BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 1(47), 2005, Pages 11–18
ISSN 1024–7696

On the structure of finite medial quasigroups

V.A. Shcherbacov

Abstract. Some variants of Toyoda, Murdoch and Ježek-Kepka theorems on medial quasigroups are given. The structure of finite medial quasigroups is described.

Mathematics subject classification: 20N05.
Keywords and phrases: Quasigroup, medial quasigroup, idempotent.

We shall use basic terms and concepts from books [1–3]. To economize time of readers we recall some known facts.

A quasigroup $(Q, \cdot)$ with the identity

$$xy \cdot uv = xu \cdot yv \tag{1}$$

is called medial. Crucial Toyoda theorem ([1, 2, 4–6]) says that every medial quasigroup $(Q, \cdot)$ can be presented in the form:

$$x \cdot y = \varphi x + \psi y + a, \tag{2}$$

where $(Q, +)$ is an abelian group, φ, ψ are automorphisms of $(Q, +)$ such that $\varphi\psi = \psi\varphi$, $x, y \in Q$, a is some fixed element from the set Q.

In view of Toyoda theorem the theory of medial quasigroups is very close to the theory of abelian groups but it is not exactly the theory of abelian groups. For example, a very simple for abelian groups fact, that every simple abelian group is finite, was proved for medial quasigroups only in 1977 [7].

Medial quasigroups as well as other classes of quasigroups isotopic to groups give us a possibility to construct quasigroups with preassigned properties. Often these properties can be expressed on the language of properties of groups and components of isotopy.

As usual, $L_a : L_a x = a \cdot x$, $R_a : R_a x = x \cdot a$ are respectively left and right translation of a quasigroup $(Q, \cdot)$. An element d such that $d \cdot d = d$ is called an idempotent element of a binary quasigroup $(Q, \cdot)$. By ε we mean the identity permutation.

A quasigroup $(Q, \circ)$ is called an *isotope of a quasigroup* $(Q, \cdot)$ if there exist permutations α, β, γ of the set Q such that $x \circ y = \gamma^{-1}(\alpha x \cdot \beta y)$ for all $x, y \in Q$. If $(Q, \circ) = (Q, \cdot)$, then the triple (α, β, γ) is an *autotopy* of the quasigroup $(Q, \cdot)$, the permutation γ is a *quasiautomorphism* of the quasigroup $(Q, \cdot)$. An isotopy of the form $(\varepsilon, \varepsilon, \gamma)$ is called a *principal isotopy* [1–3].

A quasigroup $(Q, \cdot)$ with the identity $x \cdot x = x$ is called an *idempotent quasigroup*. A quasigroup $(Q, \cdot)$ with the identity $x \cdot x = e$, where e is a fixed element of the set Q, is called an *unipotent quasigroup*.

© V. A. Shcherbacov, 2005

Any quasiautomorphism γ of a group $(Q,+)$ has the form $R_a^+\beta$, where $a \in Q$, $\beta \in Aut(Q,+)$ ([1]; [2], p.24). Obviously $\beta 0 = 0$, where, as usual, 0 denotes the identity element of $(Q,+)$.

Medial quasigroups (as well as any other quasigroup class) can be divided into 2 classes: 1) quasigroups that have one or more idempotent elements; 2) quasigroups that have not any idempotent.

Theorem 1. *Conditions (i) and (ii) are equivalent:*

(i) $(Q,\cdot)$ *is a medial quasigroup that has idempotent element* 0*;*

(ii) there exist an abelian group $(Q,+)$ *with the identity element* 0*, two its commuting automorphisms* α, β *such that* $x \cdot y = \alpha x + \beta y + a$ *for all* $x, y \in Q$*, where* $-a \in (\alpha + \beta - \varepsilon)Q$*.*

Proof. (i) $\Longrightarrow$ (ii). LP-isotope $(R_0^{-1}, L_0^{-1}, \varepsilon)$ of quasigroup $(Q,\cdot)$ is a loop $(Q,+)$ with the identity element $0 \cdot 0 = 0$, i.e. $x + y = R_0^{-1}x \cdot L_0^{-1}y$ [1]. Then $x \cdot y = R_0 x + L_0 y, R_0 0 = 0, L_0 0 = 0$. Let $R_0 = \alpha, L_0 = \beta$. Therefore $x \cdot y = \alpha x + \beta y$. So we can rewrite medial identity in terms of the operation $+$ in the following way.

$$\alpha(\alpha x + \beta y) + \beta(\alpha u + \beta v) = \alpha(\alpha x + \beta u) + \beta(\alpha y + \beta v). \tag{3}$$

If we take $x = y = v = 0$ in (3), then we obtain $\alpha\beta y = \beta\alpha y$, i.e.

$$\alpha\beta = \beta\alpha. \tag{4}$$

By $u = v = 0$ in (3) we have $\alpha(\alpha x + \beta y) = \alpha^2 x + \beta\alpha y =^{(4)} \alpha^2 x + \alpha\beta y$. Therefore $\alpha \in Aut(Q,+)$.

If we substitute in (3) $x = y = 0$, then $\beta(\alpha u + \beta v) = \alpha\beta u + \beta^2 v =^{(4)} \beta\alpha u + \beta^2 v$, $\beta \in Aut(Q,+)$.

By $x = v = 0$ equality (3) takes the form $\alpha\beta y + \beta\alpha u = \alpha\beta u + \beta\alpha y$. Since $\alpha\beta = \beta\alpha$, we have $\alpha\beta y + \alpha\beta u = \alpha\beta u + \alpha\beta y$. Therefore $(Q,+)$ is a commutative loop.

Let $v = 0$ in relation (3). Since $\alpha, \beta \in Aut(Q,+), \alpha\beta = \beta\alpha$, further we obtain $(\alpha^2 x + \alpha\beta y) + \alpha\beta u = (\alpha^2 x + \alpha\beta u) + \alpha\beta y$. Then $(\alpha\beta y + \alpha^2 x) + \alpha\beta u = \alpha\beta y + (\alpha^2 x + \alpha\beta u)$, since $(Q,+)$ is a commutative loop. From the last equality we have that $(Q,+)$ is associative. Therefore $(Q,+)$ is an abelian group. It is easy to see that $0 \in (\alpha + \beta - \varepsilon)Q$.

(ii) $\Longrightarrow$ (i).

If conditions (ii) are fulfilled, then it is easy to check that the identity (1) holds. Indeed, $\alpha(\alpha x + \beta y + a) + \beta(\alpha u + \beta v + a) + a = \alpha(\alpha x + \beta u + a) + \beta(\alpha y + \beta v + a) + a$, $\alpha^2 x + \alpha\beta y + \alpha a + \beta\alpha u + \beta^2 v + \beta a + a = \alpha^2 x + \alpha\beta u + \alpha a + \beta\alpha y + \beta^2 v + \beta a + a$, $\alpha\beta y + \alpha\beta u = \alpha\beta u + \alpha\beta y$, $0 = 0$.

A quasigroup of such kind has at least one idempotent element. Indeed, let $-a = \alpha d + \beta d - d$, i.e. $\alpha d + \beta d = d - a$. Then $d \cdot d = \alpha d + \beta d + a = d - a + a = d$.

The theorem is proved.

From the proof of Theorem 1 follows the following

Corollary 1. *Any medial quasigroup $(Q,\cdot)$ with an idempotent element 0 can be presented in the form: $x\cdot y=\alpha x+\beta y$, where $(Q,+)$ is an abelian group with the identity element 0 and α,β are commuting automorphisms of the group $(Q,+)$.*

Remark. Equivalence of conditions (i) and (ii) of Theorem 1 it is possible to deduce from results of book [8] (3.1.4. Proposition).

Theorem 2. *Conditions (i) and (ii) are equivalent:*

(i) $(Q,\cdot)$ is a medial quasigroup that has not any idempotent element;

(ii) there exist an abelian group $(Q,+)$, its automorphisms α, φ, $\alpha\varphi=\varphi\alpha$, an element $a\in Q$, $-a\notin(\alpha+\varphi-\varepsilon)Q$ such that $x\cdot y=\alpha x+\varphi y+a$ for all $x,y\in Q$.

(i) $\Longrightarrow$ (ii). By proving this implication in the main we follow the book [2]. Let us consider a LP-isotope $(Q,+)$ of a medial quasigroup $(Q,\cdot)$ of the form: $x+y=R^{-1}_{r(0)}\cdot L_0^{-1}$ where $0\cdot r(0)=0$, i.e. $r(0)$ is a right local identity element of the element 0. This LP-isotope $(Q,+)$ is a loop with the identity element $0\cdot r(0)=0$. Denote $R_{r(0)}$ by α and L_0 by β. We remark that $R_{r(0)}0=0$, then $\alpha 0=0$.

Using our notations we can write medial identity in the following form:

$$\alpha(\alpha x+\beta y)+\beta(\alpha u+\beta v)=\alpha(\alpha x+\beta u)+\beta(\alpha y+\beta v). \tag{5}$$

By $x=0,y=\beta^{-1}0$ from (5) we have

$$\beta(\alpha u+\beta v)=\alpha\beta u+\beta(\alpha\beta^{-1}0+\beta v). \tag{6}$$

Therefore the permutation β is a quasiautomorphism of the loop $(Q,+)$.

By $u=0,v=\beta^{-2}0$ in (5) we have

$$\alpha(\alpha x+\beta y)=\alpha(\alpha x+\beta 0)+\beta(\alpha y+\beta^{-1}0) \tag{7}$$

and we obtain that the permutation α is a quasiautomorphism of the loop $(Q,+)$.

If we use equalities (6) and (7) in (5), then we have

$$(\alpha R_{\beta 0}\alpha x+\beta R_{\beta^{-1}0}\alpha y)+(\alpha\beta u+\beta L_{\alpha\beta^{-1}0}\beta v)=$$

$$(\alpha R_{\beta 0}\alpha x+\beta R_{\beta^{-1}0}\alpha u)+(\alpha\beta y+\beta L_{\alpha\beta^{-1}0}\beta v). \tag{8}$$

If we change in equality (8) the element x by the element $\alpha^{-1}R^{-1}_{\beta 0}\alpha^{-1}x$, the element y by $\alpha^{-1}R^{-1}_{\beta^{-1}0}\beta^{-1}y$, the element u by the element $\beta^{-1}\alpha^{-1}u$, the element v by the element $\beta^{-1}L^{-1}_{\alpha\beta^{-1}0}\beta^{-1}v$, then we have

$$(x+y)+(u+v)=(x+\beta R_{\beta^{-1}0}\alpha\beta^{-1}\alpha^{-1}u)+(\alpha\beta\alpha^{-1}R^{-1}_{\beta^{-1}0}\beta^{-1}y+v).$$

If we take $u=0$ in the last equality, then we have

$$(x+y)+v=(x+\beta R_{\beta^{-1}0}\alpha\beta^{-1}0)+(\alpha\beta\alpha^{-1}R^{-1}_{\beta^{-1}0}\beta^{-1}y+v). \tag{9}$$

If we take in (9) $v=0$, then we obtain $x+y=(x+r)+\alpha\beta\alpha^{-1}R^{-1}_{\beta^{-1}0}\beta^{-1}y$ where $r=\beta R_{\beta^{-1}0}\alpha\beta^{-1}0$ is a fixed element of the set Q.

If we change in equality (9) $x+y$ by the right side of the last equality, then we have

$$((x+r)+\alpha\beta\alpha^{-1}R^{-1}_{\beta^{-1}0}\beta^{-1}y)+v=(x+r)+(\alpha\beta\alpha^{-1}R^{-1}_{\beta^{-1}0}\beta^{-1}y+v).$$

From the last equality it follows that the loop $(Q,+)$ is associative, i.e. is a group.

Since α is quasiautomorphism of the group and $\alpha 0=0$, we have that the permutation α is an automorphism of the group $(Q,+)$. The permutation β has the form $\beta=R_a\varphi$ where $\varphi\in Aut(Q,+)$.

Then we can rewrite the medial identity in the form $\alpha^2x+\alpha\varphi y+\alpha a+\varphi\alpha u+\varphi^2v+\varphi a+a=\alpha^2x+\alpha\varphi u+\alpha a+\varphi\alpha y+\varphi^2v+\varphi a+a$ and, after the reduction in the last equality, we obtain

$$\alpha\varphi y+\alpha a+\varphi\alpha u=\alpha\varphi u+\alpha a+\varphi\alpha y. \tag{10}$$

From the last equality by $u=0$ we have $\alpha\varphi y+\alpha a=\alpha a+\varphi\alpha y$ and by $y=0$ we have $\alpha a+\varphi\alpha u=\alpha\varphi u+\alpha a$. Using these last equalities we can rewrite equality (10) in the form $\alpha a+\varphi\alpha y+\varphi\alpha u=\alpha a+\varphi\alpha u+\varphi\alpha y$. Hence $\varphi\alpha y+\varphi\alpha u=\varphi\alpha u+\varphi\alpha y$, $(Q,+)$ is an abelian group.

Then from equality $\alpha\varphi y+\alpha a=\alpha a+\varphi\alpha y$ it follows that $\alpha\varphi y=\varphi\alpha y$. Therefore $x\cdot y=\alpha x+\varphi y+a$, where $(Q,+)$ is an abelian group, α,φ are automorphisms of $(Q,+)$ such that $\alpha\varphi=\varphi\alpha$.

Now we must only demonstrate that the element $-a\notin(\alpha+\varphi-\varepsilon)Q$. Let us suppose the inverse. Let medial quasigroup $(Q,\cdot)$ have an idempotent element, for example, let $u\cdot u=u$. Then $\alpha u+\varphi u+a=u$, therefore $-a=\alpha u+\varphi u-u=(\alpha+\varphi-\varepsilon)u$ hence $-a\in(\alpha+\varphi-\varepsilon)Q$. We received a contradiction. Our assumption is not true. Hence, if medial quasigroup $(Q,\cdot)$ has not any idempotent element, then $-a\notin(\alpha+\varphi-\varepsilon)Q$.

(ii) $\Longrightarrow$ (i). This implication can be checked easy and we omit the proof of this implication. The theorem is proved.

The following theorem on the structure of finite medial quasigroups has been proved by D.C. Murdoch. We give Murdoch theorem in a slightly modernized form [9].

For a quasigroup $(Q,\cdot)$ we define the map s: $s(x)=x\cdot x$ for all $x\in Q$. As usual, $s^2(x)=s(s(x))$ and so on. For any medial quasigroup $(Q,\cdot)$ the map s is an endomorphism of this quasigroup, indeed, $s(xy)=xy\cdot xy=xx\cdot yy=s(x)\cdot(y)$.

Definition 1. *A quasigroup $(Q,\cdot)$ is called an unipotently-solvable quasigroup of degree m if there exists the following finite chain of unipotent quasigroups:*

$$Q/s(Q),s(Q)/s^2(Q),\dots,s^m(Q)/s^{m+1}(Q),$$

where the number m is the minimal number with the property $|s^m(Q)/s^{m+1}(Q)|=1$ [9].

Theorem 3. *Any finite medial quasigroup $(Q,\cdot)$ is isomorphic to the direct product of a medial unipotently-solvable quasigroup $(Q_1,\circ)$ and a principal isotope of the form $(\varepsilon,\varepsilon,\gamma)$ of a medial idempotent quasigroup $(Q_2,*)$, where $\gamma\in Aut(Q_2,*)$.*

It is clear that Theorem 3 reduces the study of the structure of finite medial quasigroups to the study of the structure of finite medial unipotent and idempotent quasigroups.

We notice, for any unipotent quasigroup $(Q,\cdot)$ with idempotent element e we have $s(Q)=e$, for any idempotent quasigroup $(Q,\cdot)$ we have $s=\varepsilon$. Therefore, in these cases we cannot say anything on the structure of medial unipotent and medial idempotent quasigroup using the endomorphism s.

As it has been mentioned above, simple medial quasigroups were described by J. Ježek and T. Kepka in [7]. We recall some definitions. As usual, a binary relation θ is an equivalence relation on Q if and only if θ is a reflexive, symmetric and transitive subset of Q^2. An equivalence θ is a *congruence* of a quasigroup $(Q,\cdot)$ if and only if the following implications are true: $a\theta b \Longrightarrow ac\theta bc$ and $a\theta b \Longrightarrow ca\theta cb$ for all $a,b,c\in Q$.

A congruence θ of a quasigroup $(Q,\cdot)$ is called *normal* if the following implications are true: $ac\theta bc \Longrightarrow a\theta b$, $ca\theta cb \Longrightarrow a\theta b$ for all $a,b,c\in Q$ [1,3].

A quasigroup $(Q,\cdot)$ is *simple* if its only normal congruences are the diagonal $\hat{Q}=\{(q,q)\,|q\in Q\}$ and $Q\times Q$ [1,3].

We give Ježek-Kepka Theorem in the following form [10].

Theorem 4. *If a medial quasigroup $(Q,\cdot)$ of the form $x\cdot y=\alpha x+\beta y+a$ over an abelian group $(Q,+)$ is simple, then*

1. *the group $(Q,+)$ is the additive group of a finite Galois field $GF(p^k)$;*
2. *the group $<\alpha,\beta>$ is the multiplicative group of the field $GF(p^k)$ in the case $k>1$, the group $<\alpha,\beta>$ is any subgroup of the group $Aut(Z_p,+)$ in the case $k=1$;*
3. *the quasigroup $(Q,\cdot)$ in the case $|Q|>1$ can be quasigroup from one of the following disjoint quasigroup classes:*
   (a) *$\alpha+\beta=\varepsilon, a=0$; in this case the quasigroup $(Q,\cdot)$ is an idempotent quasigroup;*
   (b) *$\alpha+\beta=\varepsilon$ and $a\neq 0$; in this case the quasigroup $(Q,\cdot)$ does not have any idempotent element, the quasigroup $(Q,\cdot)$ is isomorphic to the quasigroup $(Q,*)$ with the form $x*y=\alpha x+\beta y+1$ over the same abelian group $(Q,+)$;*
   (c) *$\alpha+\beta\neq\varepsilon$; in this case the quasigroup $(Q,\cdot)$ has exactly one idempotent element, the quasigroup $(Q,\cdot)$ is isomorphic to the quasigroup $(Q,\circ)$ of the form $x\circ y=\alpha x+\beta y$ over the group $(Q,+)$.*

Proposition 1. *Any medial quasigroup $(Q,\circ)$ of the form $x\circ y=\alpha x+\beta y$ over an abelian group $(Q,+)$, where $\alpha+\beta\neq\varepsilon$, is either an unipotent quasigroup, or it is a principal isotope of the medial idempotent quasigroup $(Q,\cdot)$ of the form $x\cdot y=(\alpha+\beta)^{-1}(\alpha x+\beta y)$.*

Proof. If we suppose, that $(\alpha+\beta)x = 0$ for all $x \in Q$, where 0 denotes zero element of the group $(Q,+)$, then $x \circ x = \alpha x + \beta x = (\alpha+\beta)x = 0$ for all $x \in Q$.

If $\alpha + \beta \neq 0$, then there exists an element μ of the group $Aut(Q,+)$ such that $\mu(\alpha+\beta) = \varepsilon$, i.e. $\mu = (\alpha+\beta)^{-1}$. Therefore, $x \cdot x = (\alpha+\beta)^{-1}(\alpha x + \beta x) = (\alpha+\beta)^{-1}(\alpha+\beta)x = x$ for all $x \in Q$.

The quasigroup $(Q,\cdot)$ is medial ([12], Theorem 25). We repeat the proof of Theorem 25: since $\mu\alpha + \mu\beta = \varepsilon$, we have $\mu\alpha\mu\beta = \mu\alpha(\varepsilon - \mu\alpha) = \mu\alpha - (\mu\alpha)^2 = (\varepsilon - \mu\alpha)\mu\alpha = \mu\beta\mu\alpha$. The proposition is proved.

It is well known that the direct product of medial idempotent quasigroups is an idempotent quasigroup, a similar situation takes place for unipotent quasigroups.

Proposition 2. *If $(Q,\cdot)$ is a medial quasigroup such that $(Q,\cdot) = (Q_1,\cdot_1) \times (Q_2,\cdot_2)$ and the forms of quasigroups $(Q,\cdot)$, $(Q_1,\cdot_1)$ and $(Q_2,\cdot_2)$ are defined over groups $(Q,+)$, $(Q_1,+_1)$ and $(Q_2,+_2)$ respectively, then $(Q,+) \cong (Q_1,+_1) \times (Q_2,+_2)$* [9].

Example 1. *There exist directly irreducible finite idempotent medial quasigroups, finite unipotent medial quasigroups.*

Proof. We denote by $(Z_9,+)$ the additive group of residues modulo 9. The quasigroup $(Z_9,\circ)$ of the form $x \circ y = 2 \cdot x + 8 \cdot y$ is a medial idempotent quasigroup, quasigroup $(Z_9,*)$ of the form $x * y = 1 \cdot x + 8 \cdot y$ is a medial unipotent quasigroup.

These quasigroups are not simple. Indeed, if $Q = \{0,3,6\}$, then $(Q,\circ) \lhd (Z_9,\circ)$ and $(Q,*) \lhd (Z_9,*)$.

These quasigroups are directly irreducible. Indeed, if we suppose, that these quasigroups are directly reducible, then by Proposition 2 the group $(Z_9,+)$ is reducible into the direct product of subgroups of order 3. As it is well known [11], it is not true.

Proposition 3. *Any subquasigroup $(H,\cdot)$ of a medial quasigroup $(Q,\cdot)$ is normal, i.e. the set H coincides with an equivalence class of a normal congruence θ of the quasigroup $(Q,\cdot)$* ([12], Theorem 43).

Taking into consideration Proposition 3 we can say that in a simple medial quasigroup $(Q,\cdot)$ its only subquasigroups are one-element subquasigroups and the quasigroup $(Q,\cdot)$.

Remark. We notice, in general there exist non-simple medial quasigroups with only trivial subquasigroups. For example, the quasigroup $(Z_9,\diamond)$ with the form $x \diamond y = 2 \cdot x + 8 \cdot y + 1$, where $(Z_9,+)$ is the additive group of residues modulo 9, is a non-simple quasigroup without proper subquasigroups.

But situation is better for medial idempotent and medial unipotent quasigroups, since these quasigroups contain idempotent elements.

It is known ([1], p. 57; [2], p. 41), if θ is a normal congruence of a quasigroup $(Q,\cdot)$ and there exists an idempotent element e of the quasigroup $(Q,\cdot)$, then the equivalence class $\theta(e)$ forms a normal subquasigroup $(\theta(e),\cdot)$ of the quasigroup $(Q,\cdot)$.

We can summarize our remarks in the following

Proposition 4. *In an idempotent medial quasigroup or in an unipotent medial quasigroup $(Q,\cdot)$ any normal congruence θ contains at least one equivalence class $\theta(e)$ such that $(\theta(e),\cdot)$ is a normal subquasigroup of the quasigroup $(Q,\cdot)$.*

Proof. Any subquasigroup of an idempotent quasigroup is an idempotent subquasigroup, any subquasigroup of an unipotent quasigroup is an unipotent subquasigroup.

To reformulate Theorem 3 in more details we give the following

Definition 2. *We shall say that a quasigroup $(Q,\cdot)$ is solvable if there exists the following finite chain of quasigroups*

$$Q/Q_1, Q_1/Q_2, \ldots, Q_m/Q_{m+1},$$

where the quasigroup Q_{i+1} is a maximal normal subquasigroup of the quasigroup Q_i and m is the minimal number such that $|Q_m/Q_{m+1}| = 1$.

Remark. Definition 2 differs from definition of solvability of groups [11].

Proposition 5. *Any finite medial idempotent quasigroup $(Q,\cdot)$ is solvable and any quasigroup Q_i/Q_{i+1} is a finite simple medial idempotent quasigroup.*

Proof. The proof it follows from Proposition 4 and the fact that the quasigroup $(Q,\cdot)$ is finite. The proposition is proved.

Proposition 6. *Any finite medial unipotent quasigroup $(Q,\cdot)$ is solvable and any quasigroup Q_i/Q_{i+1} is a finite simple medial unipotent quasigroup.*

Proof. The proof is similar to the proof of Proposition 5.

Taking into consideration Propositions 5 and 6 we can concretize Theorem 3.

Theorem 5. *Any finite medial quasigroup $(Q,\cdot)$ is isomorphic to the direct product of a medial unipotently-solvable quasigroup $(Q_1,\circ)$ and a principal isotope of a medial idempotent quasigroup $(Q_2,*)$, where the quasigroups $(Q_i,\circ)/(Q_{i+1},\circ)$ and $(Q_2,*)$ are solvable for all admissible values of index i, $\gamma \in Aut(Q_2,*)$.*

Theorem 6. *A quasigroup $(Q,\cdot)$ of the form $x\cdot y = \alpha x + \beta y$ is isomorphic to a quasigroup $(Q,*)$ of the form $x*y = \gamma x + \delta y$, where $\alpha,\beta,\gamma,\delta$ are automorphisms of an abelian group $(Q,+)$, if and only if there exists an automorphism ψ of the group $(Q,+)$ such that $\psi\alpha = \gamma\psi$, $\psi\beta = \delta\psi$.*

Proof. The proof of this theorem, in fact, repeats the proof of the similar theorem from [14] and we omit it.

It is easy to see that Theorem 6 is true for medial idempotent quasigroups and for medial unipotent quasigroups.

Example 2. *We denote by $(Z_{16},+)$ the additive group of residues modulo 16. The quasigroup $(Z_{16},\circ)$ of the form $x\circ y = 3\cdot x + 15\cdot y + 1$ is isomorphic to the quasigroup $(Q,*)$ of the form $x*y = 3\cdot x + 15\cdot y$.*

This follows from Theorem 1. Furthermore, the quasigroup $(Q,*)$ is a quasigroup with the unique idempotent element 0, the quasigroup $(Q,*)$ is an unipotently-solvable quasigroup of degree 4, since $s^4(Q) = s^5(Q)$.

Example 3. *Let $(Z_{16}, +)$ be the additive group of residues modulo 16. The quasigroup $(Z_{16}, *)$ of the form $x * y = 1 \cdot x + 15 \cdot y$ is a solvable unipotent quasigroup of degree 3.*

Some results of this note were announced in [15].

Acknowledgement. The author thanks Prof. E.A. Zamorzaeva for her helpful comments.

References

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

[2] Belousov V.D. *Elements of the quasigroup theory, A special course*. Kishinev, 1981 (in Russian).

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

[4] Murdoch D.C. *Structure of abelian quasigroups*. Trans. Amer. Math. Soc., 1941, **47**, p. 134–138.

[5] Toyoda K. *On axioms of linear functions*. Proc. Imp. Acad. Tokyo, 1941, **17**, p. 221–227.

[6] Bruck R.H. *Some results in the theory of quasigroups*. Trans. Amer. Math. Soc., 1944, **55**, p. 19–52.

[7] Ježek J., Kepka T. *Varieties of abelian quasigroups*. Czech. Mathem. J., 1977, **27**, p. 473–503.

[8] Ježek J., Kepka T. *Medial groupoids*. Rozpravy Československe Academie VĚD, 1983, Ročnik 93, sešit 2, Academia, Praha.

[9] Shcherbacov V.A. *On structure of finite n-ary medial quasigroups and automorphism groups of these quasigroups*. Quasigroups and Related Systems, 2005, **13** (accepted for publication.)

[10] Shcherbacov V.A. *On simple n-ary medial quasigroups*. Proceedings of Conference "Computational Commutative and Non-Commutative Algebraic Geometry", to be published in NATO Science Series III. Computer and Systems Sciences, IOS Press.

[11] Kargapolov M.I., Merzlyakov Yu.I. *Foundations of the Group Theory*. Moskva, Nauka, 1977, (in Russian).

[12] Kepka T., Němec P. *T-quasigroups, II*. Acta Universitatis Carolinae, Math. et Physica, 1971, **12**, N 2, p. 31–49.

[13] Němec P., Kepka T. *T-quasigroups, I*. Acta Universitatis Carolinae, Math. et Physica, 1971, **12**, N 1, p. 39–49.

[14] Shcherbacov V.A. *On leftdistributive quasigroups isotopic to groups*. Proceedings of the XI Conference of Young Scientists of Friendship of Nations University, Moskva, 1988. Dep. v VINITI 01.07.88, No 5305-B88, p. 148–149, (in Russian).

[15] Shcherbacov V.A. *On Bruck-Toyoda-Murdoch theorem and isomorphisms of some quasigroups*. First Conference of the Mathematical Society of the Republic Moldova, Chişinău, August 16–18, 2001, p. 138–139.

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
5 Academiei str., Chişinău MD−2028
Moldova
E-mail: *scerb@math.md*

Received March 4, 2005