Quasigroups and Related Systems **16** (2008), 17 − 24

On middle translations of finite quasigroups

Ivan I. Deriyenko

Abstract

We prove that a finite quasigroup is isotopic to a group if and only if some set of bijections induced by middle transformations of this quasigroup is a group.

1. Introduction

Let $Q = \{1, 2, 3, \ldots, n\}$ be a finite set, φ and ψ permutations of Q. The multiplication (composition) of permutations is defined as $\varphi\psi(x) = \varphi(\psi(x))$.

Let $Q(\cdot)$ be a quasigroup. Permutations $L_a : x \to a \cdot x$, $R_a : x \to x \cdot a$ are called *left* and *right translations* of $Q(\cdot)$. Permutations λ_i, φ_i $(i \in Q)$ of Q such that

$$\lambda_i(x) \cdot x = i, \tag{1}$$

$$x \cdot \varphi_i(x) = i \tag{2}$$

for all $x \in Q$, are called *left* (respectively: *right*) *middle translations* of an element i in a quasigroup $Q(\cdot)$. Such translation were firstly studied by V. D. Belousov (cf. [1]) in connection with some groups associated with quasigroups. Next, the investigations of such translations were continued by many authors, see for example [3] or [5].

The above two conditions say that in a Latin square $n \times n$ connected with a quasigroup $Q(\cdot)$ of order n we select n cells, one in each row, one in each column, containing the same fixed element i. $\lambda_i(x)$ means that to find in the column x the cell containing an element i we must select the row $\lambda_i(x)$. Analogously, $\varphi_i(x)$ means that to find in the row x the cell containing i we must select the column $\varphi_i(x)$. Thus, λ_i is a selection of

2000 Mathematics Subject Classification: 05B15; 20N05
Keywords: Quasigroup, loop, group, isotopy, translation

rows, φ_i – a selection of columns, containing an element i. In connection with this fact λ_i will be called a *left track* (*l-track*), φ_i - a *right track* (*r-track*) of an element i. It is clear that for a quasigroup $Q(\cdot)$ of order n the set $\{\lambda_1, \lambda_2, \dots, \lambda_n\}$ uniquely determines its Latin square, and conversely, any Latin square $n \times n$ uniquely determines the set $\{\lambda_1, \lambda_2, \dots, \lambda_n\}$. A similar situation holds for $\{\varphi_1, \varphi_2, \dots, \varphi_n\}$.

More interesting facts on connections of translations with Latin squares one can find in [2].

As a simple consequence of the above definitions we obtain

Proposition 1.1. *In any quasigroup $Q(\cdot)$ the following identities hold:*

1) $\lambda_i = \varphi_i^{-1}$,

2) $\varphi_i^{-1}(x) \cdot x = i$,

3) $L_i(x) = (\lambda_i(x) \cdot x) \cdot x$,

4) $L_i(x) = (x \cdot \varphi_i(x)) \cdot x$,

5) $R_i(x) = x \cdot (\lambda_i(x) \cdot x)$,

6) $R_i(x) = x \cdot (x \cdot \varphi_i(x))$. □

Corollary 1.2. *In any group $G(\cdot)$ we have*

1) $\varphi_i(x) = x^{-1} \cdot i, \quad \lambda_i(x) = i \cdot x^{-1}$,

2) $\varphi_1(x) = \lambda_1(x) = x^{-1}$,

3) $L_i(x) = \lambda_i(x) \cdot x^2$,

4) $R_i(x) = x^2 \cdot \varphi_i(x)$,

where 1 *is the identity element of the group $G(\cdot)$.* □

2. Isotopy invariants in quasigroups

Two quasigroups $Q(\cdot)$ and $Q(\circ)$ are *isotopic* if there exists an ordered triple $T = (\alpha, \beta, \gamma)$ of bijections $\alpha, \beta, \gamma : Q \to Q$ such that

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

for all $x, y \in Q$.

For $y = \psi_i(x)$, where ψ_i is a r-track of a quasigroup $Q(\circ)$, this identity has the form

$$\gamma(x \circ \psi_i(x)) = \alpha(x) \cdot \beta\psi_i(x),$$

whence, according to (2), we obtain

$$\gamma(i) = \alpha(x) \cdot \beta\psi_i(x).$$

This for $z = \alpha(x)$ and $j = \gamma(i)$ gives

$$j = z \cdot \beta\psi_i\alpha^{-1}(z).$$

Since

$$j = z \cdot \varphi_j(z) = z \cdot \varphi_{\gamma(i)}(z)$$

for r-tracks φ_j and $\varphi_{\gamma(i)}$ of a quasigroup $Q(\cdot)$, the above implies

$$\varphi_{\gamma(i)} = \beta\psi_i\alpha^{-1}. \tag{3}$$

Remark 2.1. For l-tracks λ_i and μ_i of isotopic quasigroups $Q(\cdot)$ and $Q(\circ)$ we have

$$\lambda_{\gamma(i)} = \alpha\mu_i\beta^{-1}. \tag{4}$$

Definition 2.2. By a *spin* of a quasigroup $Q(\cdot)$ we mean the permutation

$$\varphi_{ij} = \varphi_i\varphi_j^{-1} = \varphi_i\lambda_j,$$

where φ_i and λ_j are tracks of $Q(\cdot)$. The spin φ_{ii} is called trivial.

The set of all spins of a quasigroup $Q(\cdot)$ is denoted by $\Phi_Q(\cdot)$.

Proposition 2.3. *Spins have the following properties*

1) $\varphi_{ij}(x) \neq x$ *for all* $x \in Q$ *and* $i \neq j$,

2) $\varphi_{pi}(x) \neq \varphi_{pj}(x)$ *for all* $x \in Q$ *and* $i \neq j$,

3) $\varphi_{ij} = \varphi_{ji}^{-1}$,

4) $\varphi_{ki}\varphi_{il} = \varphi_{kl}$,

5) $\varphi_{mk} = \varphi_{im}^{-1}\varphi_{ik}$.

Proof. (1) If $\varphi_{ij}(x) = x$ holds for some $i \neq j$ and $x \in Q$, then, according to the definition of φ_{ij}, we have $\varphi_i\varphi_j^{-1}(x) = x$. Whence, for $x = \varphi_j(y)$, we obtain $\varphi_i(y) = \varphi_j(y)$. Consequently $y \cdot \varphi_i(y) = y \cdot \varphi_j(y)$, i.e., $i = j$. This contradicts our assumption. So, $\varphi_{ij}(x) \neq x$ for all $x \in Q$ and $i \neq j$.

(2) Analogously as (1).

(3) $\varphi_{ij} = \varphi_i\varphi_j^{-1} = (\varphi_j\varphi_i^{-1})^{-1} = \varphi_{ji}^{-1}$.

(4) $\varphi_{ki}\varphi_{il} = (\varphi_k\varphi_i^{-1})(\varphi_i\varphi_l^{-1}) = \varphi_k(\varphi_i^{-1}\varphi_i)\varphi_l^{-1} = \varphi_{kl}$.

(5) $\varphi_{mk} = \varphi_m\varphi_k^{-1} = \varphi_m\varphi_i^{-1}\varphi_i\varphi_k^{-1} = (\varphi_i\varphi_m^{-1})^{-1}(\varphi_i\varphi_k^{-1}) = \varphi_{im}^{-1}\varphi_{ik}$. □

As it is well-known any permutation φ of the set Q of order n can be decomposed into $r \leqslant n$ cycles of the length $k_1, \ldots, k_r$ and $k_1 + \ldots + k_r = n$. We denote this fact by

$$Z(\varphi) = [k_1, k_2, \ldots, k_r]\,.$$

Since conjugate permutations are decomposable into cycles of the same length (see for example [4]), for any two conjugate permutations φ and ψ we have $Z(\varphi) = Z(\psi)$. Obviously $Z(\varphi) = Z(\varphi^{-1})$ for any permutation φ. So, $Z(\varphi_{ij}) = Z(\varphi_{ji})$ for all spins.

Definition 2.4. Let $\Phi = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ be a collection of permutations of the set Q. The set

$$Sp(\Phi) = [Z(\varphi_1), Z(\varphi_2), \ldots, Z(\varphi_n)]$$

is called the *spectrum* of Φ.

Two collections $\Phi = \{\varphi_1, \varphi_2, \ldots, \varphi_n\}$ and $\Sigma = \{\sigma_1, \sigma_2, \ldots, \sigma_n\}$ of permutations of Q have the same spectrum if and only if there exists a permutation γ of Q such that $Z(\varphi_i) = Z(\sigma_{\gamma(i)})$ for all $i = 1, 2, \ldots, n$.

The spectrum of all spins of a quasigroup $Q(\cdot)$, i.e., the set

$$[Z(\varphi_{11}), Z(\varphi_{12}), \ldots, Z(\varphi_{nn})]$$

is called the *spin-spectrum* of $Q(\cdot)$ and is denoted by $Ssp(Q, \cdot)$.

Theorem 2.5. *Finite isotopic quasigroups have the same spin-spectrum.*

Proof. Let $Q(\cdot)$ and $Q(\circ)$ be isotopic quasigroups. Then

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

for some permutations α, β, γ of Q.

In this case tracks of $Q(\cdot)$ and $Q(\circ)$ are connected by the formula (3). Spins of $Q(\cdot)$ and $Q(\circ)$ are pairwise conjugate. Namely

$$\varphi_{\gamma(i)\gamma(j)} = \beta\psi_{ij}\beta^{-1}.$$

Indeed,

$$\begin{aligned}\varphi_{\gamma(i)\gamma(j)} &= \varphi_{\gamma(i)}\varphi^{-1}_{\gamma(j)} = (\beta\psi_i\alpha^{-1})(\beta\psi_j\alpha^{-1})^{-1} \\ &= (\beta\psi_i\alpha^{-1})(\alpha\psi_j^{-1}\beta^{-1}) = \beta\psi_i\psi_j^{-1}\beta^{-1} = \beta\psi_{ij}\beta^{-1}.\end{aligned}$$

Since spins $\varphi_{\gamma(i)\gamma(j)}$ and ψ_{ij} are conjugate, we have $Z\left(\varphi_{\gamma(i)\gamma(j)}\right) = Z(\psi_{ij})$. This means that $Q(\cdot)$ and $Q(\circ)$ have the same spin-spectrum. □

Corollary 2.6. *If the isotopy of quasigroups $Q(\cdot)$ and $Q(\circ)$ has the form (α, α, γ), then also sets of all r-tracks (l-tracks) of these quasigroups have the same spectrum.*

Proof. Indeed, from (3) and (4), it follows that in this case l-tracks (respectively, r-tracks) of these quasigroups are pairwise conjugate. □

3. Spin-basis of quasigroups

Definition 3.1. Let Φ be a collection of all nontrivial spins of a quasigroup $Q(\cdot)$. A minimal subset B of Φ is called a *basis* of Φ if each spin from Φ can be written as a multiplication of spins (and their inverses) from B.

For example, the set

$$B_0 = \{\varphi_{12}, \varphi_{23}, \dots, \varphi_{i(i+1)}, \dots, \varphi_{(n-1)n}\}$$

containing $(n-1)$ spins is a basis since each spin φ_{pq}, where $p < q$, can be written in the form

$$\begin{aligned}\varphi_{pq} &= \varphi_p\varphi_q^{-1} = \varphi_p(\varphi^{-1}_{p+1}\varphi_{p+1}\varphi^{-1}_{p+2}\varphi_{p+2}\cdots\varphi^{-1}_{q-1}\varphi_{q-1})\varphi_q^{-1} \\ &= (\varphi_p\varphi^{-1}_{p+1})(\varphi_{p+1}\varphi^{-1}_{p+2})\dots(\varphi_{q-1}\varphi_q^{-1}) = \varphi_{p(p+1)}\varphi_{(p+1)(p+2)}\cdots\varphi_{(q-1)q}.\end{aligned}$$

Also

$$B_i = \{\varphi_{i1}, \varphi_{i2}, \dots, \varphi_{ik}, \dots, \varphi_{in}\}, \quad i \neq k,$$

is a basis for every $i = 1, 2, \dots, n$. Indeed, according to Proposition 2.3 (5), each spin φ_{pq} can be written in the form

$$\varphi_{pq} = \varphi^{-1}_{ip}\varphi_{iq}.$$

Definition 3.2. Let $Q(\cdot)$ be a quasigroup of order n. The set

$$\chi_i(Q,\cdot) = \{\varphi_{i1}, \varphi_{i2}, \dots, \varphi_{ii}, \dots, \varphi_{in}\} = B_i \cup \{\varphi_{ii}\}$$

is called the *ith spin-basis* of $Q(\cdot)$.

It coincides with the ith row of the matrix $[\varphi_{ij}]$. In general, it is not closed under multiplication of spins, but in some cases it is a group. Since $\varphi_{ki}\varphi_{ij} = \varphi_{kj}$, by Proposition 2.3, for all $i, k = 1, 2, \dots, n$ holds

$$\varphi_{ki}(\chi_i(Q,\cdot)) = \chi_k(Q,\cdot).$$

Proposition 3.3. *If one of the spin-basis of a quasigroup $Q(\cdot)$ is a group, then each of its spin-basis is a group and*

$$\chi_1(Q,\cdot) = \chi_2(Q,\cdot) = \ldots = \chi_n(Q,\cdot).$$

Proof. Let $\chi_i(Q,\cdot)$ be a group. Then $\chi_i(Q,\cdot)$ together with φ_{ik} contains also $\varphi_{ik}^{-1} = \varphi_{ki}$. This means that $\{\varphi_{1i}, \varphi_{2i}, \dots, \varphi_{ni}\} \subseteq \chi_i(Q,\cdot)$. Therefore each spin φ_{kj} belongs to $\chi_i(G,\cdot)$ because $\varphi_{kj} = \varphi_{ki}\varphi_{ij} \in \chi_i(G,\cdot)$ for all j, k. So, $\chi_k(Q,\cdot) \subseteq \chi_i(Q,\cdot)$ and $\varphi_{ki}(\chi_i(Q,\cdot)) = \chi_k(Q,\cdot)$ which completes the proof. $\square$

Proposition 3.4. *Let quasigroups $Q(\cdot)$ and $Q(\circ)$ be isotopic. If one spin-basis of $Q(\cdot)$ is a group, then each spin-basis of $Q(\circ)$ is a group and for all $i = 1, \dots, n$ we have $\chi_i(Q,\cdot) \cong \chi_i(Q,\circ)$.*

Proof. Let $\gamma(x \circ y) = \alpha(x) \cdot \beta(y)$. Then, as in the proof of Theorem 2.5,

$$\varphi_{\gamma(i)\gamma(j)} = \beta\psi_{ij}\beta^{-1}.$$

Whence

$$\psi_{ij} = \beta^{-1}\varphi_{\gamma(i)\gamma(j)}\beta. \tag{5}$$

To prove that

$$\chi_i(G,\circ) = \{\psi_{i1}, \psi_{i2}, \dots, \psi_{in}\}$$

is a group observe that for all $\psi_{ip}, \psi_{iq} \in \chi_i(Q,\circ)$ we have

$$\psi_{ip}\psi_{iq} = \beta^{-1}\varphi_{\gamma(i)\gamma(p)}\varphi_{\gamma(i)\gamma(q)}\beta = \beta^{-1}\varphi_{\gamma(i)k}\beta = \psi_{it},$$

where $\gamma(t) = k$, since, by Proposition 3.3, each spin-basis of $Q(\cdot)$ is a group. Moreover, for every $\psi_{ik} \in \chi_i(Q,\circ)$, by (5) and Proposition 2.3, we obtain

$$\psi_{ik}^{-1} = \psi_{ki} = \beta^{-1}\varphi_{\gamma(k)\gamma(i)}\beta = \beta^{-1}\varphi_{\gamma(i)\gamma(k)}^{-1}\beta = \beta^{-1}\varphi_{\gamma(i)r}\beta = \psi_{is},$$

where $\gamma(s) = r$. This means that $\chi_i(Q, \circ)$ together with ψ_{ik} also contains ψ_{ik}^{-1}. So, it is a group. Clearly $\chi_i(Q, \circ) = \chi_k(Q, \circ)$ for all $k = 1, \dots, n$.

In view of (5) the isomorphism $h : \chi_{\gamma(i)}(Q, \cdot) \to \chi_i(Q, \circ) = \chi_{\gamma(i)}(Q, \circ)$ has the form $h(\varphi_{\gamma(i)\gamma(j)}) = \beta^{-1}\varphi_{\gamma(i)\gamma(j)}\beta$. □

Theorem 3.5. *A finite quasigroup which is a group is isomorphic to its spin-basis.*

Proof. Let $G(\cdot)$ be a group and $\chi_1(G, \cdot) = \{\varphi_{11}, \varphi_{12}, \dots, \varphi_{1n}\}$ its spin-basis. Then, according to the definition of spins, Proposition 1.1 and Corollary 1.2,

$$\varphi_{1i}(x) = \varphi_1(\lambda_i(x)) = \varphi_1(i \cdot x^{-1}) = (i \cdot x^{-1})^{-1} = x \cdot i^{-1} = R_{i^{-1}}(x),$$

which means that the spin-basis $\chi_1(G, \cdot)$ can be identified with the set of all right translations of $G(\cdot)$. So, $\chi_1(G, \cdot)$ and $G(\cdot)$ are isomorphic.

Proposition 3.3 completes the proof. □

Theorem 3.6. *A quasigroup for which the spin-basis is a group is isotopic to this group.*

Proof. Let $Q(\circ)$ be a quasigroup. Since it is isotopic to some loop $Q(\cdot)$ with the identity 1, in view of Propositions 3.3 and 3.4, it is sufficient to prove that $Q(\cdot)$ is isotopic to the group $\chi_1(Q, \cdot) = \{\varphi_{11}, \varphi_{12}, \varphi_{13}, \dots, \varphi_{1n}\}$.

For this we consider the mapping

$$h : \chi_1(Q, \cdot) \longrightarrow Q(\cdot) \quad \text{such that} \quad h(\varphi_{1i}) = i.$$

It is one-to-one and onto. We prove that it is an isomorphism, i.e.,

$$h(\varphi_{1k}\varphi_{1l}) = h(\varphi_{1k}) \cdot h(\varphi_{1l})$$

for all φ_{1k}, φ_{1l} from $\chi_i(Q, \cdot)$.

As $\chi_1(Q, \cdot)$ is a group, the product of φ_{1k} and φ_{1l} also belongs to $\chi_1(Q, \cdot)$. Let

$$\varphi_{1k}\varphi_{1l} = \varphi_{1p}.$$

By the definition of spins, the last equality is equivalent to

$$\varphi_1\varphi_k^{-1}\varphi_1\varphi_l^{-1} = \varphi_1\varphi_p^{-1},$$

i.e., to

$$\varphi_k^{-1}\varphi_1\varphi_l^{-1} = \varphi_p^{-1}$$

which can be written as
$$\varphi_p = \varphi_l \varphi_1^{-1} \varphi_k.$$
This means that
$$\varphi_p(x) = \varphi_l \varphi_1^{-1} \varphi_k(x)$$
holds for every $x \in Q$. Since $Q(\cdot)$ is a loop, the last identity is equivalent to
$$x \cdot \varphi_p(x) = x \cdot \varphi_l \varphi_1^{-1} \varphi_k(x),$$
whence, by (2), for $x = k$ we obtain
$$p = k \cdot \varphi_p(k) = k \cdot \varphi_l \varphi_1^{-1} \varphi_k(k) = k \cdot \varphi_l \varphi_1^{-1}(1) = k \cdot \varphi_l(1) = k \cdot l$$
because in any loop $\varphi_k(k) = 1$ and $\varphi_k(1) = k$.

So, $h(\varphi_{1k}\varphi_{1l}) = p = k \cdot l = h(\varphi_{1k}) \cdot h(\varphi_{1l})$, which completes the proof. □

As a consequence of the above results we obtain

Theorem 3.7. *A finite quasigroup is isotopic to a group if and only if its spin-basis is a group.*

References

[1] **V. D. Belousov**: *On group associated with a quasigroup* (Russian), Mat. Issled. **4** (1969), no. 3, 21 − 39.

[2] **J. Dénes and A. D. Keedwell**: *Latin squares and their applications*, Akadémiai Kiadó, Budapest, 1974.

[3] **I. I. Deriyenko** (Derienko): *Necessary conditions of the isotopy of finite quasigroups*, (Russian) Mat. Issled. **120** (1991), 51 − 63.

[4] **M. Hall**: *The theory of groups*, Macmillan, 1959.

[5] **V. A. Shcherbacov**: *Some properties of full associated group of IP-loop*, (Russian), Izvestia AN Mold. SSR. Ser. fiz.-techn. i mat. nauk **2** (1984), 51−52.

Received February 12, 2008

Kremenchuk State Polytechnical University
Pervomayskaya 20
39600 Kremenchuk
Ukraine
E-mail: ivan.deriyenko@gmail.com