BULETINUL ACADEMIEI DE ŞTIINŢE
A REPUBLICII MOLDOVA. MATEMATICA
Number 3(64), 2010, Pages 29–34
ISSN 1024–7696

On isotopy, parastrophy and orthogonality of quasigroups

K. K. Shchukin

Abstract. This paper contains new results on conditions of an isotopy of two quasigroups and their orthogonality to parastrophes. The structure of parastrophe group of a quasigroup is defined. The results of this paper complement investigations of V. D. Belousov in [1, 2] and continue studies from [3].

Mathematics subject classification: 20N05.
Keywords and phrases: Quasigroup, isotopy, parastrophy, orthogonality.

To the 85 Anniversary of V. D. Belousov (1925–1988)

1 Main results

1. Every quasigroup $(Q,\cdot)$ defines three permutations on the set Q. These are left $L_a(y) = ay$ and right $R_a(y) = ya$ translations for all $a, y \in Q$. A middle one J_a and its inversion J_a^{-1} are defined by $xJ_a(x) = a$, $J_a^{-1}(x)x = a$, $x, a \in Q$ respectively. A quasigroup $(Q, *)$ is conjugate to a quasigroup $(Q,\cdot)$ if $x * y = yx$ is true for all $x, y \in Q$. It is evident that $L_a^*(y) = R_a(y)$ for all $a, y \in Q$, so $L_a^* = R_a$ and $L_a = L_a^{**} = R_a^*$.

Theorem 1 (see [3]). *Let $(Q,\cdot)$ and $(Q,\circ)$ be quasigroups and (φ,ψ,χ) be an ordered triple of permutations on the set Q.*

(i) The formula $\chi(xy) = \varphi(x)\circ\psi(y)$, for all $x, y \in Q$, defines an isotopy of $(Q,\cdot)$ and $(Q,\circ)$ if and only if

$$\psi J_a\varphi^{-1}(\varphi(x)) = J^\circ_{\chi(a)}(\varphi(x))$$

for all $x, y \in Q$, $xy = a$.

The equalities $\varphi = \psi = \chi$ define an isomorphism of these quasigroups:

$$\chi J_a\chi^{-1}(\chi(x)) = J^\circ_{\chi(a)}(\chi(x))$$

for all $x, y \in Q$, $xy = a$.

(ii) the formula $\chi(xy) = \psi(y)\circ\varphi(x)$, for all $x, y \in Q$, defines an anti-isotopy of $(Q,\cdot)$ and $(Q,\circ)$ if and only if

$$\psi J_a\varphi^{-1}(\varphi(x)) = (J^\circ_{\chi(a)})^{-1}(\varphi(x))$$

for all $x, y \in Q$, $xy = a$.

The equalities $\varphi = \psi = \chi$ *define an anti-isomorphism of* $(Q, \cdot)$ *and* $(Q, \circ)$ *if and only if*

$$\chi J_a \chi^{-1}(\chi(x)) = (J^{\circ}_{\chi(a)})^{-1}(\chi(x))$$

for all $x, y \in Q$, $xy = a$.

(iii) *There are equivalences of an isotopy* (φ, ψ, χ) *of the quasigroups* $(Q, \cdot)$ *and* $(Q, \circ)$ *for all* $x, y \in Q$: $\chi(xy) = \varphi(x) \circ \psi(y) \iff \chi L_x \psi^{-1}(y) = L^{\circ}_{\varphi(x)}(y) \iff \chi R_y \varphi^{-1}(x) = R^{\circ}_{\psi(y)}(x)$.

Proof. The statement (i) is established by the following chain of equivalences: $\chi(xy) = \varphi(x) \circ \psi(y) \Leftrightarrow \chi(a) = \varphi(x) \circ J^{\circ}_{\chi(a)}\varphi(x) \Leftrightarrow J^{\circ}_{\chi(a)}\varphi(x) = \psi(y) = \psi J_a \varphi^{-1}(\varphi(x)) \Leftrightarrow J^{\circ}_{\chi(a)}\varphi(x) = \psi J_a \varphi^{-1}(\varphi x)$ for all $x, y \in Q$, putting $xy = a$, where a depends on x, y. The case $\varphi = \psi = \chi$ reduces to three equivalent conditions of isomorphism of $(Q, \cdot)$ and $(Q, \circ)$.

The statement (ii) is verified like (i): $\chi(xy) = \psi(y) \circ \varphi(x) \Leftrightarrow \chi(a) = \psi(y) \circ J^{\circ}_{\chi(a)}(\psi(y)) \Leftrightarrow J^{\circ}_{\chi(a)}\psi(y) = \varphi(x) = \varphi J_a^{-1}\psi^{-1}(y) \Leftrightarrow (J^{\circ}_{\chi(a)})^{-1}\varphi(x) = \psi J_a \varphi^{-1}(\varphi(x))$ for all $x, y \in Q, xy = a$. Three equivalent conditions of anti-isomorphism of the quasigroups $(Q, \cdot)$ and $(Q, \circ)$ follow by $\varphi = \psi = \chi$. $\square$

We consider the *signature* $(Q, \cdot)$ of a finite quasigroup $(Q, \cdot)$ of order n as an ordered triple of signs:

$$signature\ (Q, \cdot) = (sign\ Q_L, sign\ Q_R, sign\ Q_J),$$

where $Q_L = L_1 \dots L_n$, $Q_R = R_1 \dots R_n$, $Q_J = J_1 \dots J_n$ are the products of translations of $(Q, \cdot)$.

As it is known, a complete associated group of a quasigroup is generated by all left, right and middle translations of this quasigroup [1].

From Theorem 1 we easy obtain

Corollary 1. *a) Isomorphic or anti-isomorphic quasigroups have isomorphic or anti-isomorphic complete associated groups, respectively.*

b) Let $(Q, \circ)$ *be an isotope or an anti-isotope of a finite quasigroup* $(Q, \cdot)$ *of order* n. *There are the following formulas (cf.*(iii)*):*

Signature $(Q, \circ) = (sign(\chi\psi)^n sign Q_L, sign(\chi\varphi)^n sign Q_R, sign(\varphi\psi)^n sign Q_J)$ *by an isotopy* $\chi(x, y) = \varphi(x) \circ \psi(y)$

To get the formula of signature $(Q, \circ)$ *of an anti-isotope it is sufficient only to exchange the first and the second components of the formula for isotopy* (i).

There is the equality *signature* $(Q, \circ) =$ *signature* $(Q, \cdot)$ in both cases (i) and (ii) for $n = 2m$ or $\varphi = \psi = \chi$.

2. We preserve here the notation of the paper [3] (see also [4, p. 13–14]). If $\alpha = (\odot)$ is a quasigroup operation, then α, $\beta = * = \alpha^*$, $\gamma = \alpha^{-1}$, $\delta = {}^{-1}\alpha$,

$\varepsilon = {}^{-1}(\alpha^{-1}) = \gamma^*$, $\eta = \left({}^{-1}\alpha\right)^{-1} = \delta^*$ will denote the inverse operations of the quasigroup $(Q,\odot) = Q(\alpha)$ and $\prod = \{\alpha,\beta,\gamma,\delta,\varepsilon,\eta\}$.

Let the composition $\theta^{''} \circ \theta^{'}$ mean the application of $\theta^{''}$ to the inverse operation defined θ', then $\theta^{''} \circ \theta^{'} = \theta \in \prod$ for all $\theta^{'}, \theta^{''} \in \prod$ (cf. [4, p. 14]).

In general a non-commutative quasigroup can have six pairwise different inverse operations. It is easy to check in general case $\alpha \circ \theta = \theta = \theta \circ \alpha$ for all $\theta \in \prod$ and $\alpha = \alpha\circ\alpha = \beta\circ\beta = \gamma\circ\gamma = \delta\circ\delta$, $\varepsilon\circ\varepsilon = \eta$, $\eta\circ\eta = \varepsilon$, $\varepsilon\circ(\varepsilon\circ\varepsilon) = \alpha = (\varepsilon\circ\varepsilon)\circ\varepsilon$, $\varepsilon^{-1} = \eta$, $\delta\circ\varepsilon = \beta = \gamma\circ\eta$, etc [4].

We can now construct the multiplication table of $(\prod,\circ)$, using the received formulas and an algorithm of [4]. This is Table 1 for a non-commutative quasigroup with six pairwise distinct parastrophes, and otherwise $(\prod,\circ)$ is isomorphic to a subgroup of the symmetric group S_3.

Each $\theta \in \prod$ defines the parastrophe $(Q,\theta) = Q(\theta)$ of a quasigroup $(Q,\odot) = Q(\alpha)$ and the parastrophy $(Q,\odot) = Q(\alpha) \xrightarrow{\theta} Q(\theta)$ as a mapping. An (ordered) sixtuple $\prod(Q(\alpha)) = (Q(\alpha), Q(\beta), Q(\gamma), Q(\delta), Q(\varepsilon), Q(\eta))$ is called a parastrophe system of the quasigroup $(Q,\odot) = Q(\alpha)$. The diagram

$$\begin{tikzcd}
(Q,\odot)=Q(\alpha) \arrow[rr, "\theta^{'}"] \arrow[dr, "\theta"'] & & Q(\theta^{'}) \arrow[dl, "\theta^{''}"] \\
& Q(\theta^{''}\circ\theta^{'}) &
\end{tikzcd}$$

of the action of parastrophies on the system $\prod(Q(\alpha))$ is commutative and $Q(\theta^{''}\circ\theta^{'}) = Q(\theta)$. So all parastrophs of the quasigroup $(Q,\odot) = Q(\alpha)$ form a group $(\prod,\cdot)$ relative to the action on the system $\prod(Q(\alpha))$. It is isomorphic to the group $(\prod,\circ)$.

Theorem 2. *The group $(\prod,\cdot)$ of parastrophies acting on $\prod(Q(\alpha))$ is isomorphic to the group $(\prod,\circ)$ relative to the composition of taking of inverse operations of the quasigroup $(Q,\odot) = Q(\alpha)$. Both these group are isomorphic to some subgroup of the symmetric group S_3. Table 1 serves as the multiplication table for a quasigroup with pairwise distinct parastrophes.*

$\cdot$	α	β	γ	δ	ε	η
α	α	β	γ	δ	ε	η
β	β	α	ε	η	γ	δ
γ	γ	η	α	ε	δ	β
δ	δ	ε	η	α	β	γ
ε	ε	δ	β	γ	η	α
η	η	γ	δ	β	α	ε

Table 1

Remark 1. We will denote the conjugation as $\beta\theta$ instead of θ^* using the second row $\beta\theta = \theta^*$, $\theta \in \Pi$, of the multiplication table.

In the paper [3] it is proved:

The action of an isotopy (φ, ψ, λ) on a quasigroup $(Q, \cdot) = Q(\alpha)$ induces identically an isotopy $\theta(\varphi, \psi, \lambda)$ on each $Q(\theta) \in \Pi(Q(\alpha))$.

The results of this action are presented by the following table:

$Q(\alpha)$	$Q(\beta)$	$Q(\gamma)$	$Q(\delta)$	$Q(\varepsilon)$	$Q(\eta)$
(φ, ψ, χ)	(ψ, φ, χ)	(φ, χ, ψ)	(χ, ψ, φ)	(χ, φ, ψ)	(ψ, χ, φ)

Table 2

We use the second table and also the natural commutative diagram for $\theta \in \Pi$:

$$\begin{array}{ccc} Q(\alpha) & \xrightarrow{\theta} & Q(\theta) \\ {\scriptstyle(\varphi,\psi,\chi)}\big\downarrow & & \big\downarrow{\scriptstyle(\lambda,\mu,\nu)} \\ Q(\alpha(\circ)) & \xrightarrow{\theta} & Q(\theta(\circ)) \end{array}$$

(where $(Q, \cdot) = Q(\alpha)$ and λ, μ, ν depend on θ) to derive six conditions of the permutability of the isotopy and parastrophy:

$\alpha(\varphi, \psi, \chi) = (\varphi, \psi, \chi)\alpha$	$\delta(\varphi, \psi, \chi) = (\chi, \psi, \varphi)\delta$
$\beta(\varphi, \psi, \chi) = (\psi, \varphi, \chi)\beta$	$\varepsilon(\varphi, \psi, \chi) = (\chi, \varphi, \psi)\varepsilon$
$\gamma(\varphi, \psi, \chi) = (\varphi, \chi, \psi)\gamma$	$\eta(\varphi, \psi, \chi) = (\psi, \chi, \varphi)\eta$

Table 3

The full multiplication table of the parastrophies and the isotopies of a quasigroup is the following:

$\cdot$	(φ, ψ, χ)	(ψ, φ, χ)	(φ, χ, ψ)	(χ, ψ, φ)	(χ, φ, ψ)	(ψ, χ, φ)
α	$(\varphi, \psi, \chi)\alpha$	$(\psi, \varphi, \chi)\alpha$	$(\varphi, \chi, \psi)\alpha$	$(\chi, \psi, \varphi)\alpha$	$(\chi, \varphi, \psi)\alpha$	$(\psi, \chi, \varphi)\alpha$
β	$(\psi, \varphi, \chi)\beta$	$(\varphi, \psi, \chi)\alpha$	$(\chi, \varphi, \psi)\varepsilon$	$(\psi, \chi, \varphi)\eta$	$(\varphi, \chi, \psi)\gamma$	$(\chi, \psi, \varphi)\delta$
γ	$(\varphi, \chi, \psi)\gamma$	$(\psi, \chi, \varphi)\eta$	$(\varphi, \psi, \chi)\alpha$	$(\chi, \varphi, \psi)\varepsilon$	$(\chi, \psi, \varphi)\delta$	$(\psi, \varphi, \chi)\beta$
δ	$(\chi, \psi, \varphi)\delta$	$(\chi, \varphi, \psi)\varepsilon$	$(\psi, \chi, \varphi)\eta$	$(\varphi, \psi, \chi)\alpha$	$(\psi, \varphi, \chi)\beta$	$(\varphi, \chi, \psi)\gamma$
ε	$(\chi, \varphi, \psi)\varepsilon$	$(\chi, \psi, \varphi)\delta$	$(\psi, \varphi, \chi)\beta$	$(\varphi, \chi, \psi)\gamma$	$(\psi, \chi, \varphi)\eta$	$(\varphi, \psi, \chi)\alpha$
η	$(\psi, \chi, \varphi)\eta$	$(\varphi, \chi, \psi)\gamma$	$(\chi, \psi, \varphi)\delta$	$(\psi, \varphi, \chi)\beta$	$(\varphi, \psi, \chi)\alpha$	$(\chi, \varphi, \psi)\varepsilon$

Table 4

Recall that each of the products of a parastrophy with an isotopy and of an isotopy with a parastrophy is called an isostrophy (see [2, p. 28]).

Corollary 2. *of the mappings. This group G is semi-direct S_P by S_Π i.e. G is isomorphic to the holomorph $HolS_3 = S_3 \cdot AutS_3$. Each quasigroup $(Q, \odot) = Q(\alpha)$ has no more than 36 pairwise different isostrophies. The number of these isostrophies depends on order of the group $(\Pi, \cdot)$.*

It follows from Theorem 2 and Table 4.

3. According to [2] two quasigroups $(Q, \cdot)$ and $(Q, \circ)$ are mutually orthogonal if and only if the system of the equations $xy = a$, $x \circ y = b$ is identically resolved for all $a, b \in Q$. In this case it is denoted $(Q, \cdot) \perp (Q, \circ)$ or $(Q, \circ) \perp (Q, \cdot)$.

In [2] V. D. Belousov investigated he question on orthogonality of a quasigroup to its parastrophes. In order to continue this idea we use another equivalent definition of orthogonality of quasigroups.

Proposition 1. $(Q, \cdot) \perp (Q, \circ)$ *is true if and only if at least one of two equations*

$$L_x^\circ L_x^{-1}(a) = b, \tag{L}$$

$$R_y^\circ R_y^{-1}(a) = b \tag{R}$$

is identically resolved for all $a, b \in Q$.

Theorem 3. *Let* $\Pi(Q(\alpha)) = (Q(\alpha), Q(\beta), Q(\gamma), Q(\delta), Q(\varepsilon), Q(\eta))$ *be the parastrophe system of a quasigroup* $(Q, \cdot) = Q(\alpha)$. *The following statements are valid:*

(i) $Q(\alpha) \perp Q(\gamma) \Leftrightarrow Q(\beta) \perp Q(\varepsilon) \Leftrightarrow$ *the equation* $L_x^2(b) = a$ *is identically resolved for all* $a, b \in Q$,

(ii) $Q(\alpha) \perp Q(\delta) \Leftrightarrow Q(\beta) \perp Q(\eta) \Leftrightarrow$ *the equation* $R_y^2(b) = a$ *is identically resolved for all* $a, b \in Q$,

(iii) $Q(\alpha) \perp Q(\beta) \Leftrightarrow$ *the equation* $L_x R_x^{-1}(b) = a$ *is identically resolved for all* $a, b \in Q$.

Proof. We use Proposition 1 and representation of parastrophes of a quasigroup $(Q, \cdot) = Q(\alpha)$ (see [1]).

(i) The equation (L) is fulfilled by $L_x^\circ = L_x^\gamma = L_x^{-1}$. It is also evident that $Q(\alpha) \perp Q(\gamma) \Leftrightarrow Q(\beta) \perp Q(\varepsilon)$ since the the equalities $Q(\beta\alpha) = Q(\beta)$ and $Q(\beta\gamma) = Q(\varepsilon)$ are true (see Table 1).

(ii) The equation (R) will be realized by $R_y^\circ = R_y^\delta = R_y^{-1}$. It is also evident that $Q(\alpha) \perp Q(\delta) \Leftrightarrow Q(\beta) \perp Q(\eta)$ since the equalities $Q(\beta\alpha) = Q(\beta)$ and $Q(\beta\delta) = Q(\eta)$ are true (see Table 1).

(iii) The equation (L) will be fulfilled by $L_x^0 = L_x^\beta = R_x$. □

Corollary 3. *Let* $(Q, \cdot)$ *be a finite quasigroup. At least one from the conditions* $(i), (ii), (iii)$ *of Theorem 3 is broken if some permutation from* $L_x^2, R_y^2, L_x R_x^{-1}$ *contains a transposition* (a, b), $a, b \in Q$.

Example 1. The left translations $L_1 = (1)$, $L_2 = (12)(345)$, $L_3 = (13524)$, $L_4 = (14325)$, $L_5 = (15423)$ define a loop $(Q, \cdot)$ of order five. $(Q, \cdot) = Q(\alpha)$ is non-orthogonal to $Q(\gamma), Q(\delta)$ and $Q(\beta)$ since $L_2 = R_2 = (12)(345)$.

There are some addifional conditions for a quasigroup by which it is orthogonal to some its parastrophes. Such identities are investigated in [2] where seven minimal identities are determined. We use below some of these identities to prove Theorem 3:

Conditions of Theorem 3	Supplimentary identities	Reorganized conditions of Theorem 3
$(i)\ L_x^2(b) = a$	$(x \cdot xy)x = y$	$R_x^{-1}(b) = a$
	$x(x \cdot xy) = y$	$L_x^{-1}(b) = a$
$(ii)\ R_y^2(b) = a$	$(xy \cdot y)y = x$	$R_y^{-1}(b) = a$
	$y(xy \cdot y) = x$	$L_y^{-1}(b) = a$
$(iii)\ L_x R_x^{-1}(b) = a$	$x \cdot xy = yx$	$L_x^{-1}(b) = a$

Table 5

It should be noted that there exist quasigroups which are orthogonal to some their parastrophes and non-parastrophes.

Example 2. A finite cyclic group $(Q, \cdot) = Q(\alpha)$ has only two parastrophes $Q(\gamma)$ and $Q(\delta)$. By Theorem 3 $Q(\alpha) \perp Q(\gamma)$ and $Q(\alpha) \perp Q(\delta)$ if $CardQ > 2$ is an odd number.

Moreover a quasigroup may exist a non-parastrophe $(Q, \circ)$ of which is orthogonal to the group $Q(\alpha)$. This situation is demonstrated by the following 3×3-Latin squares:

$$[\alpha] = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}, \quad [\gamma] = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}, \quad [\delta] = \begin{bmatrix} 1 & 3 & 2 \\ 2 & 1 & 3 \\ 3 & 2 & 1 \end{bmatrix},$$

$$[\circ] = \begin{bmatrix} 2 & 3 & 1 \\ 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}, \quad [\alpha, \circ] = \begin{bmatrix} 12 & 23 & 31 \\ 21 & 32 & 13 \\ 33 & 11 & 22 \end{bmatrix},$$

Table 6

where $[\alpha] \perp [\gamma]$, $[\alpha] \perp [\delta]$ and $[\alpha] \perp [\circ]$.

Acknowledge. I wish to thank prof. Yu. Rogozhin and Prof. M. Glukhov for their very useful notes, advice and support.

References

[1] Belousov V. D. *On an associated group of a quasigroup.* Matematiceskie issledovania, Academia Nauk Moldavskoi SSR, 1969, **4**, No. 3, 27–39 (in Russian).

[2] Belousov V. D. *Parastrophic-orthogonal quasigroups.* Quasigroups and Related Systems, 2005, **13**, No. 1, 25–72.

[3] Shchukin K. K., Gushan V. V. *Representation of parastrophes of loops and quasigroups.* Discrete Mathematics, 2004, **16**, No. 4, 149–157 (in Russian).

[4] Belousov V. D. *Elements of the theory of quasigroups.* (A special course for students), Kishinev, 1983 (in Russian).

Shchukin Krasarm
p/o MD-2043, box 1415
Chisinau, Moldova
E-mail: *Krasarm@newmail.ru*

Received March 18, 2010