BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 2(81), 2016, Pages 125–142
ISSN 1024–7696

On pseudoisomorphy and distributivity of quasigroups

Fedir M. Sokhatsky

Abstract. A repeated bijection in an isotopism of quasigroups is called a *companion* of the third component. The last is called a *pseudoisomorphism* with the companion. Isotopy coincides with pseudoisomorphy* in the class of inverse property loops and with isomorphy in the class of commutative inverse property loops. This result is a generalization of the corresponding theorem for commutative Moufang loops. A notion of middle distributivity is introduced: a quasigroup is *middle distributive* if all its middle translations are automorphisms. In every quasigroup two identities of distributivity (left, right and middle) imply the third. This fact and some others help us to find a short proof of a theorem which gives necessary and sufficient conditions for a quasigroup to be distributive. There is but a slight difference between this theorem and the well-known Belousov's theorem.

Mathematics subject classification: 20N05.
Keywords and phrases: Quasigroup, distributive quasigroup, Moufang loop, isotopy, pseudoisomorphy.

This article is dedicated to the memory of my dear teacher professor Valentin Danilovich Belousov

Introduction

V. D. Belousov's monograph [1] was published almost 50 years ago and became very popular among mathematicians. It is still a desk book for many algebraists.

The growth of applications of the quasigroup theory in information processing, and expansion of research methods by computer tools and nascence of computer algebra have increased the need to form a coherent quasigroup theory. The author hopes that the proposed article will promote the development of this theory.

Here, a different approach to the proof of Belousov's theorem is suggested. Due to this approach, it became possible to significantly simplify the proof of the theorem and all related statements. The article is self-contained, i. e., it includes all the necessary properties with proofs despite the fact that some of them are well known and can be found in [1], [2]. A historical overview of the results of distributive quasigroups is not discussed here because it has already been done in [4].

In the first part of the paper, some properties of loop isotopy are established and they are applied in the second part. The importance of study of isotopy relation in quasigroup theory is explained by the following fact: each homotopism of

*isotopy, pseudoisomorphy, isomorphy denote relation among groupoids and isotopism, psuedoisomorphism, isomorphism are the corresponding sequence of bijections quasigroups can be represented as a composition of isotopisms from quasigroups to loops and homomorphisms of loops. V. D. Belousov [1] has proposed a programm of development of the quasigroup theory in problems, which are mainly related to the study of isotopy.

Isotopisms with two coinciding components are proposed to be considered. The repeated bijection is called a *companion* of the third component. The third component is called a *pseudoisomorphism*. This notion is a generalization of the notion of pseudoautomorphism, its companions are bijections, but not elements. The following fact shows the importance of the concept: isotopy coincides with pseudoisomorphy for inverse property loops (Corollary 3). It is easy to deduce that isotopy coincides with isomorphy for commutative inverse property loops (Corollary 5). This result is a generalization of the corresponding theorem for commutative Moufang loops [1, Theorem 6.7], [2, Theorem IV.5.6].

Questions about the relations between different types of isotopy arise. For example, when are pseudoisomorphic quasigroups isomorphic? A partial answer is given in Theorem 1: pseudoisomorphic commutative loops with coinciding nuclei are isomorphic. Or what properties are invariant under pseudoisomorphy? Etc.

It is suggested to consider also the middle distributivity identity, defining it in the similar way as the identities of the left and right distributivity: a quasigroup is *middle distributive* if all its middle translations are automorphisms of the quasigroup. It is proved that in every quasigroup two identities of distributivity imply the third (Theorem 9). Therefore, any distributive quasigroup satisfies left, right and middle distributive identities. This fact and some others help us to give a short proof of Theorem 3, which gives necessary and sufficient conditions for a quasigroup to be distributive. There is but a slight difference between this theorem and the well-known Belousov's theorem (Corollary 11).

The theorem implies that every distributive quasigroup is defined over some commutative Moufang loop by an automorphism of the loop which satisfies (16). This identity is equivalent to all identities of distributivity in the loop. Finally, it is proved that any two automorphisms defining distributive quasigroups over the same commutative Moufang loop 1) differ in a central endomorphism of the loop (Corollary 13); 2) define isomorphic distributive quasigroups if and only if they are conjugate by an automorphism of the loop (Corollary 14).

1 Preliminaries

Let Q be an arbitrary set and $(\cdot)$ be an invertible operation defined on Q, then the pair $(Q;\cdot)$ is called a *quasigroup. Invertibility* means that for arbitrary $a, b \in Q$ each of the equations $x \cdot a = b$ and $a \cdot y = b$ is uniquely solvable in Q.

A τ-parastrophe $(Q;\overset{\tau}{\cdot})$ of a quasigroup $(Q;\cdot)$ is defined by

$$x_{1\tau} \overset{\tau}{\cdot} x_{2\tau} = x_{3\tau} :\Leftrightarrow x_1 \cdot x_2 = x_3$$

for every $\tau \in S_3 := \{\iota, \ell, r, s, s\ell, sr\}$, where $s := (12)$, $\ell := (13)$, $r := (23)$. Special notation: $(*) := (\overset{s}{\cdot})$, $(\backslash) := (\overset{r}{\cdot})$, $(/) := (\overset{\ell}{\cdot})$. All parastrophes can be defined by identities. Some of them are the following

$$(x \cdot y)/y = x, \quad (x/y) \cdot y = x, \quad x\backslash(x \cdot y) = y, \quad x \cdot (x\backslash y) = y. \tag{1}$$

A *left* $L_{a,\tau}$, *right* $R_{a,\tau}$ and *middle* $M_{a,\tau}$ translations of the quasigroup $(Q; \overset{\tau}{\cdot})$ are defined by

$$L_{a,\tau}(x) := a \overset{\tau}{\cdot} x, \quad R_{a,\tau}(x) := x \overset{\tau}{\cdot} a, \quad M_{a,\tau}(x) = y :\Leftrightarrow x \overset{\tau}{\cdot} y = a \tag{2}$$

for any $a \in Q$ and $\tau \in S_3$. As usual, the translations $L_{a,\iota}$, $R_{a,\iota}$, $M_{a,\iota}$ are denoted by L_a, R_a, M_a respectively. In general, there are six parastrophes of a quasigroup. The set of all their translations consists of the following six transformations:

$$\begin{aligned} &L_a(x) = a \cdot x = a \overset{\iota}{\cdot} x, \quad &&R_a(x) = x \cdot a = x \overset{\iota}{\cdot} a, \quad &&M_a(x) = x\backslash a = x \overset{r}{\cdot} a, \\ &L_a^{-1}(x) = a\backslash x = a \overset{r}{\cdot} x, \quad &&R_a^{-1}(x) = x/a = x \overset{\ell}{\cdot} a, \quad &&M_a^{-1}(x) = a/x = a \overset{\ell}{\cdot} x. \end{aligned} \tag{3}$$

The relations among translations of parastrophic operations are easily verifiable (see, for example [3]) and can be expressed in the following table:

$\cdot\cdot\cdot\ \tau$	ι	s	ℓ	r	$s\ell$	sr
$L_{a,\tau}$	L_a	R_a	M_a^{-1}	L_a^{-1}	R_a^{-1}	M_a
$R_{a,\tau}$	R_a	L_a	R_a^{-1}	M_a	M_a^{-1}	L_a^{-1}
$M_{a,\tau}$	M_a	M_a^{-1}	L_a^{-1}	R_a	L_a	R_a^{-1}

(4)

A triplet (α, β, γ) of mappings from a set Q_o into a set Q is called a *homotopism* of a groupoid $(Q_o; \circ)$ into a groupoid $(Q; \cdot)$ if

$$\gamma(x \circ y) = \alpha x \cdot \beta y$$

holds for all $x, y \in Q_o$. A homotopism (α, β, γ) is called an *isotopism* if α, β, γ are bijections. If in addition $Q_o = Q$ and $(\cdot) = (\circ)$, then it is an *autotopism* of $(Q; \cdot)$.

A triplet $(Q; \cdot, e)$ is called a *loop* if $(Q; \cdot)$ is a quasigroup and e is its *neutral element*, i.e., $e \cdot x = x \cdot e = x$ holds for all $x \in Q$.

Left, *right* and *middle nuclei* of a loop $(Q; \cdot, e)$ are defined by

$$\begin{aligned} N_\ell^{(\cdot)} &:= \{a \mid ax \cdot y = a \cdot xy\} = \{a \mid (L_a, \iota, L_a) \text{ is an autotopism of } (Q; \cdot, e)\}, \\ N_r^{(\cdot)} &:= \{a \mid x \cdot ya = xy \cdot a\} = \{a \mid (\iota, R_a, R_a) \text{ is an autotopism of } (Q; \cdot, e)\}, \\ N_m^{(\cdot)} &:= \{a \mid xa \cdot y = x \cdot ay\} = \{a \mid (R_a^{-1}, L_a, \iota) \text{ is an autotopism of } (Q; \cdot, e)\}. \end{aligned} \tag{5}$$

An element of a loop is called *central* if it commutes and associates with all elements of the loop. In other words, c is central if

$$c \in N_\ell^{(\cdot)} \cap N_r^{(\cdot)} \cap N_m^{(\cdot)} \cap \{a \mid ax = xa\}.$$

An element a of a loop $(Q;\cdot,e)$ is called a *Moufang* element if there exists a bijection λ of Q such that $(L_a;R_a;\lambda)$ is an autotopism of the loop, i.e.,

$$ay\cdot za=\lambda(y\cdot z) \tag{6}$$

for all $y,z\in Q$. Remark that if we put $y=e$, thereafter $z=e$, we obtain $\lambda=L_aR_a=R_aL_a$. A loop is called a *Moufang* loop if its every element is Moufang, i.e. if one of the identities

$$xy\cdot zx=x(y\cdot z)\cdot x,\qquad xy\cdot zx=x\cdot(y\cdot z)x \tag{7}$$

hold.

2 Pseudoisomorphy

Let $(Q_o;\circ)$ and $(Q;\cdot)$ be groupoids, $\alpha,\beta:\ Q_o\to Q$ be bijections, then α will be called

- a *left pseudoisomorphism* if (β,α,β) is an isotopism of the groupoids;
- a *right pseudoisomorphism* if (α,β,β) is an isotopism of the groupoids;
- a *middle pseudoisomorphism* if (β,β,α) is an isotopism of the groupoids;
- a *pseudoisomorphism* if it is both left and right pseudoisomorphism.

In these cases, the bijection β will be called a *companion* of the corresponding pseudoisomorphism. If $\alpha=\beta$ the pseudoisomorphism is an isomorphism.

It is easy to see that the set of all left (right and middle) pseudoautomorphisms of a quasigroup as well as their corresponding companions forms groups Ψ_ℓ, Ψ_ℓ^* (Ψ_r, Ψ_r^* and Ψ_m, Ψ_m^* respectively).

Relationships between pseudoisomorphy and neutrality are given in the following proposition.

Proposition 1. *Let $(Q;\cdot)$ be a quasigroup and θ be its*

1) *left pseudoautomorphism with a companion β, then $(Q;\cdot)$ has a left neutral element if and only if $\beta=L_a\theta$ for some element $a\in Q$;*

2) *right pseudoautomorphism with a companion β, then $(Q;\cdot)$ has a right neutral element if and only if $\beta=R_b\theta$ for some element $b\in Q$;*

3) *middle pseudoautomorphism with a companion β, then $(Q;\cdot)$ has a neutral element if and only if $\beta=L_c^{-1}\theta$ for some element $c\in Q$ such that $xc=cx$ for all $x\in Q$.*

Proof. Let θ be a left pseudoautomorphism of a quasigroup $(Q;\cdot)$ with a companion β, then $(\beta;\theta;\beta)$ is an autotopism of $(Q;\cdot)$, i.e.,

$$\beta x \cdot \theta y = \beta(x \cdot y)$$

Putting $x := e$ and $a := \beta e$, where e denotes the left neutral element of $(Q;\cdot)$, we obtain $\beta = L_a\theta$. Conversely, let the previous equality be true for some $a \in Q$, i.e.,

$$(a \cdot \theta x) \cdot \theta y = a \cdot \theta(x \cdot y).$$

Substituting $x = e := \theta^{-1}L_a^{-1}a$, we obtain

$$(a \cdot L_a^{-1}a) \cdot \theta y = a \cdot \theta(e \cdot y), \quad \text{i.e.} \quad a \cdot \theta y = a \cdot \theta(e \cdot y).$$

Cancelling out, we have $y = e \cdot y$. The item 2) can be proved analogously.

To prove 3) suppose that $(\beta;\beta;\theta)$ is an autotopism of $(Q;\cdot)$ and let e denote its neutral element, i.e.,

$$\beta x \cdot \beta y = \theta(x \cdot y)$$

for all $x, y \in Q$. When $x = e$ and $y = e$ the equality implies $L_c\beta = \theta$ and $R_c\beta = \theta$ respectively, where $c := \beta e$, so $xc = cx$ for all $x \in Q$. Conversely, since $(L_c^{-1}\theta, L_c^{-1}\theta, \theta)$ is an autotopism of $(Q;\cdot)$, then

$$L_c^{-1}\theta x \cdot L_c^{-1}\theta y = \theta(x \cdot y)$$

holds. As c commutes with all elements of Q, i.e. $L_c = R_c$, it is easy to verify that $e := \theta^{-1}L_c(c)$ is a neutral element in $(Q;\cdot)$ replacing successively x and y with e in the centralized formula. □

Note. Proposition 1 implies that for loops the introduced concept of pseudoautomorphism coincides with the well-known notion, except the notion of companion. A companion is a bijection in the definition given here, and an element in the well-known notion, but both of them uniquely define each other. Indeed, let a bijection β be a companion of θ, then

$$\beta x \cdot \theta y = \beta(x \cdot y) \quad \text{or} \quad \theta y \cdot \beta x = \beta(y \cdot y)$$

holds. Let e denote the neutral element of the loop and let $x := e$, we obtain $L_{\beta e}\theta = \beta$ or $R_{\beta e}\theta = \beta$. In both cases βe is a companion element of the pseudoautomorphism θ. Conversely, if an element c is a companion of θ, then the bijection $L_a\theta$ is its companion, in the case when θ is a left pseudoautomorphism; and $R_a\theta$ is its companion if θ is a right pseudoautomorphism. We will use both companions: an element and a bijection, but companion-element does not exist in the case when the quasigroup has no left and no right neutral elements.

2.1 Isotopism of loops

Some relations between isotopy and pseudoisomorphy for loops are given in the following lemma.

Lemma 1. *Let $(\alpha;\beta;\gamma)$ be an arbitrary isotopism of a loop $(Q_o;\circ,e)$ on a quasigroup $(Q;\cdot)$ and let $a:=\alpha e$, $b:=\beta e$. Then the following statements are true.*

1. $\alpha=R_b^{-1}\gamma$, $\beta=L_a^{-1}\gamma$;
2. *β is a left pseudoisomorphism, i.e. $\alpha=\gamma$ if and only if b is a right neutral element in $(Q;\cdot)$;*
3. *If β is a left pseudoisomorphism, then*
   - *(a) the loops $(Q;\circ)$ and $(Q;\odot)$ are isomorphic, where $x\odot y:=L_a^{-1}(ax\cdot y)$, i.e., $(\alpha;\beta;\gamma)=(L_a\beta;\beta;L_a\beta)$,*
   - *(b) β is an isomorphism of $(Q;\circ)$ and $(Q;\cdot)$ if and only if $a\in N_\ell^{(\cdot)}$;*
4. *α is a right pseudoisomorphism, i.e. $\beta=\gamma$ if and only if a is a left neutral element in $(Q;\cdot)$;*
5. *If α is a right pseudoisomorphism, then*
   - *(a) the loops $(Q;\circ)$ and $(Q;\bullet)$ are isomorphic, where $x\bullet y:=R_b^{-1}(x\cdot yb)$, i.e., $(\alpha;\beta;\gamma)=(\alpha;R_b\alpha;R_b\alpha)$;*
   - *(b) α is an isomorphism of the quasigroups $(Q;\circ)$ and $(Q;\cdot)$ if and only if $b\in N_r^{(\cdot)}$;*
6. *γ is a middle pseudoisomorphism, i.e. $\alpha=\beta$, if and only if $a:=\alpha e=\beta e$ and $a\cdot x=x\cdot a$ for all $x\in Q$.*
7. *If γ is a middle pseudoisomorphism, then*
   - *(a) the loops $(Q;\circ)$ and $(Q;\star)$ are isomorphic, where $x\star y:=L_a^{-1}x\cdot L_a^{-1}y$, i.e., $(\alpha;\beta;\gamma)=(L_a^{-1}\gamma;L_a^{-1}\gamma;\gamma)$;*
   - *(b) γ is an isomorphism between $(Q;\circ)$ and $(Q;\cdot)$ if and only if $a\in N_m^{(\cdot)}$ and $a\cdot a$ is a neutral element of the quasigroup $(Q;\cdot)$;*
8. *$\alpha=\beta=\gamma$ is an isomorphism if and only if $\alpha e=\beta e$ is a neutral element of the quasigroup $(Q;\cdot)$.*

Proof. The condition of the lemma means the truth of the equality

$$\gamma(x\circ y)=\alpha x\cdot\beta y \tag{8}$$

for all $x,y\in Q$. We successively put $x:=e$, $y:=e$ and obtain

$$\gamma y=\alpha(e)\cdot\beta y=a\cdot\beta y,\qquad \gamma x=\alpha x\cdot\beta(e)=\alpha x\cdot b.$$

Herefrom $\beta = L_a^{-1}\gamma$ and $\alpha = R_b^{-1}\gamma$, that is why the items 1, 2 are obvious.

Now suppose that β is a left pseudoisomorphism, i.e., $\alpha = \gamma$. But $\alpha = R_b^{-1}\gamma$, so $R_b = \iota$, then the equality (8) can be written as follows

$$L_a\beta x \cdot \beta y = L_a\beta(x \circ y). \tag{9}$$

Applying L_a^{-1} to the equality and replacing x with $\beta^{-1}x$, y with $\beta^{-1}y$, we obtain

$$L_a^{-1}(L_a x \cdot y) = \beta(\beta^{-1}x \circ \beta^{-1}y). \tag{10}$$

So, β is an isomorphism between $(Q;\circ)$ and $(Q;\odot)$.

If β is an isomorphism of $(Q;\circ)$ and $(Q;\cdot)$, then (10) implies

$$L_a^{-1}(L_a x \cdot y) = x \cdot y.$$

It means that $a \in N_\ell^{(\cdot)}$.

Thus, items 3a, 3b have been proved. The other statements of the lemma can be proved in the same way. $\square$

This lemma immediately implies the following corollary.

Corollary 1. *Let $(\alpha;\beta;\gamma)$ be an isotopism of a loop $(Q;\circ;e_1)$ on a loop $(Q;\cdot,e)$, then*

- *β is a left pseudoisomorphism if and only if $\beta e_1 = e$;*
- *α is a right pseudoisomorphism if and only if $\alpha e_1 = e$;*
- *γ is a middle pseudoisomorphism if and only if $a := \alpha e_1 = \beta e_1$ and $ax = xa$ for all $x \in Q$;*
- *γ is an isomorphism if and only if $\alpha e_1 = \beta e_1 = e$.*

Lemma 2. *Let θ be a left (or right) pseudoisomorphism with a companion c of a commutative loop $(Q;\oplus)$ on a commutative loop $(Q;+)$ with coinciding neclei, then θ is an isomorphism and c is a central element in the loop $(Q;+)$.*

Proof. Conditions of the lemma imply that

$$(c + \theta x) + \theta y = c + \theta(x \oplus y) \tag{11}$$

is true for all $x, y \in Q$. Using commutativity of both operations, we obtain

$$\theta y + (c + \theta x) = c + \theta(y \oplus x).$$

Mutually relabeling x and y, we have

$$\theta x + (c + \theta y) = c + \theta(x \oplus y).$$

So, the left sides of this equality and (11) are equal:

$$(c + \theta x) + \theta y = \theta x + (c + \theta y).$$

It means that c belongs to the middle nucleus of $(Q; +)$. But, according to the lemma's condition, the middle nucleus coincides with the center of the loop. Therefore, we can cancel out c in (11) and conclude that the pseudoisomorphism θ is an isomorphism of these loops. $\square$

This lemma immediately implies the following theorem.

Theorem 1. *Pseudoisomorphic commutative loops with coinciding nuclei are isomorphic.*

3 Inverse property loops

Inverse property loop (briefly IP-loop) is a loop $(Q; \cdot, e)$ that has a transformation I of Q such that

$$Ix \cdot (x \cdot y) = y, \qquad (x \cdot y) \cdot Iy = x$$

for all x, $y \in Q$. It is easy to verify that $Ix = x^{-1}$, $I^{-1} = I$ and $x \cdot x^{-1} = x^{-1} \cdot x = e$.

IP-loop $(Q; \cdot)$ with a neutral element e and unary operation $I(x) := x^{-1}$ will be denoted by $(Q; \cdot, I, e)$.

Lemma 3. *Let $(\alpha; \beta; \gamma)$ be an isotopism of an IP-loop $(Q; \circ, I_1, e_1)$ on an IP-loop $(Q; \cdot, I, e)$, then both the triplets $(I\alpha I_1; \gamma; \beta)$ and $(\gamma; I\beta I_1; \alpha)$ are isotopisms of the same loops.*

Proof. The conditions of the lemma imply the equality $\alpha x \cdot \beta y = \gamma(x \circ y)$. We put here successively $y := I_1 x \circ u$ and $x = v \circ I_1 y$:

$$\alpha x \cdot \beta(I_1 x \circ u) = \gamma u, \qquad \alpha(v \circ I_1 y) \cdot \beta y = \gamma v.$$

In the first equality, we replace x with $I_1 t$, in the second one y with $I_1 z$:

$$\beta(t \circ u) = I\alpha I_1 t \cdot \gamma u, \quad \alpha(v \circ z) = \gamma v \cdot I\beta I_1 z.$$

Thus, $(I\alpha I_1; \gamma; \beta)$ and $(\gamma; I\beta I_1; \alpha)$ are isotopisms of $(Q; \circ, I_1, e_1)$ on $(Q; \cdot, I, e)$. $\square$

Corollary 2. *Nuclei of an inverse property loop coincide.*

Proof. Let $(Q; \cdot, I, e)$ be an IP-loop. Belonging of an element a to the left nucleus $N_\ell^{(\cdot)}$ of the loop means that the triplet $(L_a; L_a; \iota)$ is an autotopism of $(Q; \cdot, I, e)$. Lemma 3 implies that both

$$(IL_a I; L_a; \iota) \quad \text{and} \quad (\iota; IL_a I; IL_a I)^{-1}$$

are its autotopisms. Using the equality $IL_aI = R_a^{-1}$, we conclude that both

$$(R_a^{-1}; L_a; \iota) \quad \text{and} \quad (\iota; R_a; R_a)$$

are autotopisms. So, an arbitrary element $a \in Q$ belongs to the left and middle nucleus as well as to the left and right nucleus simultaneously, i.e., the nuclei coincide. $\square$

Lemma 4. *The sets of all left and right pseudoisomorphisms between inverse property loops coincide. If α is a pseudoisomorphism of an inverse property loop $(Q; \circ, I_1, e_1)$ on an inverse property loop $(Q; \cdot, I, e)$, then $\alpha e_1 = e$; $I\alpha = \alpha I_1$.*

Proof. Let $(\alpha; \beta; \beta)$ be an isotopism of an IP-loop $(Q; \circ)$ on an IP-loop $(Q; \cdot)$. Applying Lemma 3, we conclude that $(I\beta I_1; \alpha; I\beta I_1)$ and $(I\alpha I_1, \beta, \beta)$ are isotopisms of these loops. So, α is a left pseudoisomorphism of these loops. Since any two components of an isotopism of quasigroups uniquely define the third, then $I\alpha I_1 = \alpha$, i.e., $I\alpha = \alpha I_1$. $\square$

Theorem 2. *Let $T := (\alpha; \beta; \gamma)$ be an isotopism of an inverse property loop $(Q_1; \circ, e_1)$ on an inverse property loop $(Q; \cdot; e)$ and let $a := \alpha(e_1)$, $b := \beta(e_1)$, then:*

1. *$\theta := L_a^{-1}\alpha$ is a pseudoisomorphism of $(Q_1; \circ, I_1, e_1)$ on $(Q; \cdot; I, e)$ with the right companion $c := b \cdot a^{-1}$;*
2. *the elements a, b, $a \cdot b$ are Moufang;*
3. *$(\alpha; \beta; \gamma) = (L_a; R_a; L_aR_a)(\theta; R_c\theta; R_c\theta)$.*

Proof. Lemma 1 and Lemma 3 imply that $\alpha = R_b^{-1}\gamma$, $\beta = L_a^{-1}\gamma$ and the triplet $T_1 := (I\alpha I_1; \gamma; \beta)$ is an isotopism of these loops. Hence, the triplet

$$TT_1^{-1} = (R_b^{-1}\gamma; L_a^{-1}\gamma; \gamma)(I_1\gamma^{-1}R_bI; \gamma^{-1}; \gamma^{-1}L_a) = (\lambda; L_a^{-1}; L_a)$$

is an autotopism of $(Q; \cdot, e)$ for some bijection λ of the set Q. According to Lemma 3,

$$T_2 := (L_a; IL_a^{-1}I; \lambda) = (L_a; R_a; \lambda)$$

is an autotopism of $(Q; \cdot, e)$. So, a is Moufang in $(Q; \cdot, e)$ and $\lambda = L_aR_a = R_aL_a$.

Lemma 3 implies that $(\gamma; I\beta I_1; \alpha)$ and $(\beta; I\gamma I_1; I\alpha I_1)$ are autotopisms, consequently, the elements $ab = \alpha(e_1) \cdot \beta(e_1) = \gamma(e_1 \circ e_1) = \gamma(e_1)$ and $b = \beta(e_1)$ are Moufang too. Hence, the item 2. has been proved.

Then $T_2^{-1}T$ is an isotopism of $(Q_1; \circ, I_1, e_1)$ on $(Q; \cdot, I, e)$ and

$$T_2^{-1}T = (L_a^{-1}\alpha; R_a^{-1}\beta; L_a^{-1}R_a^{-1}\gamma).$$

As $L_a^{-1}\alpha(e_1) = L_a^{-1}a = e$, by virtue of Corollary 1 and Proposition 1, $L_a^{-1}\alpha =: \theta$ is a pseudoisomorphism with the right companion $c := R_a^{-1}\beta(e_1) = b \cdot a^{-1}$. This proves the item 1). Thus, $T_2^{-1}T = (\theta; R_c\theta; R_c\theta)$. Therefrom, we obtain the item 3. $\square$

Corollary 3. *Isotopic inverse property loops are pseudoisomorphic.*

Proof. It follows from the item 1 of Theorem 2. □

Corollary 4. *Let* (α, β, γ) *be an isotopism of a commutative inverse property loop* $(Q_o; \circ, e)$ *on a commutative inverse property loop* $(Q; +, 0)$*, then there exists an isomorphism* θ *of* $(Q_o; \circ, e)$ *on* $(Q; +, 0)$*, a central element* c *in* $(Q; +, 0)$ *and a Moufang element* $a \in Q$ *such that* $\alpha = L_a\theta$*,* $\beta = L_aL_c\theta$*,* $\gamma = L_a^2L_c\theta$*.*

Proof. According to Theorem 2 there exists a pseudoisomorphism θ of $(Q_o; \circ, e)$ on $(Q; +, 0)$ with a companion c and a Moufang element a such that

$$\alpha = L_a\theta, \qquad \beta = R_aR_c\theta, \qquad \gamma = L_aR_aR_c\theta.$$

Since the nuclei coincide in these loops (Corollary 2), then by virtue of Lemma 2 θ is an isomorphism of these loops and c is a central element in the loop $(Q; +, 0)$. Commutativity means $L_x = R_x$ for all x. □

Corollary 5. *Isotopic commutative inverse property loops are isomorphic.*

Proof. The proof follows from Corollary 4. □

Since every Moufang loop has the inverse property, then the following statement is true.

Corollary 6. *Isotopic commutative Moufang loops are isomorphic.*

Corollary 7. *In an arbitrary inverse property loop the set of all Moufang elements form a subloop, which is a Moufang loop.*

Proof. Let a, b be Moufang elements of an IP-loop $(Q; \cdot, I, e)$, i.e.

$$(L_a, R_a, L_aR_a) \quad \text{and} \quad (L_b, R_b, L_bR_b)$$

are autotopisms. Then their inverses and composition are autotopisms too. By virtue of the item 2 of Theorem 2, the elements $a^{-1} = L_a^{-1}(e)$ and $a \cdot b = L_aL_b(e)$ are Moufang. Consequently, Moufang elements form a subloop. □

4 Distributive quasigroups

A quasigroup is called *left* (*right*, *middle*) *distributive* if every its left (right, middle) translations is its automorphism.

In other words, such quasigroups are defined by the identity of *left*, *right*, *middle distributivity*:

$$x \cdot yz = xy \cdot xz, \tag{12}$$

$$yz \cdot x = yx \cdot zx, \tag{13}$$

$$yz\backslash x = (y\backslash x) \cdot (z\backslash x) \tag{14}$$

respectively.

A quasigroup is called *distributive* if it is both left and right distributive.

Lemma 5. *For any element $a \in Q$ of a distributive quasigroup $(Q;\cdot)$, the translations L_a, R_a, M_a are pairwise commuting automorphisms of every parastrophe of the quasigroup.*

Proof. The left and right distributivity mean that L_a and R_a are automorphisms of $(Q;\cdot)$. Since automorphism groups of all parastrophes coincide, then L_a, R_a as well as L_a^{-1}, R_a^{-1} are automorphisms of all parastrophes of the quasigroup.

Multiply the equality $z \cdot (z\backslash y) = y$ (see (1)) by $z\backslash u$ from the right and use (13):

$$z(z\backslash u) \cdot (z\backslash y)(z\backslash u) = y(z\backslash u).$$

As $z(z\backslash u) = u$ and L_z^{-1}, L_y are automorphisms of $(Q;\cdot)$ (see (3)), then

$$u \cdot z\backslash(yu) = yz\backslash yu.$$

Let $yu = a$, i.e., $y\backslash a = u$, then

$$(y\backslash a)(z\backslash a) = yz\backslash a.$$

It means that for arbitrary $a \in Q$ the middle translation M_a is an automorphism of $(Q;\cdot)$, and, consequently, of every its parastrophe.

Every of the identities (12), (13), (14) implies idempotency $xx = x$ (when $x = y = z$). The previous identity implies the equalities $L_a(a) = R_a(a) = M_a(a) = a$, that is why

$$L_aR_a(x) = L_a(xa) = L_a(x) \cdot L_a(a) = L_a(x) \cdot a = R_aL_a(x),$$

$$M_aL_a(x) = M_a(ax) = M_a(a) \cdot M_a(x) = a \cdot M_a(x) = L_aM_a(x).$$

Analogously, $M_aR_a = R_aM_a$. □

Corollary 8. *All parastrophes of a distributive quasigroup are distributive and pairwise distributive.*

In other words, for every $\sigma, \tau \in S_3$ the follow identities are true

$$x \overset{\sigma}{\cdot} (y \overset{\tau}{\cdot} z) = (z \overset{\sigma}{\cdot} y) \overset{\tau}{\cdot} (x \overset{\sigma}{\cdot} z), \qquad (y \overset{\tau}{\cdot} z) \overset{\sigma}{\cdot} x = (y \overset{\sigma}{\cdot} x) \overset{\tau}{\cdot} (z \overset{\sigma}{\cdot} x).$$

Proof. From the table (4), we conclude that L_x, R_x, M_x, L_x^{-1}, R_x^{-1}, M_x^{-1}, where $x \in Q$, are all translations of all parastrophes of a quasigroup $(Q;\cdot)$. That is why Lemma 5 implies this corollary. □

Corollary 9. *Every two of the identities (12), (13), (14) imply the third.*

Proof. If a quasigroup $(Q;\cdot)$ satisfies (12) and (13), then Lemma 5 implies (14). If (12) and (14) hold in the quasigroup, then the table (4) implies that $(Q;\backslash)$ is left and right distributive and, according to Lemma 5, it is middle distributive. Relations between translations (the table (4)) induce right distributivity of $(Q;\cdot)$, i.e., (13) holds.

The implication (13) & (14) $\Rightarrow$ (12) can be proved in the same way. □

Corollary 10. *A quasigroup is distributive if and only if all its translations are its automorphisms.*

The following theorem is a specification of the corresponding Belousov's result.

Theorem 3. *A quasigroup $(Q;\cdot)$ is distributive if and only if there exists a commutative Moufang loop $(Q;+)$ and its automorphism φ such that $\psi:=\iota-\varphi$ is an automorphism of $(Q;+)$ and*

$$x\cdot y=\varphi x+\psi y, \tag{15}$$

$$x+(y+z)=(\varphi x+y)+(\psi x+z). \tag{16}$$

Proof. Let $(Q;\cdot)$ be an arbitrary distributive quasigroup and 0 be an arbitrary fixed element from Q. In this proof, we will write L, R, M instead of L_0, R_0, M_0. We define an operation $(+)$ on the set Q putting

$$x+y:=R^{-1}(x)\cdot L^{-1}(y). \tag{17}$$

Herefrom

$$x\cdot y=R(x)+L(y). \tag{18}$$

Idempotency of $(Q;\cdot)$ implies that 0 is a neutral element in $(Q;+)$.

Since L and R are commuting automorphisms of $(Q;\cdot)$, then they are automorphisms of the loop $(Q;+)$. For example,

$$L(x+y)\overset{(17)}{=}L(R^{-1}(x)\cdot L^{-1}(y))\overset{Lemma\ 5}{=}LR^{-1}(x)\cdot LL^{-1}(y)=$$
$$\overset{Lemma\ 5}{=}R^{-1}L(x)\cdot L^{-1}L(y)\overset{(17)}{=}L(x)+L(y).$$

We show that $(Q;+)$ is a right IP-loop, i.e., for some mapping I the identity

$$(y+x)+I(x)=y \tag{19}$$

holds. Put $I:=LMR^{-1}$ and, for brevity, we denote $u:=R^{-2}(y)$, $t:=R^{-1}L^{-1}(x)$. Hence, we have

$$(y+x)+I(x)\overset{(17)}{=}R^{-1}\big(R^{-1}(y)\cdot L^{-1}(x)\big)\cdot L^{-1}LMR^{-1}(x)=$$
$$\overset{\text{Lemma 5}}{=}\big(R^{-2}(y)\cdot R^{-1}L^{-1}(x)\big)\cdot LMR^{-1}L^{-1}(x)=ut\cdot\big(0\cdot M(t)\big)=$$
$$\overset{(12)}{=}(ut\cdot 0)\big(ut\cdot M(t)\big)\overset{(13)}{=}(ut\cdot 0)\big(uM(t)\cdot tM(t)\big)=(ut\cdot 0)\big(uM(t)\cdot 0\big)=$$
$$\overset{(13)}{=}\big(ut\cdot uM(t)\big)\cdot 0\overset{(12)}{=}R\big(u\cdot tM(t)\big)=R(u\cdot 0)=R^2R^{-2}(y)=y.$$

To prove commutativity of $(+)$, we note that for all $x,y\in Q$ the equality

$$(x+y)+I(x)=y \tag{20}$$

holds. Denote $z := R^{-2}(x)$, $v := R^{-1}L^{-1}(y)$, then

$$\begin{aligned}(x+y)+I(x) &\overset{(17)}{=} R^{-1}\big(R^{-1}(x)\cdot L^{-1}(y)\big)\cdot L^{-1}LMR^{-1}(x) =\\ &= \Big(R^{-2}(x)\cdot R^{-1}L^{-1}(y)\Big)\cdot M\Big(R^{-2}(x)\cdot 0\Big) = zv\cdot M(z0) =\\ &= L_{z0}^{-1}\Big(z0\cdot\big(zv\cdot M(z0)\big)\Big) \overset{(12)}{=} L_{z0}^{-1}\Big((z0\cdot zv)\cdot\big(z0\cdot M(z0)\big)\Big) =\\ &= L_{z0}^{-1}\Big((z0\cdot zv)\cdot 0\Big) \overset{(12)}{=} L_{z0}^{-1}\Big((z\cdot 0v)\cdot 0\Big) =\\ &\overset{(13)}{=} L_{z0}^{-1}\Big(z0\cdot(0v\cdot 0)\Big) = 0v\cdot 0 = RLR^{-1}L^{-1}(y) = y.\end{aligned}$$

The equality of the right sides of (19) and (20) implies the equality of their left sides: $(y+x)+I(x) = (x+y)+I(x)$, that is why $y+x = x+y$. Hence, $(Q;+)$ is a commutative IP-loop.

Using (18), we replace the second and the forth appearances of the operation $(\cdot)$ with $(+)$ in (12):

$$x\cdot(Ry+Lz) = R(xy)+L(xz).$$

Replacing Ry with y and Lz with z, we obtain:

$$L_x(y+z) = RL_xR^{-1}(y)+LL_xL^{-1}(z).$$

It means that the triplet $(RL_xR^{-1}; LL_xL^{-1}; L_x)$ is an autotopism of the IP-loop $(Q;+)$ for all $x\in Q$. Theorem 2 implies that the element $L_x(0) = x\cdot 0 = R(x)$ is a Moufang element in $(Q;+)$. As R is a bijection of Q, then an arbitrary element from Q is Moufang, so $(Q;+)$ is a commutative Moufang loop.

Idempotency $x\cdot x = x$ of $(\cdot)$ means that $\varphi x+\psi x = x$, i.e., $\psi = \iota-\varphi$.

It remains to prove that in a commutative Moufang loop $(Q;+)$ which has two commuting automorphisms φ and ψ such that the equality (15) holds, two identities of distributivity (12) and (13) are equivalent to the identity (16). For this purpose, we replace $(\cdot)$ with $(+)$ in (12) and (13):

$$\varphi x+(\psi\varphi y+\psi^2 z) = (\varphi^2 x+\varphi\psi y)+(\psi\varphi x+\psi^2 z),$$

$$(\varphi^2 y+\varphi\psi z)+\psi x = (\varphi^2 y+\varphi\psi x)+(\psi\varphi z+\psi^2 x).$$

In the first identity, we replace φx with x, $\psi\varphi y$ with y and $\psi^2 z$ with z, and in the second one $\varphi^2 y$ with y, $\varphi\psi z$ with z and ψx with x. Since $\varphi\psi = \psi\varphi$, then we obtain identities being equivalent to above mentioned:

$$x+(y+z) = (\varphi x+y)+(\psi x+z),$$

$$(y+z)+x = (y+\varphi x)+(z+\psi x).$$

Commutativity of $(+)$ implies coincidence of both of them with (16). $\square$

Remark that it is easy to verify that middle distributivity (14) coincides with (16) if we replace $(\cdot)$ with $(+)$.

Corollary 11 (V. D. Belousov [1])**.** *Every distributive quasigroup is isotopic to a commutative Moufang loop.*

Note that Theorem 3 implies that any distributive quasigroup can be considered as a *corresponding algebra* $(Q;+,\varphi)$ which satisfies the conditions:

1) $(Q;+)$ is a commutative Moufang loop;
2) φ and $\iota-\varphi:=\psi$ are automorphisms of $(Q;+)$;
3) the identity (16) holds.

(Compare with Belousov-Onoi module [4].) We will also say that "*the automorphism φ defines a distributive quasigroup $(Q;\cdot)$ on the commutative Moufang loop $(Q;+)$*".

Theorem 3 creates a possibility for studying distributive quasigroups via commutative Moufang loops. For example, we have to answer questions like "When distributive quasigroups are isotopic? isomorphic?" and so on. The next three propositions give answers to some of such questions.

Corollary 12. *Distributive quasigroups are isotopic if and only if the corresponding commutative Moufang loops are isomorphic.*

Proof. The truth of the corollary follows from Corollary 5. □

Taking into account Corollary 12, we may restrict our attention to distributive quasigroups defined on the same commutative Moufang loop and the first question that arises is the following: "What relation between automorphisms of the same commutative Moufang loop which define distributive quasigroups?"

Corollary 13. *Let an automorphism φ of a commutative Moufang loop $(Q;+)$ define a distributive quasigroup on $(Q;+)$. Then a bijection φ_o defines a distributive quasigroup on $(Q;+)$ if and only if there exists a homomorphism ν from $(Q;+)$ into its center such that $\varphi_o=\varphi+\nu$ and $\psi_o=\iota-\varphi-\nu$ are bijections of Q.*

Proof. Let automorphisms φ and φ_o define distributive quasigroups on a commutative Moufang loop $(Q;+)$. It implies that (16) and

$$x+(y+z)=(\varphi_o x+y)+(\psi_o x+z)$$

hold. Consequently, the right sides of these identities are equal:

$$(\varphi x+y)+(\psi x+z)=(\varphi_o x+y)+(\psi_o x+z).$$

Replace z with $-\psi_o x+z$ and y with $-\varphi x+y$:

$$y+(\psi x+(-\psi_o x+z))=(\varphi_o x+(-\varphi x+y))+z. \tag{21}$$

Let $\nu := \varphi_o - \varphi$, then $\psi - \psi_o = (\iota - \varphi) - (\iota - \varphi_o) = \varphi_o - \varphi = \nu$. When $y = 0$ and when $z = 0$ the equality (21) implies

$$\psi x + (-\psi_o x + z) = \nu x + z \qquad \text{and} \qquad y + \nu x = \varphi_o x + (-\varphi x + y).$$

So, (21) can be written as follows

$$y + (\nu x + z) = (y + \nu x) + z.$$

So, ν is a mapping from the loop $(Q;+)$ into its center and $\varphi_o = \varphi + \nu$.

Since φ_o is an automorphism of the loop $(Q;+)$, then

$$(\varphi + \nu)x + (\varphi + \nu)y = (\varphi + \nu)(x + y),$$

i.e.,

$$(\varphi x + \nu x) + (\varphi y + \nu y) = (\varphi x + \varphi y) + \nu(x + y).$$

As νx is a central element for all $x \in Q$, then we can change the left side of the equality:

$$(\varphi x + \varphi y) + \nu x + \nu y = (\varphi x + \varphi y) + \nu(x + y).$$

Cancelling out $\varphi x + \varphi y$, we obtain a homomorphic property for ν.

Vice versa, let ν be an arbitrary homomorphism from a commutative Moufang loop $(Q;+)$ into its center and let $\nu + \varphi$ and $\iota - \varphi - \nu$ be bijections of Q. Define transformations

$$\varphi_o := \varphi + \nu \quad \text{and} \quad \psi_o := \iota - \varphi - \nu = \iota - \varphi_o = \psi - \nu.$$

Both of them are automorphisms of $(Q;+)$. Indeed, they are bijections according to the assumption. In the following proof of the homomorphic property of φ_o we are using the fact that νx is a central element of $(Q;+)$ for arbitrary $x \in Q$:

$$\begin{aligned}\varphi_o(x + y) &= (\varphi + \nu)(x + y) = \varphi(x + y) + \nu(x + y) = (\varphi x + \varphi y) + (\nu x + \nu y) = \\ &= (\varphi x + \nu x) + (\varphi y + \nu y) = (\varphi + \nu)x + (\varphi + \nu)y = \varphi_o x + \varphi_o y.\end{aligned}$$

As $\psi_o = \psi - \nu$, we have

$$\begin{aligned}\psi_o x + \psi_o y &= (\psi - \nu)x + (\psi - \nu)y = (\psi x - \nu x) + (\psi y - \nu y) = \\ &= (\psi x + \psi y) - (\nu x + \nu y) = \psi(x + y) - \nu(x + y) = (\psi - \nu)(x + y) = \\ &= \psi_o(x + y).\end{aligned}$$

It remains to prove that (16) is true for φ_o. For this purpose, we add the neutral element 0 in the form $0 = \nu x + (-\nu x)$ to the right side of (16):

$$x + (y + z) = (\varphi x + \nu x + y) + (\psi x - \nu x + z) = (\varphi_o x + y) + (\psi_o x + z).$$

Thus, according to Theorem 3, the automorphism φ_o defines a distributive quasigroup on the commutative Moufang loop $(Q;+)$. $\square$

The next theorem gives a isomorphy criterion of distributive quasigroups (it is close to [5, Lemma 12.3]).

Theorem 4. *Distributive quasigroups are isomorphic if and only if their corresponding algebras are isomorphic.*

Proof. Let $(Q;\circ)$ and $(Q;\cdot)$ be distributive quasigroups, which are defined on commutative Moufang loops $(Q_o;\oplus,0')$ and $(Q;+,0)$ by their automorphisms φ_o and φ respectively, that is $(Q_o;\oplus,\varphi_o)$ and $(Q;+,\varphi)$ are corresponding algebras. According to Theorem 3, the mappings $\psi:=\iota-\varphi$ and $\psi_o:=\iota\ominus\varphi_o$ are automorphisms of $(Q;+,0)$ and $(Q_o;\oplus,0')$ respectively, besides (15) and

$$x\circ y=\varphi_o x\oplus\psi_o y$$

hold.

Let α be an isomorphism from $(Q_o;\circ)$ onto $(Q;\cdot)$, i.e.,

$$\alpha x\cdot\alpha y=\alpha(x\circ y)$$

for all $x,y\in Q$. This equality can be written as follows

$$\varphi\alpha x+\psi\alpha y=\alpha(\varphi_o x\oplus\psi_o y).$$

Replace x with $\varphi_o^{-1}(x)$ and y with $\psi_o^{-1}(y)$:

$$\varphi\alpha\varphi_o^{-1}(x)+\psi\alpha\psi_o^{-1}(y)=\alpha(x\oplus y).$$

The obtained equality means that the triplet $(\varphi\alpha\varphi_o^{-1},\psi\alpha\psi_o^{-1},\alpha)$ is an isotopism from the Moufang loop $(Q_o;\oplus)$ onto the Moufang loop $(Q;+)$. According to Corollary 4, there exists an isomorphism θ from $(Q_o;\oplus,0')$ onto $(Q;+,0)$, a central element c of $(Q;+)$ and an element $a\in Q$ such that the equalities

$$\varphi\alpha\varphi_o^{-1}=L_a\theta,\qquad \psi\alpha\psi_o^{-1}=L_aL_c\theta,\qquad \alpha=L_a^2L_c\theta$$

are true. Using the third equality, we substitute $L_a^2L_c\theta$ for α in the first one:

$$\varphi L_a^2L_c\theta\varphi_o^{-1}=L_a\theta.$$

Using Moufang identity (7), centrality of c and diassociativity of $(Q;+)$, we have

$$\begin{aligned}L_a^2L_c(x)&=a+(a+(c+x))=(a+c)+(a+x)=L_c^{-1}((a+c)+((a+c)+x))=\\&=L_c^{-1}(((a+c)+(a+c))+x)=L_c^{-1}L_{2(a+c)}(x).\end{aligned}$$

Consequently,

$$\varphi L_c^{-1}L_{2(a+c)}\theta\varphi_o^{-1}=L_a\theta.$$

As φ is an automorphism of $(Q;+)$, then

$$L_{\varphi c}^{-1}L_{\varphi(2(c+a))}\varphi\theta\varphi_o^{-1}=L_a\theta.$$

Therefrom

$$L_{\varphi(2(c+a))}\varphi\theta\varphi_o^{-1} = L_{\varphi c+a}\theta.$$

Since $\varphi\theta\varphi_o^{-1}(0') = 0$ and $\theta(0') = 0$, the previous equality implies $\varphi(2(c+a)) = \varphi c+a$. Therefore, $\varphi\theta\varphi_o^{-1} = \theta$, i.e., $\varphi\theta = \theta\varphi_o$. Thus, θ is an isomorphism from the algebra $(Q_o;\oplus,\varphi_o)$ onto the algebra $(Q;+,\varphi)$.

Vice versa, let θ be an isomorphism from $(Q_o;\oplus,\varphi_o)$ onto $(Q;+,\varphi)$. It means, that θ is an bijection from Q_o onto Q and the following relations hold:

$$\theta(x)+\theta(y) = \theta(x\oplus y), \qquad \varphi\theta = \theta\varphi_o$$

for all $x, y \in Q_o$. These equalities imply $\psi\theta = \theta\psi_o$. Indeed,

$$\begin{aligned}\psi\theta(x) &= (\iota-\varphi)\theta(x) = \theta(x)-\varphi\theta(x) = \\ &= \theta(x)\ominus\theta\varphi_o(x) = \theta(x\ominus\varphi_o(x)) = \theta(\iota\ominus\varphi_o)(x) = \theta\psi_o(x).\end{aligned}$$

That is why, we have

$$\theta x\cdot\theta y = \varphi\theta x+\psi\theta y = \theta\varphi_o x+\theta\psi_o y = \theta(\varphi x\oplus\psi y) = \theta(x\circ y).$$

Hence, θ is an isomorphism from $(Q;\circ)$ onto $(Q;\cdot)$. □

Corollary 14. *Let distributive quasigroups $(Q;\circ)$ and $(Q;\cdot)$ be defined on a commutative Moufang loop $(Q;+)$ by its automorphisms φ_o and φ respectively. Then the quasigroups are isomorphic if and only if there exists an automorphism θ of the loop $(Q;+)$ such that $\varphi_o = \theta^{-1}\varphi\theta$.*

This corollary immediately implies that there exist exactly $p-3$ non-isomorphic distributive quasigroups of a prime power $p \geqslant 3$.

Acknowledgment. The author would like to thank Vira Obshanska, Halyna Krainichuk, Iryna Fryz and Olena Tarkovska for useful comments which contributed to a better paper.

References

[1] Belousov V. D. *Foundation of the theory of quasigroups and loops.* M., Nauka, 1967, 222 p. (in Russian).

[2] Plugfelder Hala O. *Quasigroups and loops: introduction.* Berlin, Heldermann, 1990, 147 p.

[3] Mullen G. L., Shcherbacov V. A. *On orthogonality of binary operations and squares.* Buletinul Academiei de Ştiinţe a Republicii Moldova, Matematica, 2005. No. 2(48), 3–42.

[4] Stanovský David. *A guide to self-distributive quasigroups, or latin quandles.* arXiv:1505.06609v2 [math.GR].

[5] Kepka T., Němec P. *Commutative Moufang loops and distributive groupoids of small orders.* Czech. Math. J., 1981, **31/106**, 633–669.

Fedir M. Sokhatsky
Vasyl Poryk, 5, ap.37, Vinnytsia, 21021
Ukraine

E-mail: *fmsokha@ukr.net*

Received March 04, 2016