$, $r_*(\mathcal{Q}_1) = r_*(\mathcal{Q}_2)$, $r_{*+}(\mathcal{Q}_1) = r_{*+}(\mathcal{Q}_2)$.

4. Infinite cyclic quasigroups in EQ1

In this section we assume that Q is infinite.

Definition 7. Let $\mathcal{Q} = (Q, \cdot, /, \backslash, 1)$ be an entropic quasigroup with quasi-identity, $a \in Q$ and $\Phi(\mathcal{Q}) = (Q, +, -, 0, ^*)$. Let $x \in Q$. Then $B_x(Q) = \{b \in N - \{0\} : \exists_{k \in Z} bx^* = kx\}$.

The set $B_x(Q)$ does not depend on the choice of a generator x:

Proposition 8. *Let* $Q \in EQ1$ *and* $< x > = < y > = Q$. *Then* $B_x(Q) = B_y(Q)$.

Proof. Since $x \in< y >$ there exist $r, s \in Z$ such that $x = ry + sy^*$. If $z \in B_y(Q)$ then we can find $k \in Z$ such that $zy^* = ky$. Hence $zx^* = z(ry + sy^*)^* = zry^* + zsy = rky + ksy^* = kx$ and $z \in B_x(Q)$. Therefore $B_y(Q) \subseteq B_x(Q)$. Analogously $B_x(Q) \subseteq B_y(Q)$. ∎

PROPOSITION 9. *If* $Q \in EQ1$, $< x >= Q$ *and* $ax = 0$ *then* $a = 0$.

PROPOSITION 10. *If* $Q \in EQ1$, $Q =< x >$ *and* $bx^* = kx$ *then* $k = b$ *or* $k = -b$.

Proof. If $bx^* = kx$ then $b^2x^* = bkx = kbx = k^2x^*$. Hence $(b^2 - k^2)x^* = 0$ and $(b^2 - k^2)x = 0$ so $b^2 = k^2$. ∎

Let us observe that if $b \neq 0$, $bx^* = kx$ and $k = b$ then $bx^* = not = -bx$.

DEFINITION 8. Let $Q \in EQ1$ and $Q =< x >$. Then

$$B(Q) = \begin{cases} \infty & \text{for } B_x(Q) = \varnothing \\ \min B_x(Q) & \text{for } B_x(Q) \neq \varnothing. \end{cases}$$

DEFINITION 9. Let $Q \in EQ1$, $Q =< x >$ and $B(Q) \neq \infty$. Then

$$sgn_x(Q) = \begin{cases} +1 & \text{if } B(Q)x^* = B(Q)x \\ -1 & \text{if } B(Q)x^* = -B(Q)x. \end{cases}$$

Similarly to Proposition 8 it can be proved:

PROPOSITION 11. *Let* $Q \in EQ1$, $B(Q) \neq \infty$ *and* $Q =< x >=< y >$. *Then* $sgn_x(Q) = sgn_y(Q)$.

So $sgn_x(Q)$ does not depend on the choice of x and we can define $sgn(Q) = sqn_x(Q)$ for $Q \in EQ1$ such that $Q =< x >$ and $B(Q) \neq \infty$.

DEFINITION 10. Let $b \in Z - \{0\}$. Let $\gamma_b : Z \times Z \to Z \times Z$ be a mapping such that $\gamma_b(x, y) = (x + \left[\frac{y}{b}\right] b, (y)_b)$ and $(x, y) \oplus_b (z, t) = \gamma_b(x + z, y + t)$.

Similarly to Proposition 5 and Proposition 6 one can prove:

PROPOSITION 12. *Let* $b \in Z - \{0\}$.

a) *If* $(x, y) \in Z \times Z_b$ *then* $\gamma_b(x, y) = (x, y)$.
b) $(x, y) \oplus_b \gamma_b(z, t) = \gamma_b(x + z, y + t)$.

PROPOSITION 13. *Let* $b \in Z - \{0\}$. *Then* $\gamma_b \circ T \circ \gamma_b = \gamma_b \circ T$.

In the next theorem we describe some canonical infinite cyclic algebras in *AGI*.

THEOREM 12. *Let* $b \in Z - \{0\}$. *Then* $Q_b = (Z \times Z_b, \oplus_b, -, (0, 0), ^*)$ *is an abelian group with involution, where* $-(x, y) = \gamma_b(-x, -y)$ *and* $(x, y)^* = \gamma_b(y, x)$.

Proof. The proof of the fact that Q_b is an abelian group is analogous to the proof of Theorem 9.

Moreover $(0,0)^* = \gamma_b(0,0) \overset{\text{Prop. 12}}{=} (0.0)$.

The proof that $(x,y)^{**} = (x,y)$ is the same as in Theorem 10. Now we prove that $((x,y) \oplus_b (z,t))^* = (x,y)^* \oplus_b (z,t)^*$. Notice that

$$\begin{aligned}((x,y) \oplus_b (z,t))^* &= \gamma_b(T(\gamma_b(x+z,y+t))) \overset{\text{Prop. 13}}{=} \gamma_b(T(x+z,y+t))\\ &= \gamma_b(y+t,x+z) = \left(y+t+\left[\frac{x+z}{b}\right]b,(x+z)_b\right)\\ &= (L_1,(L_2)_b)\end{aligned}$$

and

$$\begin{aligned}(x,y)^* \oplus_b (z,t)^* &= \left(y+\left[\tfrac{x}{b}\right]b,(x)_b\right) \oplus_b \left(t+\left[\tfrac{z}{b}\right]b,(z)_b\right)\\ &= \gamma_b\left(y+\left[\tfrac{x}{b}\right]b+t+\left[\tfrac{z}{b}\right]b,(x)_b+(z)_b\right)\\ &= \left(y+\left[\tfrac{x}{b}\right]b+t+\left[\tfrac{z}{b}\right]b+\left[\tfrac{(x)_b+(z)_b}{b}\right]b,(x)_b+(z)_b\right)\\ &= (R_1,(R_2)_b).\end{aligned}$$

Hence $L_2 - R_2 = x+z-(x)_b-(z)_b = b\left[\frac{x}{b}\right]+b\left[\frac{z}{b}\right]$ and $b|L_2-R_2$ so $(L_2)_b = (R_2)_b$. By Proposition 4 we have

$$(*) \qquad \left[\frac{x}{b}\right]+\left[\frac{z}{b}\right]+\left[\frac{(x)_b+(z)_b}{b}\right] = \left[\frac{x+z}{b}\right],$$

so $R_1 = L_1$. ∎

The reader may verifythe following theorem by analogy with Theorem 11.

THEOREM 13. *Let $\mathcal{Q} = (Q,\cdot,/.\backslash,1)$ be infinite cyclic entropic quasigroup with quasi-identity.*

If $B(\mathcal{Q}) = \infty$ then $\Phi(\mathcal{Q}) \cong (Z\times Z,+,-,^*,(0,0))$, where $(x,y)^* = (y,x)$.

If $B(\mathcal{Q}) < \infty$ then $\Phi(\mathcal{Q}) \cong Q_{sgn(Q)B(Q)}$.

COROLLARY. *Let $\mathcal{Q}_1,\mathcal{Q}_2$ be an infinite cyclic entropic quasigroups with quasiunities. Then $\mathcal{Q}_1 \cong \mathcal{Q}_2$ if and only if $B(\mathcal{Q}_\infty) = B(\mathcal{Q}_\in) = \infty$ or $B(\mathcal{Q}_1) = B(\mathcal{Q}_2)$ and $sgn(\mathcal{Q}_1) = sgn(\mathcal{Q}_2)$.*

References

[1] G. Bińczak, J. Kaleta, *The table of characters of some quasigroups*, Discussiones Mathematicae General Algebra and Applications 27 (2007), 147–167.

[2] O. Chein, H. O. Pflugfelder, J. D. H. Smith, *Quasigroups and Loops: Theory and Applications*, Berlin (1990).

[3] V. J. Havel, A. Vanžurová, *Medial Quasigroups and Geometry*, Olomouc (2006).
[4] D. C. Murdoch, *Structure of abelian quasigroups*, Trans. Amer. Math. Soc. 49 (1941), 392–409.
[5] J. D. H. Smith, *Representation Theory of Infinite Groups and Finite Quasigroups*, Université de Montréal, 1986.
[6] K. Toyoda, *On axioms of mean transformations and automorphic transformations of abelian groups*, Tōhoku Math. J. 46 (1940), 239–251.
[7] K. Toyoda, *On affine geometry of abelian groups*, Proc. Imp. Acad. Tokyo 16 (1940), 161–164.

Grzegorz Bińczak
FACULTY OF MATHEMATICS AND INFORMATION SCIENCE
WARSAW UNIVERSITY OF TECHNOLOGY
Pl. Politechniki 1
00-661 WARSZAWA, POLAND
Email: binczak@mini.pw.edu.pl

Joanna Kaleta
DEPARTMENT OF APPLIED MATHEMATICS
WARSAW UNIVERSITY OF LIFE SCIENCES
Nowoursynowska 166
02-776 WARSZAWA, POLAND
Email: joanna˙kaleta@sggw.pl

Received April 7, 2008; revised version June 3, 2008.