Quasigroups and Related Systems **13** (2005), 125 – 156

On structure of finite n-ary medial quasigroups and automorphism groups of these quasigroups

Victor Shcherbacov

Abstract

We prove that any finite medial n-ary quasigroup is isomorphic to the direct product of a medial unipotently-solvable quasigroup and a principal isotope of a medial idempotent quasigroup. For binary case similar theorem was proved by D.C. Murdoch. This theorem gives a possibility to obtain information on automorphism groups of finite n-ary medial quasigroups.

1. Introduction

We shall use basic terms and concepts from books and articles [3], [5], [6], [25], [36], [45], [56], [58].

1.1. n-ary quasigroups and codes

We recall some known facts. Let Q be a nonempty set, let n be natural number, $n \geqslant 2$. A map f that maps all n-tuples over Q into elements of the set Q is called an *n-ary operation*, i.e. $f(x_1, x_2, \ldots, x_n) = x_{n+1}$ for all $(x_1, x_2, \ldots, x_n) \in Q^n$ and $x_{n+1} \in Q$.

We can define an n-ary operation f as the set $\mathfrak{F}$ of $(n+1)$-tuples of the following form $(x_1, x_2, \ldots, x_n, f(x_1, x_2, \ldots, x_n))$, where $x_1, x_2, \ldots, x_n$, $f(x_1, x_2, \ldots, x_n) \in Q$. Two n-ary operations f and g defined on a set Q are equal if and only if $\mathfrak{F} = \mathfrak{G}$.

A sequence $x_m, x_{m+1}, \ldots, x_n$ will be denoted by x_m^n. Of course, m, n are natural numbers with $m \leqslant n$. As usual in the study of n-ary quasigroups, $\overline{1,n} = \{1, 2, \ldots, n\}$ [5].

2000 Mathematics Subject Classification: 20N15, 20N05
Keywords: Quasigroup, medial quasigroup, multiplication group of a quasigroup, n-ary quasigroup, automorphism.

This definition of n-ary quasigroups was given by V.D. Belousov and M.D. Sandik in 1966 ([7]).

Definition 1. A nonempty set Q with an n-ary operation f such that in the equation $f(x_1, x_2, \ldots, x_n) = x_{n+1}$ knowledge of any n elements of $x_1, x_2, \ldots, x_n, x_{n+1}$ uniquely determines the remaining one is called an *n-ary quasigroup* or shortly: *n-quasigroup* ([7], [5]).

Some applications of n-ary quasigroups in Coding Theory there are in [40, 41]. We add the following definitions to make situation more clear and to show that n-ary medial quasigroups have some applications in practice, therefore study of n-ary quasigroups has not only purely theoretical motivation.

A check digit system $\mathfrak{C}$ with one check character is a systematic error detecting code over an alphabet Q which arises by appending *a check digit* a_{n+1} to every word $a_1 a_2 \ldots a_n \in Q^n$ [53].

We can view the code $\mathfrak{C}$ as a mapping over an alphabet Q such that the check symbol a_{n+1} is obtained from information symbols $a_1, a_2, \ldots, a_n$ in the following manner: $g(a_1, a_2, \ldots, a_n) = a_{n+1}$, where g is an n-ary operation on the set Q ([40]). The code $\mathfrak{C}$ was called in [40] an *n-ary code* (Q, g).

If in an n-ary code (Q, g) the operation g is an n-ary quasigroup operation, then this code is called an *n-quasigroup code* (Q, g).

Theorem 1. *Any n-ary code (Q, g) detects all single errors if and only if it is an n-ary quasigroup code* ([11, 40]).

1.2. Isotopy of n-ary quasigroups, translations

We say that n-ary quasigroup (Q, f) is an *isotope of n-ary quasigroup* (Q, g) if there exist permutations $\mu_1, \mu_2, \ldots, \mu_n, \mu$ of the set Q such that

$$f(x_1, x_2, \ldots, x_n) = \mu^{-1} g(\mu_1 x_1, \ldots, \mu_n x_n) \tag{1}$$

for all $x_1, \ldots, x_n \in Q$. We can write this fact also in the form $(Q, f) = (Q, g)T$, where $T = (\mu_1, \mu_2, \ldots, \mu_n, \mu)$.

If in (1) $f = g$, then $(n+1)$-tuple $(\mu_1, \mu_2, \ldots, \mu_n, \mu)$ of permutations of the set Q is called an *autotopy of n-quasigroup* (Q, f). The last component of an autotopy of an n-quasigroup is called a *quasi-automorphism* (by the analogy with binary case).

If in (1) $\mu_1 = \mu_2 = \cdots = \mu_n = \mu$, then quasigroups (Q, f) and (Q, g) are isomorphic.

At last, if in (1) the n-ary operations f and g are equal and $\mu_1 = \mu_2 = \cdots = \mu_n = \mu$, then we obtain an *automorphism of quasigroup* (Q, f), i.e. a permutation μ of the set Q is called an automorphism of an n-quasigroup (Q, f) if for all $x_1, \ldots, x_n \in Q$ the following relation is fulfilled: $\mu f(x_1, \ldots, x_n) = f(\mu x_1, \ldots, \mu x_n)$. We denote by $Aut(Q, f)$ the automorphism group of an n-ary quasigroup (Q, f).

As usual, $L_a^\circ : L_a^\circ x = a \circ x$, $R_a^\circ : R_a^\circ x = x \circ a$ are respectively left and right translations of binary quasigroup $(Q, \circ)$. We shall omit denotation of a quasigroup operation by using of quasigroup translations, i.e. we shall write L_a, R_a instead of L_a°, R_a°, in cases when it will be clear from context relatively which quasigroup operation we take quasigroup translations.

$M(Q, \cdot)$ denotes the group generated by all left and right translations of a binary quasigroup $(Q, \cdot)$ and it is called the *multiplication group of a quasigroup* $(Q, \cdot)$.

An element d of an n-ary quasigroup (Q, f) such that $f(d, \ldots, d) = d$ is called an *idempotent element* of quasigroup (Q, f) (in brackets we have taken the element d exactly n times). In binary case an element $d \in Q$ such that $d \cdot d = d$ is called an idempotent element of quasigroup $(Q, \cdot)$.

We shall denote the identity permutation as ε, the order of a set Q as $|Q|$.

1.3. Linear n-ary quasigroups

An n-ary quasigroup (Q, g) of the form

$$\gamma g(x_1, x_2, \ldots, x_n) = \gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_n x_n, \tag{2}$$

where $(Q, +)$ is a group, $\gamma, \gamma_1, \ldots, \gamma_n$ are some permutations of Q, we shall call an *n-ary group isotope*. This equality (as well as analogous equalities that will appear later in this article) is true for all $x_1, x_2, \ldots, x_n \in Q$.

Remark 1. It is easy to see that $(Q, g) = (Q, f)T$, where $f(x_1^n) = x_1 + x_2 + \cdots + x_n$ and the isotopy T has the form $(\gamma_1, \gamma_2, \ldots, \gamma_n, \gamma)$.

Following articles [35, 44] we shall call the equality (2) *the form of quasigroup* (Q, g).

An n-ary quasigroup (Q, f) with the form $f(x_1^n) = x_1 + x_2 + \cdots + x_n$, where $(Q, +)$ is a binary group, will be called as *n-ary derivative group of*

a binary group $(Q,+)$ ([5, 48]). Sometimes we shall denote this quasigroup as $(Q,\overset{n}{+})$.

Remark 2. The form of a quasigroup (Q,g) is some analytical definition of the n-ary operation g over a group $(Q,+)$ similar to definition of a function with help of a formula over field of real numbers or over field of some other kind of numbers.

Remark 3. In algebra usually quasigroups are studied up to isomorphism. Therefore in some cases, without loss of a generality, we will be able to choose an isotopy T of an n-ary quasigroup (Q,g) in such manner that its last component is the identity map.

Definition 2. An n-quasigroup (Q,g) of the form

$$g(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + a = \sum_{i=1}^{n} \alpha_i x_i + a, \tag{3}$$

where $(Q,+)$ is a group, $\alpha_1,\ldots,\alpha_n$ are some automorphisms of the group $(Q,+)$, the element a is some fixed element of the set Q, will be called a *linear n-ary quasigroup* (over group $(Q,+)$).

Example 1. *Gluskin-Hosszú theorem.*
Any n-ary group (Q,g) ([5, 20, 25, 48]) has the following form

$$g(x_1^n) = x_1 + \theta x_2 + \theta^2 x_3 + \cdots + \theta^{n-2} x_{n-1} + \theta^{n-1} x_n + c,$$

where $(Q,+)$ is a binary group, $\theta \in Aut(Q,+)$, $c \in Q$, $\theta^{n-1}x = c + x - c$ and $\theta c = c$.

This theorem firstly was proved in [29]. The elegant short proof is given in [57]. Some important generalizations are proved in [21, 22].

From this theorem it follows that any n-ary group is a linear n-ary quasigroup. In some sense this theorem can be considered as a definition of n-ary groups. The question when an n-ary quasigroup defined by (3) is an n-ary group is solved in [59].

Lemma 1. *The form of a linear n-ary quasigroup (Q,g) over a fixed group $(Q,+)$ defines the quasigroup (Q,g) by the unique way.*

Proof. If we suppose that

$$g(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + a = \beta_1 x_1 + \beta_2 x_2 + \cdots + \beta_n x_n + b, \tag{4}$$

then, if in equality (4) we put $x_1 = \cdots = x_n = 0$, we obtain $a = b$. Further, if we suppose that in equality (4) $x_2 = \cdots = x_n = 0$, then $\alpha_1 = \beta_1$, since $a = b$. If we take in (4) $x_1 = x_3 = x_4 = \cdots = x_n = 0$, then $\alpha_2 = \beta_2$ and so on. □

An n-ary linear quasigroup (Q, g) over an abelian group $(Q, +)$ is called *n-T-quasigroup* [58]. If $n = 2$, then a quasigroup from this quasigroup class is called a *T-quasigroup* [35, 44].

1.4. n-ary medial quasigroups

The following identity of an n-ary quasigroup (Q, g)

$$g(g(x_{11}, x_{12}, \ldots, x_{1n}), g(x_{21}, x_{22}, \ldots, x_{2n}), \ldots, g(x_{n1}, x_{n2}, \ldots, x_{nn})) = g(g(x_{11}, x_{21}, \ldots, x_{n1}), g(x_{12}, x_{22}, \ldots, x_{n2}), \ldots, g(x_{1n}, x_{2n}, \ldots, x_{nn})) \quad (5)$$

is called medial identity [5]. An n-ary quasigroup with identity (5) is called a *medial n-ary quasigroup*.

In binary case from identity (5) we obtain usual *medial identity*:

$$xy \cdot uv = xu \cdot yv.$$

For a medial n-ary group the group $(Q, +)$ from Gluskin-Hosszú theorem must be abelian. Other properties of medial n-ary groups are described in [18] and [26] (see also [20]). Some special medial n-ary groups which are a set-theoretic union of finite medial n-ary groups are studied in [17].

Medial quasigroups, as well as the other classes of quasigroups isotopic to groups, give us a possibility to construct quasigroups with preassigned properties. Often it is possible to express these properties on the language of properties of groups and components of isotopy. Systematically this approach was used by study of T-quasigroups in [33], [32], [35], [44].

In [42] D.C. Murdoch proved that any finite binary medial quasigroup $(Q, \cdot)$ is either a quasigroup with a unique idempotent element, or it is a quasigroup in which the map e ($e : x \mapsto e(x)$, where $x \cdot e(x) = x$), is a permutation, or it is isomorphic to the direct product of a quasigroup $(A, \cdot)$ with a unique idempotent element and a quasigroup $(B, \cdot)$ in which the map e ($e : x \mapsto e(x)$) is a permutation.

It is easy to see that in the Murdoch theorem it is possible to use the map f, $f(x) \cdot x = x$. A little bit other proof of this theorem is for the map $s : x \mapsto s(x), s(x) = x \cdot x$. For us the map s is more suitable in n-ary ($n \geqslant 3$) case to prove an n-ary analog of Murdoch theorem. See below.

In [5] V.D. Belousov proved the following theorem. This theorem follows from results of T. Evans ([23], Theorem 6.2.), too.

Theorem 2. *Let (Q, f) be a medial n-quasigroup. Then there exist an abelian group $(Q, +)$, its pairwise commuting automorphisms $\alpha_1, \ldots, \alpha_n$, and a fixed element a of the set Q such that*

$$f(x_1, x_2, \ldots, x_n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + a = \sum_{i=1}^{n} \alpha_i x_i + a$$

for all $x_i \in Q$, $i \in \overline{1,n}$.

In a binary case from Theorem 2 it follows the classical Toyoda theorem (T-theorem) ([3], [6], [12], [42], [60]).

Remark 4. We notice, n-ary quasigroups arise in different areas of mathematics at study of various objects. Properties of n-ary medial quasigroups are described in many articles from various points of view, see, for example [1, 4, 8, 13, 14, 18, 23, 26, 43, 46, 47, 60]. The author thanks Referees for information on articles devoted n-ary medial quasigroups and listed in this remark.

Remark 5. From Theorem 2 it follows that any n-ary medial quasigroup (Q, f) can be represented as an isotope of an n-ary derivative group $(Q, \overset{n}{+})$ of an abelian group $(Q, +)$, namely $(Q, f) = (Q, \overset{n}{+})T$, where the isotopy T has the form $(\alpha_1, \ldots, \alpha_{n-1}, L_a^+ \alpha_n, \varepsilon)$, $\alpha_1, \ldots, \alpha_n \in Aut(Q, +)$, $L_a^+ x = a + x$.

1.5. Some elementary properties of binary quasigroups

We shall use the following elementary properties of binary quasigroups.

Lemma 2.

(*i*) *If $(Q, \cdot)$ is a binary quasigroup, L_a, R_b are some its left and right translations, $\varphi \in Aut(Q, \cdot)$, then $\varphi L_a = L_{\varphi a}\varphi$, $\varphi R_b = R_{\varphi b}\varphi$.*

(*ii*) *If $(Q, +)$ is a group, then $L_a R_b = R_b L_a$, $L_a^{-1} = L_{-a}, R_a^{-1} = R_{-a}$.*

(*iii*) *If $(Q, +)$ is a group, then $R_d = L_d I_d$, where I_d is the inner automorphism of the group $(Q, +)$, i.e. $I_d x = -d + x + d$ for all $x \in Q$.*

(*iv*) *Any quasi-automorphism of a group $(Q, +)$ has the form $L_a \beta$, where $a \in Q$, $\beta \in Aut(Q, +)$.*

Proof. (i) We have $\varphi L_a x = \varphi(a \cdot x) = \varphi a \cdot \varphi x = L_{\varphi a}\varphi x$, $\varphi R_b x = \varphi(x \cdot b) = \varphi x \cdot \varphi b = R_{\varphi b}\varphi x$.

(ii) $L_aR_bx = a + (x + b) = (a + x) + b = R_bL_ax$. $L_a^{-1} = L_{-a}$ since $L_a^{-1}L_ax = x = -a + a + x = L_{-a}L_ax$.

(iii) $R_dx = x + d = d - d + x + d = L_dI_dx$.

(iv) Any autotopy of a group $(Q, +)$ has the form $(L_c\theta, R_d\theta, L_cR_d\theta)$, where $\theta \in Aut(Q, +)$, L_c is a left and R_d is a right translation of the group $(Q, +)$ ([3], [6], [45]). Using (iii) further we have $L_cR_d\theta = L_cL_dI_d\theta = L_a\beta$. □

2. Congruences and direct products of quasigroups

Now we are needed in an n-quasigroup homomorphic theory and in some facts from universal algebra ([3], [6], [15], [45], [54], [58]). Most of the results of this section is a specification for n-ary quasigroups of results on Ω-algebras [15]). We do not give the definition of Ω-algebra in this article, but we would like to notice that an n-ary quasigroup is an Ω-algebra. Almost all lemmas in this paragraph are very known for binary quasigroups ([3], [45]).

2.1. Congruences and translations of n-ary quasigroups

Definition 3. ([45]) Let (Q, f) and (H, g) be n-ary quasigroups, and let φ be a single valued mapping of Q into H such that $\varphi f(x_1, \ldots, x_n) = g(\varphi x_1, \ldots, \varphi x_n)$, then φ is called a *homomorphism* of (Q, f) into (H, g) and the set $\{\varphi x \mid x \in Q\}$ is called a *homomorphic image* of (Q, f) under φ.

Even in the case $n = 2$ a homomorphic image of an n-ary quasigroup (Q, f) does not have to be a quasigroup [2], i.e class of n-ary quasigroups with signature that consists of one n-ary operation is not closed in regard to homomorphic images.

To avoid appearance of non-quasigroup homomorphic images the notion of normal congruences is defined. Any normal congruence induces such homomorphism that its (homomorphic) image is a quasigroup. To prove this fact we give some definitions.

If (B, f) and (C, g) are n-ary quasigroups (Ω-algebras), C is a subset of B (written $C \subseteq B$) and C is closed under the action f, then (C, f) is said to be a *subalgebra of* (B, f), written $(C, f) \leqslant (B, f)$ [54].

As usual, a binary relation θ is an equivalence relation on Q if and only if θ is reflexive, symmetric and transitive subset of Q^2 [15, 27].

Let V be an equivalence relation on Q. The notion xVy will often be used instead of $(x, y) \in V$. The equivalence class x^V is $\{y \in Q \mid xVy\}$. A^V

will denote the set of equivalence classes, and $nat\, V : Q \to Q^V; x \mapsto x^V$ the natural projection.

Definition 4. An equivalence θ is a congruence of an n-ary quasigroup (Q, f) if and only if such implication is true: $a_i \theta b_i, i = \overline{1,n} \Longrightarrow f(a_1^n)\theta f(b_1^n)$. In other words, an equivalence θ is a *congruence* of (Q, f) if and only if θ is a subalgebra of $(Q \times Q, (f, f))$.

A translation of an n-ary quasigroup (Q, f) will be denoted as

$$T(a_1, \ldots, a_{i-1}, -, a_{i+1}, \ldots, a_n)$$

where $a_i \in Q$ for all $i \in \overline{1,n}$ and

$$T(a_1, \ldots, a_{i-1}, -, a_{i+1}, \ldots, a_n)x = f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_n).$$

for all $x \in Q$.

From the definition of an n-ary quasigroup it follows that any translation of an n-ary quasigroup (Q, f) is a permutation of the set Q.

Let $\mathbf{T}(Q, f)$ be a set all translations defined above,

$$\mathbf{T^{-1}}(Q, f) = \{T^{-1} \,|\, T \in \mathbf{T}(Q, f)\}.$$

The semigroup generated by the set $\mathbf{T}$ will be denoted by $\Pi\mathbf{T}(Q, f)$ (often for a short $\Pi\mathbf{T}$), group generated by the set $\mathbf{T}$ will be denoted by $\mathrm{M}\mathbf{T}$.

If θ is an equivalence on a set Q, α is a permutation of the set Q and from $x\theta y$ it follows $\alpha x \theta \alpha y$ for all $(x, y) \in \theta$, then we shall say that the equivalence θ admits permutation α.

Remark 6. Slightly other definition of admissibility is given in [15].

Lemma 3. ([15], Proposition II.6.1) *Every congruence θ admits any element of the semigroup $\Pi\mathbf{T}(Q, f)$.*

Proof. If $a_1\theta b_1, a_2\theta a_2, \ldots, a_n\theta a_n$, then from Definition 4 it follows that $f(a_1, a_2^n)\theta f(b_1, a_2^n)$. Therefore the congruence θ admits the translation $T(-, a_2^n)$ and so on. □

Definition 5. ([58]). The congruence θ on an n-quasigroup (Q, f) is called *normal* if for every $i = \overline{1,n}$ and for every $(c_1^n) \in Q^n$ the following implication is true:

$$f(c_1^{i-1}, a, c_{i+1}^n)\, \theta\, f(c_1^{i-1}, b, c_{i+1}^n) \Longrightarrow a\theta b,$$

where $a, b \in Q$.

Lemma 4. *If a congruence θ admits any element of the set $\mathbf{T^{-1}}$, then θ is a normal congruence.*

Proof. Let $f(c_1^{i-1}, a, c_{i+1}^n)\,\theta\, f(c_1^{i-1}, b, c_{i+1}^n)$, i.e. on language of translations

$$T(c_1^{i-1}, -, c_{i+1}^n)a\,\theta\, T(c_1^{i-1}, -, c_{i+1}^n)b.$$

Since a congruence θ admits permutations from the set $\mathbf{T^{-1}}$, then we have

$$T^{-1}(c_1^{i-1}, -, c_{i+1}^n)T(c_1^{i-1}, -, c_{i+1}^n)a\,\theta\, T^{-1}(c_1^{i-1}, -, c_{i+1}^n)T(c_1^{i-1}, -, c_{i+1}^n)b,$$

therefore $a\theta b$. □

Corollary 1. *A normal congruence θ of an n-quasigroup (Q, f) admits any element of the group $M\boldsymbol{T}(Q, f)$.*

Proof. By Lemma 4 and induction. □

Lemma 5. *If φ is a homomorphism of an n-quasigroup (Q, f), then φ induces the congruence $ker(\varphi)$.*

Proof. Let φ be a homomorphism of an n-ary quasigroup (Q, f) onto an n-ary groupoid (H, g). Then φ induces the equivalence relation $ker(\varphi) = \eta$ in the following way: $a\eta b$ if and only if $\varphi a = \varphi b$.

The equivalence η is a congruence. Indeed, for the equivalence η the implication $a_i\eta b_i, i = \overline{1,n} \Rightarrow f(a_1^n)\eta f(b_1^n)$ we can rewrite as

$$\varphi a_i = \varphi b_i, i = \overline{1,n} \Rightarrow \varphi(f(a_1^n)) = \varphi(f(b_1^n)).$$

Since φ is a homomorphism, we have

$$\varphi(f(a_1^n)) = \varphi(f(b_1^n)) \Longleftrightarrow g(\varphi a_1, \ldots, \varphi a_n) = g(\varphi b_1, \ldots, \varphi b_n).$$

Therefore we have the following true implication

$$\varphi a_i = \varphi b_i, i = \overline{1,n} \Rightarrow g(\varphi a_1, \ldots, \varphi a_n) = g(\varphi b_1, \ldots, \varphi b_n),$$

which completes the proof. □

Corollary 2. *If φ is a homomorphism of an n-quasigroup (Q, f) onto an n-ary quasigroup (H, g), then φ induces a normal congruence η.*

Proof. By Lemma 5 a relation $\eta = ker(\varphi)$ is a congruence. To prove that it is normal let $f(c_1^{i-1}, a, c_{i+1}^n)\eta f(c_1^{i-1}, b, c_{i+1}^n)$. Then

$$\varphi(f(c_1^{i-1}, a, c_{i+1}^n)) = \varphi(f(c_1^{i-1}, b, c_{i+1}^n)),$$
$$g(\varphi c_1^{i-1}, \varphi a, \varphi c_{i+1}^n) = g(\varphi c_1^{i-1}, \varphi b, \varphi c_{i+1}^n).$$

Since (H, g) is a quasigroup, we have $\varphi a = \varphi b,\ a\eta b$. □

Lemma 6. *If θ is a normal congruence on an n-quasigroup (Q, f), then θ determines the homomorphism $nat\,(\theta)$ of a quasigroup (Q, f) onto an n-quasigroup (Q^θ, f).*

Proof. Let θ be a normal congruence, i.e. θ admits any element of the group M**T**. The set Q^θ with an n-ary operation $f(a_1^\theta, \dots, a_n^\theta) = (f(a_1, \dots, a_n))^\theta$ forms a quasigroup.

Indeed, it is easy to see that an element $f(a_1^\theta, \dots, a_n^\theta)$ is uniquely determined. The equation $f(a_1^\theta, \dots, a_{i-1}^\theta, x^\theta, a_{i+1}^\theta, \dots, a_n^\theta) = a_{n+1}^\theta$ has a solution b^θ, where $f(a_1^{i-1}, b, a_{i+1}^n) = a_{n+1}$.

We prove that this solution is unique. Let

$$f(a_1^\theta, \dots, a_{i-1}^\theta, b_1^\theta, a_{i+1}^\theta, \dots, a_n^\theta) = f(a_1^\theta, \dots, a_{i-1}^\theta, b_2^\theta, a_{i+1}^\theta, \dots, a_n^\theta).$$

Then

$$f(a_1^{i-1}, b_1, a_{i+1}^n)\,\theta\, f(a_1^{i-1}, b_2, a_{i+1}^n) \Longrightarrow b_1\,\theta\, b_2 \Rightarrow b_1^\theta = b_2^\theta,$$

which completes the proof. □

Lemma 7. *If (Q, f) is a finite n-ary quasigroup, then any its congruence is normal and any its homomorphic image is an n-ary quasigroup.*

Proof. In a finite n-ary quasigroup (Q, f) $\Pi\mathbf{T} = M\mathbf{T}$. Indeed, for any translation T of the quasigroup (Q, f) there exist a natural number n such that $T^n = T^{-1}$.

Thus from Lemmas 3 and 4 it follows that in this case any congruence is normal.

Since a homomorphism φ of an n-ary quasigroup (Q, f) induces a congruence $ker\ (\varphi)$ (Lemma 5) and any congruence of a finite n-quasigroup is normal, then a homomorphism φ of the quasigroup (Q, f) induces a normal congruence $ker\ (\varphi)$.

From Lemma 6 it follows that a homomorphic image $nat\ ker\ (\varphi) = \varphi(Q, f)$ of the quasigroup (Q, f) is an n-ary quasigroup. □

Remark 7. Using the terminology more near to the terminology of the group theory or the ring theory we can call a quasigroup $\varphi(Q, f)$, which is a homomorphic image of a quasigroup (Q, f), as a factor-quasigroup of the quasigroup (Q, f).

Remark 8. It is possible to prove that a homomorphic image (H, g) of a homomorphism φ of a quasigroup (Q, f) is a quasigroup if and only if corresponding congruence of a homomorphism φ is normal.

2.2. Direct products of n-ary quasigroups

Direct products of quasigroups and Ω-algebras are studied in many articles and books, see, for example, [9, 10, 15, 31, 35, 54]. The concept of a direct product of quasigroups was used already in [42].

Definition 6. If (B, f) and (C, g) are n-ary quasigroups (Ω-algebras) then $B \times C$ with the action f on the first component and g on the second component is called the *direct product of* (B, f) *and* (C, g) *and denoted by* $(B \times C, (f, g))$.

We give and more usual definition of the direct product of n-ary quasigroups.

Definition 7. If (Q_1, f_1), (Q_2, f_2) are n-ary quasigroups, then their (*external*) *direct product* $(Q, f) = (Q_1, f_1) \times (Q_2, f_2)$ is the set of all ordered pairs (a', a''), where $a' \in Q_1$, $a'' \in Q_2$, and where the operation in (Q, f) is defined component-wise, that is, $f(a_1^n) = (f_1((a')_1^n), f_2((a'')_1^n))$.

That $(Q, f) = (Q_1, f_1) \times (Q_2, f_2)$ is an n-ary quasigroup is immediate.

If we have an additive form of group operations, then we shall speak instead of the direct product about the direct sum, instead of factors we shall speak about items and write $G = G_1 \oplus G_2$.

In [54] there is a definition of the (internal) direct product of Ω-algebras. For our aims this approach is more preferable. We notice that internal direct products of quasigroups and Ω-algebras was studied in many articles, some of these articles are listed above.

If U and W are equivalence relations on a set A, then

$$U \circ W = \{(x, y) \in A^2 \mid \exists\, t \in A, xUtWy\}$$

and

$$U \vee W = \{(x, y) \in A^2 \mid \exists\, n \in N,\ \exists\, t_0, t_1, \ldots, t_{2n} \in A, \\ x = t_0 U t_1 W t_2\, U \ldots U t_{2n-1} W t_{2n} = y\}.$$

$U \vee W$ is an equivalence relation on A called the *join* of U and W. If U and W are equivalence relations on A for which $U \circ W = W \circ U$, then we say that U and W are said to commute [54]. In this case $U \circ W = U \vee W$.

If A is an Ω-algebra and U, W are congruences on A, then $U \vee W$, and $U \cap W$ are also congruences on A.

Definition 8. If U and W are congruences on the algebra A which commute and for which $U \cap W = \hat{A} = \{(a, a) | \forall\, a \in A\}$, then the join $U \circ W = U \vee W$ of U and W is called the *direct product* $U \sqcap W$ *of* U *and* W [54].

The following theorem establishes the connection between concepts of internal and external direct products of Ω-algebras ([54], p.16).

Theorem 3. *Ω-algebra A is isomorphic to a direct product of Ω-algebras B and C with an isomorphism $e : A \to B \times C$, if and only if there exist such congruences U and W of A for which $A^2 = U \sqcap W$.*

Proof. If $e : A \to B \times C$ is an isomorphism, and $\varphi : B \times C \to B$ and $\psi : B \times C \to C$ are projections, $U = ker\, \varphi e$, $W = ker\, \psi e$. Then $A^2 = U \sqcap W$.

Conversely, if $A^2 = U \sqcap W$, then every element of A is uniquely determined by its U-class and its V-class. Thus $A^2 = A^U \times A^W$. □

Lemma 8. *If (Q, f) is a finite n-ary quasigroup, then each pair of congruences on (Q, f) commute.*

Proof. From [38] it follows that congruences commute on all algebras with transitive groups of invertible translations. A translation is invertible if it is a product of translations of this algebra.

Since in finite n-ary quasigroup for any translation T there exists a finite natural number k such that $T^k = \varepsilon$, then $T^{k-1} = T^{-1}$, i.e. every translation is invertible.

For any pair of elements a and b of a quasigroup (Q, f) there exists a translation $T(-, c_2^n)$ such that $T(-, c_2^n)a = b$. For example, elements $c_3, \ldots, c_n$ can be any fixed elements of the set Q and element c_2 must be a solution of the equation $f(a, c_2, c_3^n) = b$. □

Lemmas 7, 8 give us a possibility to use Theorem 3 for finite n-ary quasigroups.

3. n-ary linear quasigroups

3.1. Multiplication groups of n-ary T-quasigroups

Theorem 4. *The multiplication group $M\mathbf{T}(Q, f)$ of an n-ary T-quasigroup (Q, f) with the form $f(x_1^n) = \sum_{j=1}^{n} \alpha_j x_j + a$ over an abelian group $(Q, +)$ has the following structure*

$$M\mathbf{T}(Q, f) \cong (\bigoplus_{j=1}^{n-1} (Q, +)_j) \leftthreetimes < \alpha_1, \ldots, \alpha_n > .$$

Proof. Any translation T_i of the quasigroup (Q, f) has the form

$$\begin{aligned} T_i(a_1^{i-1}, -, a_{i+1}^n)x &= \alpha_1 a_1 + \ldots + \alpha_{i-1}a_{i-1} + \alpha_i x + \alpha_{i+1}a_{i+1} + \cdots + \alpha_n a_n + a \\ &= \alpha_1 a_1 + \ldots + \alpha_{i-1}a_{i-1} + \alpha_{i+1}a_{i+1} + \cdots + \alpha_n a_n + a + \alpha_i x \\ &= L^+_{\alpha_1 a_1} L^+_{\alpha_2 a_2} \ldots L^+_{\alpha_{i-1}a_{i-1}} L^+_{\alpha_{i+1}a_{i+1}} \ldots L^+_{\alpha_n a_n + a} \alpha_i x. \end{aligned}$$

From the group theory ([34]) it follows that

$$M_i\mathbf{T}(Q, f) \cong (\bigoplus_{j=1}^{n-1}(Q, +)_j) \rtimes < \alpha_i > .$$

Using Lemma 2 we can prove that any element of the group $M\mathbf{T}(Q, f)$ can be represented in the form $L^+_{a_1} L^+_{a_2} \ldots L^+_{a_{n-1}} \beta$, where $a_1, \ldots, a_{n-1} \in Q$, $\beta \in < \alpha_1, \ldots, \alpha_n >$.

Further, the proof is also standard [39], and, we hope that this part of the proof can be easy re-established. □

3.2. Homomorphisms and direct products

On Algebraic Seminar at Charles University (Prague, October, 2003) Prof. Jan Trlifaj raised the following question:

Let n-ary medial quasigroup (Q, f) be a direct product of n-ary medial quasigroups (Q_1, f_1) and (Q_2, f_2), i.e. $(Q, f) \cong (Q_1, f_1) \times (Q_2, f_2)$. What connections there exist between the form f of the quasigroup (Q, f) and the forms f_1 and f_2 of the quasigroups (Q_1, f_1) and (Q_2, f_2)?

In this subsection we making attempt to answer this question. See [35, 44] for binary case.

From the definition and properties of the direct product of quasigroups we obtain the following property. *If (Q_1, f_1) is a linear quasigroup with the form $f_1((x')_1^n) = \beta_1 x'_1 +_1 \beta_2 x'_2 +_1 \cdots +_1 \beta_n x'_n +_1 b$ over a group $(Q_1, +_1)$ and (Q_2, f_2) is a linear quasigroup with the form $f_2((x'')_1^n) = \gamma_1 x''_1 +_2 \gamma_2 x''_2 +_2 \cdots +_2 \gamma_n x''_n +_2 c$ over a group $(Q_2, +_2)$, then $(Q, f) = (Q_1, f_1) \times (Q_2, f_2)$ is a linear quasigroup with the form $f(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + a$ over a group $(Q, +) = (Q_1, +_1) \times (Q_2, +_2)$, where $x_i = (x'_i, x''_i)$, $\alpha_i = (\beta_i, \gamma_i)$ for all $i \in \overline{1, n}$, $a = (b, c)$.*

If $(Q, f) = (Q_1, f_1) \times (Q_2, f_2)$ and T_1 is an isotopy of the quasigroup (Q_1, f_1), T_2 an isotopy of the quasigroup (Q_2, f_2), then $T = (T_1, T_2)$ is an isotopy of the quasigroup (Q, f) and vice versa.

Proposition 1. *Let (Q, f) be an n-ary medial quasigroup such that $(Q, f) = (Q_1, f_1) \times (Q_2, f_2)$ and the form of quasigroups (Q, f), (Q_1, f_1), (Q_2, f_2) are defined over groups $(Q, +)$, $(Q_1, +_1)$, $(Q_2, +_2)$ respectively. Then*

$$(Q, +) \cong (Q_1, +_1) \times (Q_2, +_2).$$

Proof. If (Q, f) is a medial n-ary quasigroup and $(Q, f) \cong (Q_1, f_1) \times (Q_2, f_2)$, then (Q_1, f_1) and (Q_2, f_2) are medial quasigroups too. Thus from Belousov theorem (Theorem 2) it follows (see Remarks 1 and 5) that there exist derivative n-groups $(Q, \overset{n}{+})$, $(Q_1, \overset{n}{+_1})$, $(Q_2, \overset{n}{+_2})$ of abelian groups $(Q, +)$, $(Q_1, +_1)$, $(Q_2, +_2)$ respectively, isotopies T, T_1 and T_2 such that $(Q, f) = (Q, \overset{n}{+})T$, $(Q_1, f_1) = (Q_1, \overset{n}{+_1})T_1$, $(Q_2, f_2) = (Q_2, \overset{n}{+_2})T_2$ and

$$(Q, \overset{n}{+})T = (Q_1, \overset{n}{+_1})T_1 \times (Q_2, \overset{n}{+_2})T_2.$$

Taking into consideration properties of direct products of universal algebras ([27, 15]), we conclude that from the last relation it follows $(Q, \overset{n}{+}) = (Q_1, \overset{n}{+_1}) \times (Q_2, \overset{n}{+_2})$ and $T = (T_1, T_2)$.

If $(Q, \overset{n}{+}) = (Q_1, \overset{n}{+_1}) \times (Q_2, \overset{n}{+_2})$, then $(Q, +) = (Q_1, +_1) \times (Q_2, +_2)$. Indeed, if $x_1 + x_2 + \cdots + x_n = (x'_1 +_1 x'_2 +_1 \cdots +_1 x'_n) \times (x''_1 +_2 x''_2 +_2 \cdots +_2 x''_n)$ for all $x_1^n \in Q$, $(x')_1^n \in Q_1$, $(x'')_1^n \in Q_2$, then in the case when $x_3 = x_4 = \cdots = x_n = 0$, $x'_3 = x'_4 = \cdots = x'_n = 0'$, $x''_3 = x''_4 = \cdots = x''_n = 0''$ we obtain $x_1 + x_2 = (x'_1 +_1 x'_2) \times (x''_1 +_2 x''_2)$, i.e. $(Q, +) = (Q_1, +_1) \times (Q_2, +_2)$. □

Remark 9. It is necessary to notice that an analog of Proposition 1 is true for a direct product of n-ary linear quasigroups.

Unfortunately, in general case, decomposition of a quasigroup that is a direct product of two (or more) quasigroups, cannot be carry out in an unique way.

Lemma 9. *If $\gamma_1 x_1 + \gamma_2 x_2 + \cdots + \gamma_n x_n + g$ is a form of n-T-quasigroup (Q, A) over a finite abelian group $(Q, +)$, then every congruence on (Q, A) is a congruence on $(Q, +)$.*

Proof. We repeat the proof of Proposition 5 from [58] since Lemma 9 is direct corollary of this proposition. We have

$$a \Theta b \Leftrightarrow A(\gamma_1^{-1}(a), \overset{n-2}{0}, \gamma_n^{-1}(-g)) \Theta A(\gamma_1^{-1}(b), \overset{n-2}{0}, \gamma_n^{-1}(-g)) \Leftrightarrow \gamma_1^{-1}(a) \Theta \gamma_1^{-1}(b).$$

Therefore

$$A(\gamma_1^{-1}(a), \gamma_2^{-1}(c), \overset{n-3}{0}, \gamma_n^{-1}(-g))\Theta A(\gamma_1^{-1}(b), \gamma_2^{-1}(c), \overset{n-3}{0}, \gamma_n^{-1}(-g)),$$

or $(a+c)\Theta(b+c)$, i.e. Θ is a congruence on the abelian group $(Q,+)$. We notice that the first equivalence is true since any congruence Θ of an n-ary quasigroup (Q,A) is admissible relatively any element from the group $MT(Q,A)$. □

Remark 10. Results similar to Lemma 9 there are and in [37].

Proposition 2. *If a map $\xi : Q \longrightarrow Q_1$ is a homomorphism of a finite n-ary medial quasigroup (Q,f) with the form $f(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + a$ over an abelian group $(Q,+)$ into a finite medial n-ary quasigroup (Q_1, f_1), then there exist an abelian group $(Q_1, +_1)$ such that $\xi(Q,+) = (Q_1, +_1)$ and the quasigroup (Q_1, f_1) has the form $f_1(x_1', \ldots, x_n') = \beta_1 x_1' +_1 \beta_2 x_2' +_1 \cdots +_1 \beta x_n' +_1 b$, where $\xi a = b$, $\xi\alpha_i = \beta_i \xi$, $x_i' \in Q_1$ for all $i \in \overline{1,n}$.*

Proof. It is known that using the homomorphism ξ it is possible to define a congruence θ on the set Q in the following way: $a\theta b$ if and only if $\xi a = \xi b$. Since the quasigroup (Q,f) is finite, from Lemma 9 it follows that the congruence θ of a quasigroup (Q,f) is a congruence of the group $(Q,+)$.

Using the congruence θ of the group $(Q,+)$ we can define a binary operation on the set Q_1 in such manner: if $x' = \xi x$, $y' = \xi y$, then $x' +_1 y' = \xi(x+y)$ for all $x, y \in Q$. It is a standard check that $(Q, +_1)$ is a finite abelian group.

Since ξ is a homomorphism of the group $(Q,+)$, then we obtain

$$\begin{aligned}\xi(f(x_1^n)) &= \xi(\alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + a) \\ &= \xi(\alpha_1 x_1) +_1 \xi(\alpha_2 x_2) +_1 \cdots +_1 \xi(\alpha_n x_n) +_1 \xi a.\end{aligned}$$

Therefore the quasigroup (Q_1, f_1) has a linear form over the group $(Q_1, +_1)$, i.e. it is an isotope of the group $(Q_1, \overset{n}{+_1})$.

The quasigroup (Q_1, f_1) is a finite medial n-ary quasigroup as a homomorphic image of a finite medial n-ary quasigroup. Then by the Belousov's theorem, the quasigroup (Q_1, f_1) over the group $(Q_1, +_1)$ has the form $f_1(x_1^n) = \beta_1 x_1 +_1 \beta_2 x_2 +_1 \cdots +_1 \beta_n x_n +_1 b$, where $\beta_i \in Aut(Q, +_1)$, $\beta_i \beta_j = \beta_j \beta_i$, $x_i \in Q_1$ for all $i, j \in \overline{1,n}$.

Since the map ξ is a homomorphism of the quasigroup (Q,f) into the quasigroup (Q_1, f_1), then we have $\xi f(x_1^n) = f_1(\xi x_1, \xi x_2, \ldots, \xi x_n)$, i.e. $\xi f(x_1^n) = \beta_1 \xi x_1 +_1 \beta_2 \xi x_2 +_1 \cdots +_1 \beta \xi x_n +_1 b$.

Comparing the right sides of the last equalities, we obtain

$$\xi(\alpha_1 x_1) +_1 \cdots +_1 \xi(\alpha_n x_n) +_1 \xi a = \beta_1 \xi x_1 +_1 \cdots +_1 \beta \xi x_n +_1 b. \qquad (16)$$

We notice that $\xi 0 = 0_1$, because ξ is a homomorphism of the group $(Q, +)$ into the group $(Q_1, +_1)$ and $\xi x = \xi x +_1 0_1 = \xi(x + 0) = \xi x +_1 \xi 0$.

If we put $x_1 = x_2 = \cdots = x_n = 0$ in (16), where 0 is the identity element of the group $(Q, +)$, then $\xi a = b$. Thus from (16) we get

$$\xi\alpha_1 x_1 +_1 \xi\alpha_2 x_2 +_1 \cdots +_1 \xi\alpha_n x_n = \beta_1 \xi x_1 +_1 \beta_2 \xi x_2 +_1 \cdots +_1 \beta \xi x_n. \qquad (17)$$

Putting $x_2 = x_3 = \cdots = x_n = 0$ in 17, we obtain $\xi\alpha_1 x = \beta_1 \xi x$ for all $x \in Q$.

For other values of i the equality $\xi\alpha_i = \beta_i \xi$ is proved similarly. □

Remark 11. Proposition 2 is an n-ary analog of Lemma 28 from [35] and it is very near to Proposition 9 from [58].

Corollary 3. *If (Q, f) is an n-ary finite medial quasigroup with the form $f(x_1^n) = \alpha_1 x_1 + \alpha_2 x_2 + \cdots + \alpha_n x_n + a$, $(Q, f) \cong (Q_1, f_1) \times (Q_2, f_2)$, homomorphisms ξ and χ are such that $\xi : \xi(Q, f) = (Q_1, f_1)$ and $\chi : \chi(Q, f) = (Q_2, f_2)$, then there exist abelian groups $(Q_1, +_1)$ and $(Q_2, +_2)$ such that $(Q, +) \cong (Q_1, +_1) \times (Q_2, +_2)$ and*

$$f_1(x')_1^n = \beta_1 x'_1 +_1 \beta_2 x'_2 +_1 \cdots +_1 \beta_n x'_n +_1 \xi(a),$$
$$f_2(x'')_1^n = \gamma_1 x''_1 +_2 \gamma_2 x''_2 +_2 \cdots +_2 \gamma_n x''_n +_2 \chi(a),$$

where $\beta_i \in Aut(Q_1, +_1)$, $\beta_i\beta_j = \beta_j\beta_i$, $\gamma_i \in Aut(Q_2, +_2)$, $\gamma_i\gamma_j = \gamma_j\gamma_i$, $x'_i \in Q_1$ and $x''_i \in Q_2$ for all $i, j \in \overline{1, n}$.

Proof. We can use Propositions 2 and 1. □

4. n-ary analog of Murdoch theorems

For an n-ary quasigroup (Q, f) we define the map $s_f : Q \to Q$ putting $s_f(x) = f(x, x, \ldots, x)$. Below often by using the map s_f we shall omit denotation of an n-ary operation and shall write s instead of s_f. According to Dörnte [16] the element $f(x, x, \ldots, x)$ will be denoted as $f(\overset{(n)}{x})$.

Lemma 10. *In a medial n-ary quasigroup this map is an endomorphism.*

Proof. We have $s(f(x_1^n)) = f(\overset{(n)}{f}(x_1^n))$. Using the medial identity (see (5)) we obtain

$$f(\overset{(n)}{f}(x_1), \overset{(n)}{f}(x_2), \ldots, \overset{(n)}{f}(x_n)) = f(s(x_1), s(x_2), \ldots, s(x_n)),$$

which completes the proof. □

Remark 12. For a binary medial quasigroup $(Q, \cdot)$ we have: $s(x) = x \cdot x$. Then $s(x \cdot y) = (x \cdot y) \cdot (x \cdot y) = (x \cdot x) \cdot (y \cdot y) = s(x) \cdot s(y)$.

Lemma 11. *If an n-ary medial quasigroup (Q, f) has a finite order, then there exists natural number m such that the map $s|_{s^m(Q)}$ is an automorphism of the quasigroup $s^m(Q, f)$.*

Proof. By $s^j(Q)$ we denote the endomorphic image of the quasigroup (Q, f) relative to the endomorphism s^j.

Then, since a medial n-ary quasigroup (Q, f) has a finite order, there exists a number m such that the following chain

$$Q = s^0(Q) \supset s^1(Q) \supset s^2(Q) \supset \cdots \supset s^{m-1}(Q) \supset s^m(Q)$$

becomes stable, i.e. $s^m(Q) = s^{m+1}(Q) = s^{m+2}(Q)$ and so on. □

In this case we shall say that the endomorphism s has order m.

We denote the set $\{\tau \in Aut(Q, f) \,|\, \tau\alpha = \alpha\tau\}$, where (Q, f) is an n-ary quasigroup, α is a permutation of the set Q, by $C_{Aut(Q,f)}(\alpha)$. As it is well known, the set $C_{Aut(Q,f)}(\alpha)$ forms a group with respect to the usual multiplication of permutations [34].

To prove the next lemma we shall use the following theorem from [39].

Theorem 5. *If $(Q, f) = (Q, g)T_0$ is an isotope of an n-ary idempotent quasigroup (Q, g) such that T_0 has the form $(\varepsilon, \ldots, \varepsilon, \beta_{i+1}, \varepsilon, \ldots, \varepsilon)$ (there are $(n+1)$ members in this sequence) and $i \in \overline{0, n}$, then $Aut(Q, f) = C_{Aut(Q,g)}(\beta_{i+1})$.*

Lemma 12. *Let (H, f) be an n-ary medial quasigroup and the map s_f be a bijection on H. Then an n-ary quasigroup (H, g), where $g(x_1^n) = s_f^{-1}(f(x_1^n))$ is a medial idempotent n-ary quasigroup and $s_f \in Aut(H, g)$.*

Proof. It is obviously that $s_f \in Aut(H, f)$. Let us prove that the quasigroup (H, f) is an isotope of a medial idempotent n-ary quasigroup (H, g).

At first check that the n-ary quasigroup (H, g) is idempotent:

$$s_g(x) = g(\overset{(n)}{x}) = s_f^{-1}(f(\overset{(n)}{x})) = s_f^{-1}(s_f(x)) = x.$$

We prove that the quasigroup (H, g) is a medial quasigroup. We note that by Lemma 11 the map $s^{-1} = s_f^{-1}$ is an automorphism of the quasigroup (H, f). We have

$$\begin{aligned}
&g(g(x_{11}, x_{12}, \dots, x_{1n}), \dots, g(x_{n1}, x_{n2}, \dots, x_{nn}))\\
&= s^{-1}f(s^{-1}f(x_{11}, x_{12}, \dots, x_{1n}), \dots, s^{-1}f(x_{n1}, x_{n2}, \dots, x_{nn}))\\
&= s^{-1}f(f(s^{-1}x_{11}, s^{-1}x_{12}, \dots, s^{-1}x_{1n}), \dots, f(s^{-1}x_{n1}, s^{-1}x_{n2}, \dots, s^{-1}x_{nn}))\\
&= s^{-1}f(f(s^{-1}x_{11}, s^{-1}x_{21}, \dots, s^{-1}x_{n1}), \dots, f(s^{-1}x_{1n}, s^{-1}x_{2n}, \dots, s^{-1}x_{nn}))\\
&= s^{-1}f(s^{-1}f(x_{11}, x_{21}, \dots, x_{n1}), \dots, s^{-1}f(x_{1n}, x_{2n}, \dots, x_{nn}))\\
&= g(g(x_{11}, x_{21}, \dots, x_{n1}), \dots, g(x_{1n}, x_{2n}, \dots, x_{nn})).
\end{aligned}$$

From Theorem 5 it follows that $Aut(H, f) \cong C_{Aut(H,g)}(s_f)$. Therefore $Aut(H, f) \subseteq Aut(H, g)$ and $s_f \in Aut(H, g)$ since $s_f \in Aut(H, f)$. □

We recall that an n-ary quasigroup (Q, f) is called *unipotent* if there exists an element $e \in Q$ such that $f(\overset{(n)}{x}) = e$ for all $x \in Q$.

Theorem 6. *Let (Q, f) be an n-ary finite medial quasigroup. Then (Q, f) is either an isotope of a special form of an idempotent medial quasigroup, or (Q, f) is a quasigroup with unique idempotent element, or $(Q, f) \cong (A, f_1) \times (B, f_2)$, where (A, f_1) is a medial n-ary quasigroup with exactly one idempotent element and (B, f_2) is an isotope of an n-ary medial idempotent quasigroup.*

Proof. If the map s_f is a permutation of the set Q, then by Lemma 12 (Q, f) is an isotope of a special form of an idempotent medial quasigroup.

If $s_f^m(Q) = a$, where a is a fixed element of the set Q, then the quasigroup (Q, f) is a quasigroup with a unique idempotent element a.

Let us to suppose that $|s^m(Q)| = |s^{m+1}(Q)|$, where $m \geqslant 1$.

We define a binary relation δ on the n-ary quasigroup (Q, f) putting: $x\delta y$ if and only if $s^m(x) = s^m(y)$, where $s(x) = f(\overset{(n)}{x})$ for any element $x \in Q$, m is the order of the endomorphism s.

From Lemma 7 it follows that $s^m(Q,f) = (H,f)$ is a normal n-ary subquasigroup of the n-ary quasigroup (Q,f).

We define the binary relation ρ on the n-ary quasigroup (Q,f) putting: $x\rho y$ if and only if there exist elements $h_2, h_3, \ldots, h_{n-1}$ of the n-ary subquasigroup (H,f) such that

$$f(x, h_2^{n-1}, H) = f(y, h_2^{n-1}, H),$$

where $f(x, h_2^{n-1}, H) = \{f(x, h_2^{n-1}, h') \,|\, h' \in H\}$.

It is easy to check that so defined binary relations δ and ρ are equivalence relations.

To prove that these equivalence relations δ and ρ are normal congruences it is sufficient to check that these relations are congruences because in n-ary finite quasigroup (Q,f) all congruences are normal (Lemma 7).

To prove that equivalence relation δ is a congruence we must show that the following implication is true: $x_i \delta y_i$ for all $i \in \overline{1,n} \Rightarrow f(x_1^n)\delta f(y_1^n)$. Using the definition of the binary relation δ we re-write this implication in the following equivalent form: $s^m(x_i) = s^m(y_i)$ for all $i \in \overline{1,n} \Longrightarrow s^m(f(x_1^n)) = s^m(f(y_1^n))$. Since map s^m is an endomorphism of the quasigroup (Q,f) (Lemma 10) further we have

$$\begin{aligned} &s^m(x_i) = s^m(y_i) \ \text{ for all } \ i \in \overline{1,n} \Longrightarrow \\ &f(s^m(x_1), s^m(x_2), \ldots, s^m(x_n)) = f(s^m(y_1), s^m(y_2), \ldots, s^m(y_n)). \end{aligned}$$

The last implication is true. Therefore equivalence relation δ is a normal congruence of the quasigroup (Q,f).

We prove that binary relation ρ is a normal congruence, i.e. that the following implication is true: $x_i \rho y_i$ for all $i \in \overline{1,n} \Longrightarrow f(x_1^n)\rho f(y_1^n)$.

Using the definition of the relation ρ we can re-write the last implication in the following equivalent form: if

$$\begin{aligned} &f(x_1, h_{1,2}, h_{1,3}, \ldots, h_{1,n-1}, H) = f(y_1, h_{1,2}, h_{1,3}, \ldots, h_{1,n-1}, H), \\ &f(x_2, h_{2,2}, h_{2,3}, \ldots, h_{2,n-1}, H) = f(y_2, h_{2,2}, h_{2,3}, \ldots, h_{2,n-1}, H), \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &f(x_n, h_{n,2}, h_{n,3}, \ldots, h_{n,n-1}, H) = f(y_n, h_{n,2}, h_{n,3}, \ldots, h_{n,n-1}, H), \end{aligned} \tag{14}$$

then there exist $h'_2, h'_3, \ldots, h'_{n-1} \in H$ such that the following equality is true

$$f(f(x_1^n), h'_2, h'_3, \ldots, h'_{n-1}, H) = f(f(y_1^n), h'_2, h'_3, \ldots, h'_{n-1}, H).$$

If we apply to both sides of equalities (14) the operation f, then we obtain the following equality

$$f(f(x_1, h_{1,2}, h_{1,3}, \dots, h_{1,n-1}, H), f(x_2, h_{2,2}, h_{2,3}, \dots, h_{2,n-1}, H), \dots, f(x_n, h_{n,2}, h_{n,3}, \dots, h_{n,n-1}, H))$$
$$= f(f(y_1, h_{1,2}, h_{1,3}, \dots, h_{1,n-1}, H), f(y_2, h_{2,2}, h_{2,3}, \dots, h_{2,n-1}, H), \dots, f(y_n, h_{n,2}, h_{n,3}, \dots, h_{n,n-1}, H)).$$

Using medial identity we can re-write the last equality in the form

$$f(f(x_1^n), f(h_{1,2}, h_{2,2}, \dots, h_{n,2}), \dots, f(h_{1,n-1}, h_{2,n-1}, \dots, h_{n,n-1}), f(\overset{(n)}{H}))$$
$$= f(f(y_1^n), f(h_{1,2}, h_{2,2}, \dots, h_{n,2}), \dots, f(h_{1,n-1}, h_{2,n-1}, \dots, h_{n,n-1}), f(\overset{(n)}{H})).$$

Since (H, f) is a subquasigroup of the quasigroup (Q, f), we have $f(h_{1,2}, h_{2,2}, \dots, h_{n,2}), \dots, f(h_{1,n-1}, h_{2,n-1}, \dots, h_{n,n-1}) \in H$, $f(\overset{(n)}{H}) = H$. Then from the above equality we obtain

$$f(f(x_1^n), h_2', h_3', \dots, h_{n-1}', H) = f(f(y_1^n), h_2', h_3', \dots, h_{n-1}', H),$$

where $h_2' = f(h_{1,2}, h_{2,2}, \dots, h_{n,2})$, $h_3' = f(h_{1,3}, h_{2,3}, \dots, h_{n,3}), \dots, h_{n-1}' = f(h_{1,n-1}, h_{2,n-1}, \dots, h_{n,n-1})$. Therefore the binary relation ρ is a normal congruence.

We prove that $\delta \cap \rho = \hat{Q} = \{(x, x) | \forall x \in Q\}$. From reflexivity of relations δ, ρ it follows that $\delta \cap \rho \supseteq \hat{Q}$.

Let $(x, y) \in \delta \cap \rho$, i.e. let $x \delta y$ and $x \rho y$, where $x, y \in Q$. Using the definitions of relations δ, ρ we have $s^m(x) = s^m(y)$ and there exist elements $h_2^{n-1} \in H$ such that $f(x, h_2^{n-1}, H) = f(y, h_2^{n-1}, H)$. Then there exist elements $h', h'' \in H$ such that $f(x, h_2^{n-1}, h') = f(y, h_2^{n-1}, h'')$. Thus we have

$$s^m f(x, h_2^{n-1}, h') = s^m f(y, h_2^{n-1}, h''),$$
$$f(s^m(x), s^m(h_2^{n-1}), s^m(h')) = f(s^m(y), s^m(h_2^{n-1}), s^m(h'')).$$

Since in the last equality all elements are in a subquasigroup (H, f), we can conclude that $s^m(h') = s^m(h'')$. Therefore $h' = h''$ since $s|_H$ is a permutation of the set H. Then $f(x, h_2^{n-1}, h') = f(y, h_2^{n-1}, h')$ and we obtain $x = y$. Therefore $\delta \cap \rho \subseteq \hat{Q}$, and, finally, $\delta \cap \rho = \hat{Q}$.

To prove that $\delta \vee \rho = Q \times Q$, let a, b be any fixed elements of the set Q. We prove this equality if it will be shown that there exists element $y \in Q$ such that $a \delta y$ and $y \rho b$.

From the definition of the congruence δ it follows that the condition $a\delta y$ is equivalent to the equality $s^m(a) = s^m(y)$.

From the definition of the congruence ρ it follows that the condition $y\rho b$ is equivalent to the following conditions: there exists elements $c \in Q$, $h_2^{n-1}, h', h'' \in H$ such that $y = f(c, h_2^{n-1}, h')$ and $b = f(c, h_2^{n-1}, h'')$.

Then in our new denotations the condition "there exists an element $y \in Q$ such that $a\delta y$ and $y\rho b$" takes the following equivalent form "there exists an element $h' \in H$ such that $s^m(a) = s^m f(c, h_2^{n-1}, h')$ and $b = f(c, h_2^{n-1}, h'')$, where $c \in Q$ and $h_2^{n-1}, h'' \in H$."

Passing to images of endomorphism s^m further we have

$$s^m(a) = f(s^m(c), s^m(h_2^{n-1}), s^m(h')).$$

In the last equality we have that all elements possibly with the exception of the last element there are in the set H. Since (H, f) is a subquasigroup, $s^m(h') \in H$. But the map $s\mid_H$ is a permutation of the set H and we obtain that $h' \in H$ too.

Then there exists an element h' such that $y = f(c, h_2^{n-1}, h')$, i.e. such that $a\delta y$ and $y\rho b$ for any pair $(a, b) \in Q \times Q$. Thus $(a, b) \in \delta \vee \rho$ for any pair $(a, b) \in Q \times Q$, i.e. $Q \times Q \subseteq \delta \vee \rho$. Therefore $\delta \vee \rho = Q \times Q$.

Taking into consideration Theorem 3 now we can say that the n-ary quasigroup (Q, f) is isomorphic to a direct product of quasigroups (H, f) and $(Q, f)/(H, f)$.

It is easy to see that the medial identity holds in quasigroups (H, f) and $(Q, f)/(H, f)$. The quasigroup (H, f) is medial as an endomorphic image of a medial quasigroup (Q, f). It is possible to check that the quasigroup $(Q, f)/(H, f)$ is a medial quasigroup too.

Any element of the quasigroup $(Q, f)/(H, f)$ we can be presented as a^ρ. Let $x_{11}^\rho, \ldots, x_{nn}^\rho \in (Q, f)/(H, f)$. The medial identity in the quasigroup $(Q, f)/(H, f)$ takes the form

$$\begin{aligned} f(f(x_{11}^\rho, \ldots, x_{1n}^\rho), \ldots, f(x_{n1}^\rho, \ldots, x_{nn}^\rho)) = \\ f(f(x_{11}^\rho, \ldots, x_{n1}^\rho), \ldots, f(x_{1n}^\rho, \ldots, x_{nn}^\rho)). \end{aligned}$$

If we suppose that there exist elements $b_{11}^\rho, \ldots, b_{nn}^\rho \in (Q, f)/(H, f)$ such that the medial identity is not true for these elements, then the medial identity will not be true for some elements of the quasigroup (Q, f). We receive a contradiction that shows that our supposition was not true, and, really, the medial identity holds in the quasigroup $(Q, f)/(H, f)$.

By Lemma 12 the quasigroup (H, f) is an isotope of a medial idempotent n-ary quasigroup (H, g), where $g(x_1^n) = s_f^{-1}(f(x_1^n))$.

Prove that the quasigroup $s^j(Q, f)/s^{j+1}(Q, f)$ is an unipotent quasigroup for all suitable values j.

Denote the quasigroup $s^{j+1}(Q, f)$ by K. Any element of the quasigroup $s^j(Q, f)/s^{j+1}(Q, f)$ we can write in the form: $f(a, h_2^{n-2}, K)$, where $a \in s^j(Q, f), h_2^{n-2} \in K$. Further we have $s(f(a, h_2^{n-2}, K)) = f(s(a), s(h_2^{n-2}), s(K)) \subseteq K$ since $s(a) \in K$. Therefore we obtain that the quasigroup $s^j(Q, f)/s^{j+1}(Q, f)$ is an unipotent quasigroup for all suitable values of j.

Prove that the quasigroup $(A, f) \cong (Q, f)/(H, f)$, where $s^m(Q, f) = (H, f)$, is an n-ary medial quasigroup with exactly one idempotent element over an abelian group $(A, +)$.

From the properties of quasigroup (A, f) it follows that $s^m(A) = a$, where the element a is a fixed element of the set A that corresponds to the coset H. Further, taking into consideration the properties of an endomorphism s of the quasigroup (A, f), we have $s^{m+1}A = s(s^m A) = s(a) = a$. Therefore $s(a) = a$, i.e. the element a is an idempotent element of an n-ary quasigroup (A, f).

Prove that there exists exactly one idempotent element in the quasigroup (A, f). Suppose that there is an element b of the quasigroup (A, f) such that $f(b^n) = b$, i.e. that $s(b) = b$. Then we have $s^m(b) = b = a$. □

An isotopy of the form $(\varepsilon, \varepsilon, \ldots, \varepsilon, \gamma)$ is called a *principal isotopy* [5]. A quasigroup (Q, f) is called an *unipotently-solvable quasigroup of degree* m, if there exists the following finite chain of unipotent quasigroups: $Q/s(Q), s(Q)/s^2(Q), \ldots, s^m(Q)/s^{m+1}(Q)$, where $|s^m(Q)/s^{m+1}(Q)| = 1$. Using the last definitions we can re-formulate Theorem 6 in the following form.

Corollary 4. *Any finite medial n-ary quasigroup is isomorphic to the direct product of a medial unipotently-solvable quasigroup and a principal isotope of a medial idempotent quasigroup (Q, f), where $\gamma \in Aut(Q, f)$.*

5. Automorphisms of n-ary medial quasigroups

In this section we apply the n-ary analog of Murdoch theorem to obtain information about structure of the automorphism group of any finite n-ary medial quasigroup.

Automorphisms and automorphism groups of some binary and n-ary quasigroups were studied in many articles, see, for example, [19, 30, 32, 33, 36, 37, 42, 49, 50, 51, 52, 56].

We shall use information about the structure of the automorphism group of an n-ary medial quasigroup that has at least one idempotent element [39].

Theorem 7. *If an n-T-quasigroup (Q, g) with the form $g(x_1^n) = \sum_{i=1}^{n} \varphi_i x_i + a$ has at least one idempotent element and $K = \{L_b^+ \mid b \in Q,\ \sum_{i=1}^{n} \varphi_i b = b\}$, then*

$$Aut(Q, g) \cong K \leftthreetimes C,$$

where $C = \{\omega \in Aut(Q, +) \mid\ \omega\varphi_i = \varphi_i\omega\ \ \forall i \in \overline{1, n}\}$.

Corollary 5. *If an n-T-quasigroup (Q, g) with the form $g(x_1^n) = \sum_{i=1}^{n} \varphi_i x_i$ has exactly one idempotent element, then*

$$Aut(Q, g) \cong C,$$

where $C = \{\omega \in Aut(Q, +) \mid \omega\varphi_i = \varphi_i\omega \forall\ \ i \in \overline{1, n}\}$.

Corollary 6. *If an n-T-quasigroup (Q, g) is an idempotent quasigroup with the form $g(x_1^n) = \sum_{i=1}^{n} \varphi_i x_i$ over an abelian group $(Q, +)$, then*

$$Aut(Q, g) \cong (Q, +) \leftthreetimes C,$$

where $C = \{\omega \in Aut(Q, +) \mid \omega\varphi_i = \varphi_i\omega\ \ \forall i \in \overline{1, n}\}$.

Corollary 7. *If an n-ary quasigroup (Q, f) is an isotope of an n-ary idempotent T-quasigroup (Q, g), $g(x_1^n) = \sum_{i=1}^{n} \alpha_i x_i$, and the isotopy has the form $(\varepsilon, \ldots, \varepsilon, \beta_{i+1}, \varepsilon, \ldots, \varepsilon)$, $i \in \overline{0, n}$, $\beta_{i+1} = L_d^+$, then*

$$Aut(Q, f) \cong (Q, +) \leftthreetimes S,$$

where $S = \{\theta \in C \mid \theta d = d\}$, $C = \{\omega \in Aut(Q, +) \mid \omega\alpha_i = \alpha_i\omega\ \ \forall i \in \overline{1, n}\}$.

Corollary 8. *If $(Q, f) = (Q, g)T_0$ is an isotope of an n-ary idempotent T-quasigroup (Q, g) such that T_0 has the form $(\varepsilon, \ldots, \varepsilon, \beta_{i+1}, \varepsilon, \ldots, \varepsilon)$, $i \in \overline{0, n}$ and $\beta_{i+1} = \varphi \in Aut(Q, +)$, then*

$$Aut(Q, f) \cong B \leftthreetimes N$$

where $B = \{L_b^+ \mid b \in Q, \varphi b = b\}$, $N = \{\sigma \in C \mid \sigma\varphi = \varphi\sigma\}$.

Remark 13. It is easy to see that there exist four classes of n-ary medial quasigroups over the group Z_2, namely:

1) a $(2k+1)$-ary quasigroup (Z_2, f_1) of the form $f_1(x_1^{2k+1}) = \sum\limits_{i=1}^{2k+1} x_i$,

2) a $(2k)$-ary quasigroup (Z_2, f_2) of the form $f_2(x_1^{2k}) = \sum\limits_{i=1}^{2k} x_i$,

3) a $(2k+1)$-ary quasigroup (Z_2, f_3) of the form $f_3(x_1^{2k+1}) = \sum\limits_{i=1}^{2k+1} x_i + 1$,

4) a $(2k)$-ary quasigroup (Z_2, f_4) of the form $f_4(x_1^{2k}) = \sum\limits_{i=1}^{2k} x_i + 1$.

Lemma 13. *For indicated cases we have:*

1) $s_{f_1} = \varepsilon$, $Aut(Z_2, f_1) \cong Z_2$,
2) $s_{f_2}0 = 0, s_{f_2}1 = 0$, $Aut(Z_2, f_2) \cong \varepsilon$,
3) $s_{f_3} = (01)$, $Aut(Z_2, f_3) \cong Z_2$,
4) $s_{f_4}0 = 1, s_{f_4}1 = 1$, $Aut(Z_2, f_4) \cong \varepsilon$.

Proof. 1). We have $s_{f_1} = \varepsilon$, since $s_{f_1}(0) = 0$, $s_{f_1}(1) = 1$. This quasigroup is a medial ($\alpha_i\alpha_j = \alpha_j\alpha_i$) idempotent ($(2k+1)1 = 1, (2k+1)0 = 0$) $(2k+1)$-ary quasigroup. From Corollary 6 it follows $Aut(Z_2, f_1) \cong Z_2 \leftthreetimes C \cong Z_2$ since $|C| = 1$.

2). We have $s_{f_2}0 = 0, s_{f_2}1 = 0$. This quasigroup is an unipotent quasigroup and by Corollary 5 we obtain $Aut(Z_2, f_2) \cong Aut(Z_2) = \varepsilon$.

3). In this case a map s_{f_3} has the form $s_{f_3} = (01)$, since $s_{f_3}(0) = 1$, $s_{f_3}(1) = 0$, the map s_{f_3} is a permutation of the set Z_2.

This quasigroup is an isotope of an idempotent T-quasigroup. From our Corollary 7 it follows that $Aut(Z_2, f_3) \cong Z_2 \leftthreetimes C \cong S \cong Z_2$ since $S = \{\theta \in C \mid \theta 1 = 1\} = \varepsilon$.

4). We have $s_{f_4}0 = 1, s_{f_4}1 = 1$. This quasigroup is an unipotent quasigroup, from Corollary 5 it follows $Aut(Z_2, f_4) \cong Aut(Z_2) = \varepsilon$. □

Theorem 8. *If (Q, f) is a finite medial n-ary quasigroup of the form $f(x_1^n) = \sum\limits_{i=1}^{n} \alpha_i x_i + a$, $s(x) = f(\overset{(n)}{x})$ for any element $x \in Q$ and m is the smallest natural number such that $s^m Q = s^{m+1} Q$, then*

$$Aut(Q, f) \cong Aut(Q_1, f_1) \times Aut(Q_2, f_2),$$

$(Q_1, f_1) = s^m(Q, f)$, $Aut(Q_1, f_1) \cong C_{Aut(Q_1,g)}(s_{f_1})$, $g(x_1^n) = s_{f_1}^{-1}(f_1(x_1^n))$, $Q_2 \cong Q/Q_1$, $f_2(x_1^n) = \sum_{i=1}^{n}(\overline{\alpha_i}x_i)$, $Aut(Q_2, f_2) \cong C = \{\omega \in Aut(Q_2, +) \mid \omega\overline{\alpha}_i = \overline{\alpha}_i\omega \ \forall\ i \in \overline{1,n}\}$.

Proof. From Theorem 6 it follows that any finite medial n-ary quasigroup (Q, f) it is possible to present as a direct product of two n-ary medial quasigroups, namely $(Q, f) \cong (Q_1, f_1) \times (Q_2, f_2)$, where $Q_1 = s^mQ$, $Q_2 \cong Q/Q_1$, $s(x) = f(\overset{(n)}{x})$ for any element $x \in Q$ and m is the smallest natural number such that $s^mQ = s^{m+1}Q$, the quasigroup (Q, f_1) is an isotope of special form of a medial idempotent quasigroup and the quasigroup (Q, f_2) is a medial quasigroup with exactly one idempotent element.

Therefore we have $Aut(Q, f) \supseteq Aut(Q_1, f_1) \times Aut(Q_2, f_2)$. Now we shall prove that $Aut(Q, f) \subseteq Aut(Q_1, f_1) \times Aut(Q_2, f_2)$, i.e. that $Aut(Q, f) \cong Aut(Q_1, f_1) \times Aut(Q_2, f_2)$.

For $|Q| \geqslant 3$ quasigroups (Q_1, f_1) and (Q_2, f_2) are non-isomorphic since in the quasigroup (Q_1, f_1) the map s_{f_1} is a permutation of the set Q_1 and in the quasigroup (Q_2, f_2) we have $s_{f_2}(x) = e$ for any $x \in Q_2$ and some fixed element e of the set Q_2. Moreover, any pair of subquasigroups (S, f_1) and (S_2, f_2) of quasigroups (Q_1, f_1) and (Q_2, f_2) respectively with $|S_1| \geqslant 2$ or $|S_2| \geqslant 2$ are non-isomorphic too.

Indeed, in any subquasigroup (S_1, f_1) $(|S_1| > 1)$ of the quasigroup (Q_1, f_1) the endomorphism s is a permutation of the set S_1 but in any subquasigroup (S_2, f_2) $(|S_2| > 1)$ of the quasigroup (Q_2, f_2) the endomorphism s is not a permutation of the set S_2.

Therefore in this case there does not exist an automorphism φ of the quasigroup (Q, f) such that φ is an isomorphism of the quasigroups (Q_1, f_1) and (Q_2, f_2) or the automorphism φ is an isomorphism of their subquasigroups, i.e. $\varphi(S_1, f_1) \cong (S_2, f_2)$ where the quasigroup (S_1, f_1) $(|S_1| \geqslant 2)$ is a subquasigroup of the quasigroup (Q_1, f_1) and the quasigroup (S_2, f_2) is a subquasigroup of the quasigroup (Q_2, f_2).

Let $|S_1| = |S_2| = 1$. We have to prove that in this case as well there is not any automorphism φ of a finite medial n-ary quasigroup (Q, f) such that $\varphi S_1 \cong S_2$.

It is clear that $(S_1, f_1) \times (S_2, f_2)$ is an n-ary medial quasigroup of order 2 and in this quasigroup a map s can not be a permutation.

It is well known that up to isomorphism there exists the unique abelian group of order 2, namely, Z_2. In Lemma 13 some properties of all up to

isomorphism possible classes of n-ary medial quasigroups over the group Z_2 are described.

We see that only n-ary medial quasigroups from classes 2) and 4) fulfill our condition that the map s is not a permutation. From Lemma 13 it follows that in cases 2), 4) there exists only the identity automorphism.

Then $\varphi Q_1 = Q_1$ and $\varphi Q_2 = Q_2$ for any automorphism of the quasigroup (Q, f).

Structure of the group $Aut(Q_1, f_1)$ follows from Theorem 7 and structure of the group $Aut(Q_2, f_2)$ follows from Corollary 5. □

Corollary 9. *If (Q, f) is a finite medial n-ary quasigroup and s_{f_1} is an automorphism of $Aut(Q_1, +)$, then*

$$Aut(Q, f) \cong (B \leftthreetimes N) \times C_2,$$

where $B = \{L_b^+ \mid b \in Q_1, s_{f_1}(b) = b\}$, N is a centralizer of the map s_{f_1} in the group $C_1 = C_{Aut(Q_1,+)}(\alpha_1^n)$, $C_2 = \{\omega \in Aut(Q_2, +) \mid \omega\alpha_i = \alpha_i\omega \, \forall \, i \in \overline{1,n}\}$.

Proof. This follows from Theorem 8 and Corollary 8. □

Corollary 10. *If (Q, f) is a finite medial n-ary quasigroup and $s_{f_1} = L_d^+$, $d \in Q_1$, then*

$$Aut(Q, f) \cong ((Q_1, +) \leftthreetimes S) \times C_2,$$

where $S = \{\theta \in C_1 \mid \theta d = d\}$, $C_1 = \{\omega \in Aut(Q_1, +) \mid \omega\alpha_i = \alpha_i\omega \, \forall \, i \in \overline{1,n}\}$, $C_2 = \{\omega \in Aut(Q_2, +) \mid \omega\alpha_i = \alpha_i\omega \, \forall \, i \in \overline{1,n}\}$.

Proof. This follows from Theorem 8 and Corollary 7. □

6. Examples

Example 2. The European Article Number code (EAN) is the code with the check equation

$$1 \cdot x_1 + 3 \cdot x_2 + 1 \cdot x_3 + 3 \cdot x_4 + 1 \cdot x_5 + 3 \cdot x_6 + 1 \cdot x_7 + \\ + 3 \cdot x_8 + 1 \cdot x_9 + 3 \cdot x_{10} + 1 \cdot x_{11} + 3 \cdot x_{12} + 1 \cdot x_{13} \equiv 0 \pmod{10},$$

where $x_i \in Z_{10}$, $i \in \overline{1,13}$, elements $x_1, \ldots, x_{12}$ are the information digits and element x_{13} is a check digit [53].

We can associate with this code in the following way 12-ary medial quasigroup (Z_{10}, f). From the last check equation we have

$$-x_{13} \equiv 1 \cdot x_1 + 3 \cdot x_2 + 1 \cdot x_3 + 3 \cdot x_4 + 1 \cdot x_5 + 3 \cdot x_6 + 1 \cdot x_7 + 3 \cdot x_8 + 1 \cdot x_9 + 3 \cdot x_{10} + 1 \cdot x_{11} + 3 \cdot x_{12} \pmod{10},$$

$$x_{13} \equiv 9 \cdot x_1 + 7 \cdot x_2 + 9 \cdot x_3 + 7 \cdot x_4 + 9 \cdot x_5 + 7 \cdot x_6 + 9 \cdot x_7 + 7 \cdot x_8 + 9 \cdot x_9 + 7 \cdot x_{10} + 9 \cdot x_{11} + 7 \cdot x_{12} \pmod{10}.$$

Therefore we obtain the 12-ary medial quasigroup (Z_{10}, f) with the form

$$f(x_1^{12}) \equiv 9 \cdot x_1 + 7 \cdot x_2 + 9 \cdot x_3 + 7 \cdot x_4 + 9 \cdot x_5 + 7 \cdot x_6 + 9 \cdot x_7 + 7 \cdot x_8 + 9 \cdot x_9 + 7 \cdot x_{10} + 9 \cdot x_{11} + 7 \cdot x_{12} \pmod{10}.$$

For this quasigroup we have $s_f(x) = 6 \cdot (9+7)x = 96x = 6x$ for any $x \in Z_{10}$, $s_f(Z_{10}) = \{0, 6, 2, 8, 4\} = A$, $s_f(A) = A$. Therefore $m = 1$ in this case. We notice, in this example the endomorphism s_f of the quasigroup (Z_{10}, f) is also an endomorphism of the group $(Z_{10}, +)$. It is easy to see that $s_f(Z_{10}, +) \cong (Z_5, +)$.

From Theorem 6 it follows that $(Z_{10}, f) \cong (Z_2, f_1) \times (Z_5, f_2)$.

Information from the subsection 3.2 gives us the possibility to find the forms f_1 and f_2, if we define the group $(Z_{10}, +)$ as the direct sum of groups $(Z_2, +)$ and $(Z_5, +)$ and define an isomorphism between these groups.

Let $Z_{10} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, $Z_5 = \{0, 1, 2, 3, 4\}$, $Z_2 = \{0, 1\}$, $Z_2 \oplus Z_5 = \{(0;0), (0;1), (0;2), (0;3), (0;4), (1;0), (1;1), (1;2), (1;3), (1;4)\}$.

Define an isomorphism ξ between the group $(Z_{10}, +)$ and the group $(Z_2 \oplus Z_5, +)$ as follows: $\xi(0) = (0;0)$, $\xi(1) = (1;1)$, $\xi(2) = (0;2)$, $\xi(3) = (1;3)$, $\xi(4) = (0;4)$, $\xi(5) = (1;0)$, $\xi(6) = (0;1)$, $\xi(7) = (1;2)$, $\xi(8) = (0;3)$, $\xi(9) = (1;4)$.

Multiplication of elements of the group $(Z_{10}, +)$ on element 7 or on element 9 is an automorphism of this group. Since $\xi(7) = (1, 2)$, then the following ordered pair of automorphisms: $1 : x \mapsto 1 \cdot x \pmod 2$ and $2 : x \mapsto 2 \cdot x \pmod 5$ corresponds to the automorphism $7 : x \mapsto 7 \cdot x \pmod{10}$.

Similarly, since $\xi(9) = (1;4)$, we have, that the following ordered pair of automorphisms $1 : x \mapsto 1 \cdot x \pmod 2$ and $4 : x \mapsto 4 \cdot x \pmod 5$ corresponds to the automorphism $9x \mapsto 9 \cdot x \pmod{10}$.

Now we can say, that the 12-ary medial quasigroup (Z_{10}, f) with the above form is isomorphic to the 12-ary medial quasigroup $(Z_2, f_1) \times (Z_5, f_2)$, where

$$f_1(x_1^{12}) \equiv 1 \cdot x_1 + 1 \cdot x_2 + 1 \cdot x_3 + 1 \cdot x_4 + 1 \cdot x_5 + 1 \cdot x_6 + 1 \cdot x_7 + 1 \cdot x_8 + 1 \cdot x_9 + 1 \cdot x_{10} + 1 \cdot x_{11} + 1 \cdot x_{12} \pmod 2$$

and

$$f_2(x_1^{12}) \equiv 4 \cdot x_1 + 2 \cdot x_2 + 4 \cdot x_3 + 2 \cdot x_4 + 4 \cdot x_5 + 2 \cdot x_6 + 4 \cdot x_7 + 2 \cdot x_8 + 4 \cdot x_9 + 2 \cdot x_{10} + 4 \cdot x_{11} + 2 \cdot x_{12} \pmod 5.$$

From Theorem 8 it follows that $Aut(Z_{10}, f) \cong Aut(Z_2, f_1) \times Aut(Z_5, f_2)$.

From Lemma 13 (the case 2) it follows that $Aut(Z_2, f_1) = < \varepsilon >$.

Further we have $s_{f_2}(x) = 6 \cdot (4+2)x = 1 \cdot x$ for every $x \in Z_5$. The quasigroup (Z_5, f_2) is a 12-ary medial idempotent quasigroup. We can use Corollary 6 in order to find $Aut(Z_5, f_2)$. Since the group $Aut(Z_5, +)$ is a commutative group and $Aut(Z_5, +) \cong Z_4$, we have $Aut(Z_5, f_2) \cong Z_5 \leftthreetimes Z_4$.

Finally we obtain $Aut(Z_{10}, f) \cong (Z_5 \leftthreetimes Z_4) \times < \varepsilon > \cong Z_5 \leftthreetimes Z_4$.

Remark 14. We could use also Corollary 9 in order to find $Aut(Z_{10}, f)$.

Remark 15. In [39] the automorphism group of the quasigroup (Z_{10}, f) was found without use of Theorem 6, since this quasigroup has an idempotent element (for example, the element 0 is such element) and we have a possibility to use Theorem 7.

Example 3. We find the structure and the automorphism group of the ternary medial quasigroup (Z_{12}, f) over the group $(Z_{12}, +)$ with the form $f(x_1^3) = 1 \cdot x_1 + 7 \cdot x_2 + 1 \cdot x_3 + 7$.

We have: $s(x) = 9 \cdot x + 7$. It is easy to see that this quasigroup does not contain any idempotent element. Indeed, if $9 \cdot x + 7 = x \pmod{12}$, then $8 \cdot x = -7 = 5 \pmod{12}$. It is clear that the last equation does not have a solution and in this case we do not have a possibility to apply directly Theorem 7 or its corollaries.

Further we have $s(Z_{12}) = \{7, 4, 1, 10\} = A$, $s(A) = A$. Therefore $m = 1$. In this case $s(Z_{12}, +) \cong (Z_4, +)$.

As in previous example, first of all we fix an isomorphism ξ between the group $(Z_{12}, +)$ defined on the set $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ and the group $(Z_3 \oplus Z_4, +)$ defined on the set

$$\{(0;0), (0;1), (0;2), (0;3), (1;0), (1;1), (1;2), (1;3), (2;0), (2;1), (2;2), (2;3)\}.$$

Let $\xi(1) = (1, 1)$. Then $\xi(7) = (1; 3)$.

Thus from Theorem 6 it follows that $(Z_{12}, f) \cong (Z_3, f_1) \times (Z_4, f_2)$, where $f_1(x_1^3) = 1 \cdot x_1 + 1 \cdot x_2 + 1 \cdot x_3 + 1$ and $f_1(x_1^3) = 1 \cdot x_1 + 3 \cdot x_2 + 1 \cdot x_3 + 3$ are the forms of quasigroups (Z_3, f_1) and (Z_4, f_2) respectively over groups $(Z_3, +)$ and $(Z_4, +)$.

From Theorem 8 it follows that $Aut(Z_{12}, f) \cong Aut(Z_3, f_1) \times Aut(Z_4, f_2)$. The quasigroup $Aut(Z_3, f_1)$ has exactly one idempotent element (namely,

the element 1 is an idempotent element). By Corollary 5 $Aut(Z_3, f_1) \cong C$. Therefore $Aut(Z_3, f_1) \cong Z_2$.

The quasigroup (Z_4, f_2) is an isotope of the form $(\varepsilon, \varepsilon, L_3^+, \varepsilon)$ of an idempotent 3-ary medial quasigroup (Z_4, g) with the form $g(x_1^3) = 1 \cdot x_1 + 3 \cdot x_2 + 1 \cdot x_3$. Use of Corollary 7 gives us that $Aut(Z_4, f_2) \cong Z_4 \leftthreetimes < \varepsilon > \cong Z_4$ since from two automorphisms of the group $(Z_4, +)$ only the identity automorphism fixes element 3.

Finally we obtain $Aut(Z_{12}, f) \cong Z_2 \times Z_4$.

Acknowledgment. The author thanks Prof. G.B. Belyavskaya, Prof. V.I. Arnautov, Prof. W.A. Dudek, Prof. A.I. Kashu and Referees for their helpful comments.

References

[1] **J. Aczel**: *On mean values*, Bull. Amer. Math. Soc. **54** (1948), 392 – 400.

[2] **G. E. Bates, F. Kiokemeister**: *A note on homomorphic mappings of quasigroups into multiplicative systems*, Bull. Amer. Math. Soc. **54** (1948), 1180 – 1185.

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

[4] **V. D. Belousov**: *A generalized mean value equation*, (Russian), Mat. Issled. **39** (1976), 21 – 31.

[5] **V. D. Belousov**: *n-Ary Quasigroups*, (Russian), Shtiinta, Kishinev, 1972.

[6] **V. D. Belousov**: *Elements of the Quasigroup Theory, A Special Course*, (Russian), Kishinev State Univ. Press, Kishinev, 1981.

[7] **V. D. Belousov, M. D. Sandik**: *n-Ary quasigroups and loops*, (Russian), Siberian Mat. Zh. **7** (1966), 31 – 54.

[8] **V. D. Belousov, Z. Stojaković**: *Generalized entropy on infinitary quasigroups*, Zbornik rad. Prir.-mat. fak. Univ. u Novom Sadu **5** (1975), 35 – 42.

[9] **G. B. Belyavskaya**: *Direct decompositions of quasigroups*, (Russian), Mat. Issled. **95** (1987), 23 – 38.

[10] **G. B. Belyavskaya**: *Full direct decompositions of quasigroups with an idempotent element*, (Russian), Mat. Issled. **113** (1990), 21 – 36.

[11] **G. B. Belyavskaya, V. I. Izbash, V. A. Shcherbacov**: *Check character systems over quasigroups and loops*, Quasigroups and Related Systems **10** (2003), 1 – 28.

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

[13] **J. R. Cho**: *Idempotent medial n-groupoids defined on fields*, Algebra Universalis **25** (1988), 235 – 246.

[14] **J.R. Cho**: *On n-groupoid defined on fields*, Proceedings of "Groups - Korea 1988", Pusan, 1988, 73 – 81.

[15] **P. M. Cohn**: *Universal Algebra*, Harper & Row, New York, 1965.

[16] **W. Dörnte**: *Untersuhungen über einen veralgemeinerten Gruppenbegriff*, Math. Z. **29** (1928), 1 – 19.

[17] **W. A. Dudek**: *Autodistributive n-groups*, Commentationes Math. Annales Soc. Math. Polonae, Prace Matematyczne **23** (1983), 1 – 11.

[18] **W. A. Dudek**: *Medial n-groups and skew elements*, Proceedings of the 5th Symp. "Universal and applied algebra", Turava, Poland, 1988, 55 – 80.

[19] **W. A. Dudek**: *On number of transitive distributive quasigroups*, (Russian), Mat. Issled. **120** (1991), 64 – 76.

[20] **W. A. Dudek**: *On some old and new problems in n-ary groups*, Quasigroups and Related Systems **8** (2001), 15 – 36.

[21] **W. A. Dudek, J. Michalski**: *On a generalization of Hosszú theorem*, Demonstratio Math. **15** (1982), 783 – 805.

[22] **W. A. Dudek, J. Michalski**: *On retracts of polyadic groups*, Demonstratio Math. **17** (1984), 281 – 301.

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

[24] **J. B. Fraleigh**: *A First Course in Abstract Algebra*, Third Edition, Addison-Wesley Publishing Company, London, 1982.

[25] **A. M. Gal'mak, G. N. Vorob'ev**: *Ternary Reflection Groups*, (Russian), Belaruskaya navuka, Minsk, 1998.

[26] **K. Glazek, B. Gleichgewicht**: *Abelian n-groups*, Colloq. Math. Soc. J. Bolyai **29** Universal Algebra, Esztergom (Hungary), 1977, 321 – 329.

[27] **G. Grätzer**: *Universal Algebra*, Springer-Verlag, Berlin, 1979.

[28] **I. N. Herstein**: *Abstract Algebra*, Second Edition, Macmillan Publishing Company, New York, 1990.

[29] **M. Hosszú**: *On the explicit form of n-group operations*, Publ. Math., Debrecen, **10** (1963), 88 – 92.

[30] **V. I. Izbash**: *Isomorphisms of quasigroups isotopic to groups,* Quasigroups and Related Systems **2** (1995), 34 – 50.

[31] **J. Ježek**: *Normal subsets of quasigroups*, Commen. Math. Univ. Carolinae **16** (1975), 77 – 85.

[32] **J. Ježek, T. Kepka**: *Varieties of abelian quasigroups*, Czech. Math. J. **27** (1977), 473 – 503.

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

[34] **M.I. Kargapolov, Yu.I. Merzlyakov**: *Foundations of the Group Theory*, (Russian), Nauka, Moscow, 1977.

[35] **T. Kepka, P. Nemec**: *T-quasigroups, II*, Acta Univ. Carolinae, Math. et Physica **12** (1971), no. 2, 31 – 49.

[36] **O. U. Kirnasovsky**: *The transitive and multitransitive automorphism group of the multiplace quasigroups*, Quasigroups and Related Systems **4** (1997), 23 – 38.

[37] **O. U. Kirnasovsky**: *Binary and n-ary isotopes of groups, Main algebraic notations and quantitative characteristics*, Taras Shevchenko Kiev State University, Synopsis of thesis. Kiev, 2000, 17 pages.

[38] **A.I. Mal'cev**: *On the general theory of algebraic systems*, (Russian), Mat. Sb. **35 (77)** (1954), 3 – 20.

[39] **A. Marini, V. Shcherbacov**: *On autotopies and automorphisms of n-ary linear quasigroups.* Algebra and Discrete Mathematics **2** (2004), 59 – 83.

[40] **G. L. Mullen, V. Shcherbacov**: *Properties of codes with one check symbol from a quasigroup point of view*, Bol. (Izv.) AN Rep. Moldov., Matematica No 3, 2002, 71 – 86.

[41] **G. L. Mullen, V. Shcherbacov**: *n-T-quasigroup codes with one check symbol and their error detection capabilities*, Commen. Math. Univ. Carolinae, **45** (2004), 321 – 340.

[42] **D. C. Murdoch**: *Structure of abelian quasigroups*, Trans. Amer. Math. Soc. **49** (1941), 392 – 409.

[43] **E. Natale**: *n-Quasigruppi mediali idempotenti commutativi*, Rendiconti Acad. Sci. Fis. e Mat. Napoli **46** (1979), 221 – 229.

[44] **P. Nemec, T. Kepka**: *T-quasigroups, I*, Acta Univ. Carolinae, Math. et Physica **12** (1971), 39 – 49.

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

[46] **M. Polonijo**: *Medial multiquasigroups*, Prilozi, Makedonska Akad. Nauk Umet. Odd. Mat-Tekh. Nauki **3** (1982), 31 – 36.

[47] **M. Polonijo**: *Abelian totally symetric n-quasigroups*, Proceedings of the symposium "n-ary structures", Skopje 1982, 185 – 193.

[48] **S. A. Rusakov**: *Algebraic n-ary systems: Sylow theory of n-ary groups*, (Russian), Navuka i tehnika, Minsk, 1992.

[49] **L. V. Safonova, K. K. Shchukin**: *Computation of the automorphisms and anti-automorphisms of quasigroups*, (Russian), Bul. Acad. Sci. R. S. S. Moldov. Matematica No. 3, 1990, 49 – 55.

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

[51] **V. Shcherbacov**: *On linear quasigroups and their automorphism groups*, Mat. Issled. **120** (1991), 104 – 114.

[52] **V. Shcherbacov**: *On automorphism groups of leftdistributive quasigroups*, (Russian), Bol. (Izv.) AN Rep. Moldov. Matematica, No. 2, 1994, 79 – 86.

[53] **R.-H. Schulz**: *Check character systems and anti-symmetric mappings*, Computational Discrete Mathematics, LNCS **2122** (2001), 136 – 147.

[54] **J. D. H. Smith**: *Mal'cev Varieties*, Lecture Notes in Math. **554**, 1976.

[55] **F. N. Sokhatskii**: *About isomorphism of linear quasigroups*, International Algebraic Conference, Barnaul, 1991, Abstracts of Talks, p.138.

[56] **F. Sokhatskyi, P. Syvakivskyi**: *On linear isotopes of cyclic groups*, Quasigroups and Related Systems **1** (1994), 66 – 76.

[57] **E. I. Sokolov**: *On the Gluskin-Hosszú theorem for Dörnte n-groups*, (Russian), Mat. Issled. **39** (1976), 187 – 189.

[58] **P. N. Syrbu**: *On congruences on n-ary T-quasigroups*, Quasigroups and Related Systems **6** (1999), 71 – 80.

[59] **J. Timm**: *Zur gruppentheoretischen Beschreibung n-stelliger Structuren*, Publ. Math., Debrecen **17** (1970), 183 – 192.

[60] **K. Toyoda**: *On axioms of linear functions*, Proc. Imp. Acad. Tokyo **17** (1941), 221 – 227.

Institute of Mathematics and Computer Science
Academy of Sciences of Moldova
str. Academiei 5, MD-2028
Chisinau, Moldova
e-mail: scerb@math.md

Received June, 15, 2004
Revised April 6, 2005