Quasigroups and related systems, vol.**1**, no.1(1), 1994

ABELIAN QUASIGROUPS ARE *T*-QUASIGROUPS

Galina B. Belyavskaya

Abstract

By means of known results with respect to algebras of a congruence modular variety it is proved that abelian (in the sense of McKenzie) quasigroups, i.e. quasigroups coinciding with their centre, are T-quasigroups and conversely.

In the literature on quasigroups it was accepted medial quasigroups to call abelian quasigroups. However, the latest investigations of the centre of quasigroups show that the class of abelian (in the sense of McKenzie [1]) quasigroups is the class of T-quasigroups introduced and thoroughly studied in [2,3] and including medial quasigroups.

In this note we shall prove this fact by means of known results with respect to algebras of modular varieties.

Let A be an universal algebra. According to the definition from [1,4] the *centre of A* is the set $Z(A)$ of all pairs $(a,b)\in A^2$ such that for each term operation $t(x,y_1,\dots,y_n)$ of A, each $\bar{u},\bar{v}\in A^n$:

$$t(a,\bar{u})=t(a,\bar{v})\Leftrightarrow t(b,\bar{u})=t(b,\bar{v}).$$

The centre $Z(A)$ is a congruence on A.

An algebra A is called *abelian* if $Z(A)=A^2$.

In [5,6] the concept of the h-centre Z_h, $h\in Q$, of a quasigroup $Q(\cdot)$ was introduced and studied. Z_h is a normal subset of $Q(\cdot)$ and defines the normal congruence $\theta_Z(\cdot)$. It was proved that if Z_h forms a subquasigroup of $Q(\cdot)$, then this subquasigroup is a T-quasigroup [5,6], and each T-quasigroup $Q(\cdot)$ coincides with its h-centre ($Z_h=Q$) for each $h\in Q$.

In [7] it was proved that $\theta_Z=Z(Q)$ where $Z(Q)$ is the centre of the corresponding primitive quasigroup $Q(\cdot,\backslash,/)$. These results mean that the definition of Z_h is an inner characterization of the centre $Z(Q)$. It also implies that in the variety of all primitive quasigroups the abelian quasigroups are

T-quasigroups, and conversely. It is a long way to prove this. The aim of this note is to prove directly that a primitive quasigroup $Q(\cdot,\backslash,/)$ is abelian if and only if it is a T-quasigroup by means of known results on universal algebras of a congruence modular (shortly, modular) variety. To prove this we need a number of necessary concepts and results with respect to algebras of modular varieties.

First we remind that if an algebra A lies in a modular variety, then its centre can be characterized by means of a commutator of congruences. For the first time the theory of commutators and the centre was given for universal algebras of permutable (or Mal'cev) varieties and thoroughly studied by J.D.H.Smith in [8]. Later this theory was developed by many authors in algebras of modular varieties. In [9] J.D.H.Smith called a quasigroup $Q(\cdot,\backslash,/)$ coinciding with its centre (i.e.an abelian primitive quasigroup in the sense of McKenzie) a $\mathfrak{Z}$-quasigroup.

Let α,β be congruences on an algebra A of a modular variety ($\alpha,\beta \in \mathrm{Con}A$). According to [10] define the congruence Δ_α^β on α by

$$\Delta_\alpha^\beta = <((a,a),(b,b)) | (a,b) \in \beta >_\alpha,$$

i.e. Δ_α^β is the congruence generated in α (viewed as a subalgebra of $A \times A$). In other words, Δ_α^β is the smallest congruence relation on α containing the set $\{((a,a),(b,b)) | (a,b) \in \beta\}$.

The *commutator* $[\alpha,\beta]$ of two congruences α,β on A is defined as follows:

$$[\alpha,\beta] = \{(x,y) | (x,x)\Delta_\alpha^\beta(x,y)\}.$$

A congruence θ on an algebra A of a congruence modular variety is called *central* if $[\theta, A^2] = 0_A$, where

$$0_A = \{(a,a) | a \in A\}.$$

In this case the centre $Z(A)$ is exactly the largest central congruence on A ([1], **Lemma 5.2**). Hence, an algebra A of a modular variety is abelian iff $[A^2, A^2] = 0_A$.

All abelian algebras in a modular variety form a subvariety. A variety is called abelian if every algebra of this variety is abelian.

According to **Definition 5.3** [1] a congruence α on A is called *abelian* if $[\alpha,\alpha] = 0_A$. It is evident that each central congruence is abelian since

$$[\alpha,\alpha] \le [\alpha, Q^2] = 0_A$$

implies

$$[\alpha,\alpha] = 0_A.$$

Let f be a n-ary term operation of an algebra A,

$$\overline{x} = x_1^n, \overline{y} = y_1^n, \overline{z} = z_1^n \in A^n,$$

and

$$f(\overline{x} - \overline{y} + \overline{z}) = f(x_1 - y_1 + z_1, x_2 - y_2 + z_2, \ldots, x_n - y_n + z_n).$$

Definition 1[1]. An algebra A of a modular variety is called *affine* if there is an abelian group $\overline{A} = < A, +, - >$ having the same universe as A, and a 3-ary term operation $t(x,y,z)$ on A, such that:

1) $t(x,y,z) = x - y + z$ for all $x,y,z \in A$;

2) $f(\overline{x} - \overline{y} + \overline{z}) = f(\overline{x}) - f(\overline{y}) + f(\overline{z})$

for each n-ary term operation f and $\overline{x}, \overline{y}, \overline{z} \in A^n$.

The condition **2)** is equivalent to the following statement:

each operation (and each term operation) of the algebra A is affine with respect to the group $\overline{A}$, i.e. for any given n-ary operation F there are endomorphisms $\alpha_1, \alpha_2, \ldots, \alpha_n$ of $\overline{A}$ and an element $a \in A$ such that

$$F(x_1^n) = \sum_{i=1}^{n} \alpha_i x_i + a$$

(see [1], p.46).

According to **Corollary 5.9** [1] in a modular variety every abelian algebra is affine, and conversely.

We also need the following result due to C.Herrmann [11] (see also **Theorem 3.4** [12]).

Theorem 1 [11]. *If $\mathfrak{R}$ is a modular variety, then there exists a term $p(x,y,z)$ such that for each algebra $A \in \mathfrak{R}$, each abelian $\alpha \in ConA$, each $a \in A$ on the α-class d / α containing the element d, operations "+,-" of an abelian group are defined such that for all $a,b,c \in d / \alpha$:*

$$p(a,b,c) = a - b + c,$$

and for each signature n-ary operation for all $\overline{a}, \overline{b}, \overline{c} \in A^n$ such that for $i \leq n$ a_i, b_i, c_i are α-equivalent, the equality

$$f(\overline{a} + \overline{b} - \overline{c}) = f(\overline{a}) + f(\overline{b}) - f(\overline{c})$$

holds.

From **Theorem 1, Definition 1** and **Corollary 5.9** [1] it follows

Corollary 1. *Let* α *be an abelian congruence of an algebra* A *of a modular variety and the* α*-class* d/α *forms a subalgebra of* A *for some* $d \in A$. *Then this subalgebra is affine and so an abelian algebra.*

At last, we remind that the primitive quasigroup is an algebra $Q(\cdot,\backslash,/)$ with three binary operations which satisfy the laws:

$$x(x\backslash y)=y,\ (x/y)y=x,\ x\backslash(xy)=y,\ (xy)/y=x.$$

It is known that the class of all primitive quasigroups forms a permutable (and thus a modular) variety.

A quasigroup $Q(\cdot)$ is called a T*-quasigroup* [2,3], if there exist an abelian group $Q(+)$, its automorphosms α,β and an element $a \in Q$ such that

$$xy=\alpha x+\beta y+a$$

for all $x,y \in Q$.

Medial quasigroups are a special case of T-quasigroups when the automorphisms α and β commute.

Now we can easy prove for quasigroups the following

Lemma. *Let* α *be an abelian congruence on a quasigroup* $Q(\cdot,\backslash,/)$ *and a* α*-class* H *be a subquasigroup of* $Q(\cdot,\backslash,/)$. *Then* H *is a T-quasigroup.*

Proof. By **Corollary 1** $H(\cdot,\backslash,/)$ is an affine quasigroup so

$$xy=\alpha x+\beta y+a,$$

where α,β are endomorphisms of the abelian group $(H,+,-)$. Put $x=0$ (0 is the zero of $Q(+)$), then

$$0y=\beta y+a.$$

Hence β is a permutation on Q since $Q(\cdot)$ is a quasigroup. Analogously, α is a permutation on Q. Hence, $H(\cdot)$ is a T-quasigroup.

Note that according to **Lemma 33** [3], if $Q(\cdot)$ is a T-quasigroup and

$$xy=\alpha x+\beta y+a$$

where $\alpha,\beta \in AutQ(+)$, $Q(+)$ is an abelian group, then

$$x\backslash y=-\beta^{-1}\alpha x+\beta^{-1}y-\beta^{-1}a,$$

$$x/y=\alpha^{-1}x-\alpha^{-1}\beta y-\alpha^{-1}a,$$

i.e. $Q(\backslash)$ and $Q(/)$ are also T-quasigroups.

Theorem 2. *A quasigroup* $Q(\cdot,\backslash,/)$ *is abelian if and only if it is a T-quasigroup.*

Proof. If $Q(\cdot,\backslash,/)$ is abelian, then $[Q^2,Q^2]=0$ and by **Lemma** $Q(\cdot,\backslash,/)$ is a T-quasigroup.

Conversely, let $Q(\cdot,\backslash,/)$ be a T-quasigroup:

$$xy=\alpha x+\beta y+a \tag{1}$$

Prove that $Q(\cdot,\backslash,/)$ is affine. For this consider the Mal'cev term

$$t(x,b,y)=(x/(b\backslash b))\cdot(b\backslash y)$$

for $Q(\cdot,\backslash,/)$, i.e.

$$t(x,b,y)=R_{e_b}^{-1}x\cdot L_b^{-1}y, \tag{2}$$

(here

$$be_b=b,\quad R_{e_b}x=xe_b,\quad L_bx=bx),$$

since

$$b\backslash b=e_b,\quad x/e_b=R_{e_b}^{-1}x,\quad b\backslash y=L_b^{-1}y.$$

From (2) it follows that $t(x,b,y)$ is a loop with the identity element $be_b=b$. But (1) means that the abelian group $Q(+)$ is principally isotopic to the quasigroup $Q(\cdot)$ so according to **Albert's Theorem** the loop $t(x,b,y)$ is an abelian group isomorphic to $Q(+)$. Moreover, from the proof of **Albert's Theorem** (see [13, p. 17]) it follows that

$$t(x,b,y)=x-b+y$$

since the loop $t(x,b,y)$ is principally isotopic to $Q(+)$. Therefore the condition **1)** from the definition of an affine algebra holds.

The condition **2)** is also true since it is equivalent to the fact that each of the operations $(\cdot)$, $(/)$ and $(\backslash)$ has the form

$$f(x,y)=\alpha x+\beta y+a,$$

where α,β are some endomorphisms of the same abelian group $Q(+)$. This completes the proof.

Corollary 2. *If $Q(\cdot,\backslash,/)$ is a T-quasigroup, then $[\alpha,\beta]=0$ for all congruences α, β of $Q(\cdot,\backslash,/)$.*

Indeed, $[\alpha,\beta]\le[Q^2,Q^2]=0$.

Now we can note that primitive T-quasigroups as abelian algebras of a modular variety have all properties established with respect to these algebras. Many of such properties can be found in [2] in addition to the properties of the T-quasigroups from [2,3,5,6].

In conclusion remark that if we take some variety of primitive quasigroups, then the abelian quasigroups can be a special case of T-quasigroups. For example, according to **Theorem 7** [6] the abelian quasigroups in the variety of all idempotent quasigroups are medial distributive quasigroups, and in the variety of all commutative quasigroups the abelian quasigroups are medial (commutative) quasigroups (**Corollary 6** [6]).

References

1. *Freese R., McKenzie R.* Commutator Theory for Congruence Modular Varieties. London Math. Soc. Lecture Note, Ser. **125**, 1987.

2. *Kepka T., Němec P.* T-quasigroups. Part 1. Acta Universitatis Carolinae Math. et Physica, v.**12**(1971)., No 1, p.39-49.

3. *Kepka T., Němec P* . T-quasigroups. Part 2. Acta Universitatis Carolinae Math. et Physica, v.**12**(1971), No 2, p.31-49.

4. *Burris S., Sankappanavar H.P.* A course in universal algebra. Springer-Verlag, New-York. 1981.

5. *Belyavskaya G.B.* Left, right, middle nuclei and the centre of a quasigroup (Russian). Preprint. IM AN SSRM. Kishinev, 1988.

6. *Belyavskaya G.B.* T-quasigroups and the centre of a quasigroup (Russian). Matem. issled., vyp.111, Kishinev, "Stiinca", 1989. p.24-43.

7. *Belyavskaya G.B.* On the concept of the centre in a quasigroup (Russian). Matem. issled., vyp.120, Kishinev, 1991.

8. *Smith J.D.H.* Mal'cev Varieties. Lecture Notes in Math., v.**554**, Berlin, 1976.

9. *Chein O., Pflugfelder H.O., Smith J.D.H.* Quasigroups and Loops: Theory and Applications. Sigma Ser. in Pure Math., v.**8**, 1990.

10. *Gumm H.P.* An easy way to the commutator in modular varieties. Archiv der Math., v.**34**, fasc.3, p.220-228.

11. *Herrmann C.* Affine algebras in congruence modular varieties. Acta Sci. Math., v.**41**(1979), p.119-125.

12. *Pinus A.G.* Congruence modular varieties of algebras (Russian). Irkutsk: Irkutsk University. 1986.

13. *Belousov V.D.* Foundations of the theory of quasigroups and loops (Russian). Moscow, "Nauka", 1967.

Belyavskaya G.B. **Ph.D.**
department of quasigroup theory,
Institute of Mathematics,
Academy of Sciences of Moldova,
5, Academiei str.,
Kishinau, 277028,
Moldova.

Received August 10, 1993.

Quasigroups and related systems, vol.1, no.1(1), 1994

ONE-SIDED *T*-QUASIGROUPS AND IRREDUCIBLE BALANCED IDENTITIES

Galina B. Belyavskaya , Abdullo H. Tabarov

Abstract

Left and right T-quasigroups are considered. It is proved that all primitive left (right) T-quasigroups form the variety which can be characterized by two identities. Some varieties of primitive left (right) T-quasigroups and T-quasigroups characterized by irreducible balanced identities are picked out.

Introduction.

It is known that all primitive quasigroups isotopic to groups form the variety characterized by one identity [1].

The class of linear quasigroups plays the important role in this variety. As V.D.Belousov has shown in [1] these quasigroups are closely connected with irreducible balanced identities in quasigroups.

A quasigroup $Q(\cdot)$ is called linear (over a group) if a group $Q(+)$, its automorphisms φ,ψ and an element $c \in Q$ exists such that

$$xy = \varphi x + c + \psi y \qquad (1)$$

for all $x, y \in Q$.

The automorphisms φ,ψ are called *determining automorphisms* for the quasigroup $Q(\cdot)$.

In [2] the concept of linear quasigroup was generalized as follows.

A quasigroup $Q(\cdot)$ is called a *left (right) linear quasigroup* if there exist group $Q(+)$, its automorphism φ (ψ) and an one-to-one mapping β (α) of Q onto Q such that

$$xy = \varphi x + \beta y \quad (xy = \alpha x + \psi y)$$

for all $x, y \in Q$.

As it was shown in [2], left (right) linear quasigroups are closely connected with the left (right) nucleus in quasigroups. They also arised in [1] in the investigation of irreducible balanced identities in quasigroups.

All primitive left linear quasigroups form the variety characterized by the following identity:

$$[x(u\backslash y)]z = [x(u\backslash u)]\cdot(u\backslash yz). \tag{2}$$

Analogously, all primitive right linear quasigroups are characterized by the identity

$$x[(y/u)z] = (xy/u)\cdot[(u/u)z] \tag{3}$$

(**Corollary 2** [2]).

All primitive linear quasigroups also form the variety which can be characterized by the identities (2) and (3) (**Corollary 3** [2]) or the unique identity

$$xy\cdot uv = xu\cdot(\alpha_u y\cdot v) \tag{4}$$

where α_u is a mapping of Q in Q depending on u (**Theorem 1** [3]). It is easy to see that α_u is an one-to-one mapping of Q onto Q:

$$\alpha_u y = [u\backslash(u/u)y\cdot u]/(u\backslash u).$$

The T-quasigroups, i.e. the quasigroups linear over abelian groups, are the special case of linear quasigroups. These quasigroups were introduced and studied in detail in [4,5]. The well known medial quasigroups are a special case of T-quasigroups.

In [6] it was proved that the T-quasigroups play a role in the theory of quasigroups comparable to that of abelian groups among groups. Namely, a quasigroup coincides with its centre iff it is a T-quasigroup (see **Theorem 6** [6]).

In [6] the variety of all primitive T-quasigroups is characterized by two identities: (4) and the identity

$$xy\cdot uv = (\beta_x v\cdot y)\cdot ux, \tag{5}$$

where

$$\beta_x v = [(x((x/x)v))/x]/(x\backslash x).$$

In this article we consider the one-sided T-quasigroups (left and right T-quasigroups) and prove that all primitive left (right) T-quasigroups form the variety, which can be characterized by two identities. We also pick out a number of varieties of primitive left (right) T-quasigroups and T-quasigroups characterized by irreducible balanced identities.

1. Left (right) T-quasigroups and their characterization.

The following case of a left linear quasigroup $Q(\cdot)$ arised in [1] due to V.D.Belousov when he studied quasigroups with irreducible balanced identities:

$$xy = \varphi x + \beta y,$$

where $Q(+)$ is an abelian group, φ is its automorphism, β is an one-to-one mapping of Q onto Q. Using this we say that a quasigroup $Q(\cdot)$ is a *left (right) T-quasigroup*, briefly, a *LT-quasigroup* (*RT-quasigroup*) if $Q(\cdot)$ is a left (right) linear quasigroup over an abelian group.

First, we recall that the primitive quasigroup $Q(\cdot,\backslash,/)$ corresponds to each quasigroup $Q(\cdot)$, where

$$xy = z \Leftrightarrow x \backslash z = y \Leftrightarrow z / y = x.$$

We also note that according to **Lemma 1** [2] a left linear quasigroup, which is simultaneously a right linear quasigroup, is a linear quasigroup. From this **Lemma** it immediately follows that if a LT-quasigroup is a RT-quasigroup, then it is a T-quasigroup.

Theorem 1. *All primitive LT-quasigroup form the variety characterized by the following two identities*

$$[x(u \backslash y)]z = [x(u \backslash u)] \cdot (u \backslash yz), \tag{6}$$

$$(x / u)(u \backslash y) = (y / u)(u \backslash x). \tag{7}$$

All primitive RT-quasigroups are characterized by the identity (7) *and the following identity*

$$x[(y / u)z] = (xy / u)[(u / u)z]. \tag{8}$$

Proof. According to **Corollary 2** [2] the identity (6) means that $Q(\cdot)$ is left linear over a group $Q(+)$. But (7) implies that $Q(+)$ is an abelian group. Really, write (7) as follows

$$R_u^{-1}x \cdot L_u^{-1}y = R_u^{-1}y \cdot L_u^{-1}x, \tag{9}$$

where R_u, L_u are the translations of $Q(\cdot)$ with respect to an element $u \in Q$:

$$R_u x = xu, \quad L_u x = ux.$$

Fixing in (9) the element u, we obtain that

$$x \circ y = y \circ x,$$

where $Q(\circ)$ is a loop principally isotopic to $Q(\cdot)$. Hence, the loop $Q(\circ)$ is commutative. By the **Albert's theorem** (see, for example, **Theorem 1.4** [7]) the loop $Q(\circ)$ is an abelian group. Thus, $Q(\cdot)$ is a LT-quasigroup.

Conversely, if $Q(\cdot)$ is a LT-quasigroup, then it is left linear over an abelian group $Q(+)$ and by **Corollary 2** [2] $Q(\cdot)$ satisfies the identity (6). Next, since the group $Q(+)$ is abelian, then by the **Albert's theorem** each loop, isotopic to $Q(+)$, is commutative. Hence, the equality (9) is satisfied for all $x,y,u \in Q$, i.e. the identity (7) holds. This completes the proof for the LT-quasigroups.

The proof for the RT-quasigroups is similar if we take into account that the identity (8) characterizes the variety of all right linear quasigroups (see **Corollary 2** [2]).

In the introduction it was noted that the variety of all primitive T-quasigroups is characterized by two identities (4) and (5). From **Theorem 1** an another characterization of T-quasigroups follows.

Corollary 1. *The variety of all primitive T-quasigroups can be characterized by three identities* (6),(7) *and* (8).

Indeed, it follows from above that if a LT-quasigroup $Q(\cdot)$ is also a RT-quasigroup, then $Q(\cdot)$ is a T-quasigroup. The converse follows from **Theorem 1.**

2. LT-quasigroups, RT-quasigroups, T-quasigroups and balanced identities.

Now we recall that an identity

$$w_1 = w_2$$

defined on a quasigroup $Q(\cdot)$ is called *balanced* if each variable x, which occurs on one side w_1 of the identity, occurs on the another side w_2 too and if no variable occurs in w_1 or w_2 more than once. This definition is due to A.Sade (see [8]). All balanced identities can be separated on two kinds. An identity $w_1 = w_2$ is kind 1 if the elements in w_1 and w_2 are equally ordered and is kind 2 otherwise.

An identity $w_1 = w_2$ is called *reducible* [1] if either

(i) each of w_1 and w_2 contains a "free element" x so that w_1 is of the form u_1x or xv_1 and w_2 likewise is the form u_2x or xv_2 (where u_i or v_i represents a subword of the word w_i for $i = 1,2$); or

(ii) w_1 has the product xy of two free elements x and y as a subword and w_2 has one of the product xy or yx as a subword, or the dual of this statement.

An identity which is not reducible is called *irreducible.*

V.D.Belousov has proved the following remarkable theorem (**Theorem 3** [1]): a quasigroup which satisfies an irreducible balanced identity is isotopic to a *group.*

Let

$$(x_1, x_2, \ldots, x_k) = ((\ldots((x_1x_2)x_3)\ldots))x_k,$$
$$[x_1x_2\ldots x_k] = x_1(x_2(\ldots(x_{k-2}(x_{k-1}x_k))\ldots))$$

and $m|n$ means that m is a divisor of n. By $|\varphi|$ we denote the order of the automorphism φ and let S_Q denotes the set of all one-to-one mappings of Q onto Q.

A mapping $\gamma \in S_Q$ is called a *quasiautomorphism* of a quasigroup $Q(\cdot)$ if there exist one-to-one mappings $\alpha, \beta \in S_Q$ such that

$$\gamma(xy) = \alpha x \cdot \beta y.$$

According to **Lemma 2.5** [7] if γ is a quasiautomorphism of a group $Q(+)$, then

$$\gamma x = R_s\gamma_1 x = L_s\gamma_2 x,$$

where γ_1, γ_2 are automorphisms of $Q(+)$;

$$R_s x = x + s, \quad L_s x = s + x.$$

V.D.Belousov in [1,p.79] has proved the following important for us statement, which can be formulated as follows

Theorem 2 [1]. *Let $Q(\cdot)$ be a LT-quasigroup:*

$$xy = \varphi x + \beta y,$$

φ is an automorphism of the group $Q(+)$ of the order m, θ is a permutation of the set $M = \{0,1,\ldots,n\}$, where $m|n$, satisfying the conditions:

(1) $\theta 0 \neq 0$,

(2) $\theta n \neq n$,

(3) $\theta i \equiv i (\mathrm{mod}\, m)$

for each $i \in M$. Then the following irreducible balanced identity of kind 2

$$(xy_0y_1\cdots y_{n-1}y_n) = (xy_{\theta 0}y_{\theta 1}\cdots y_{\theta(n-1)}y_{\theta n}) \tag{10}$$

is satisfied in $Q(\cdot)$.

Conversely, if the identity (10) *holds in a quasigroup* $Q(\cdot)$ *for a nonidentity permutation* θ *of* M, *then* $Q(\cdot)$ *is a LT-quasigroup:*

$$xy = \varphi x + \beta y,$$

the automorphism φ *has a finite order* m *which is a divisor of* $(\theta i - i)$ *for each* $i = 0, 1, \dots, n$ *and the permutation* θ *satisfies the conditions* (1), (2), *and* (3).

For our aims the next special case of **Theorem 2** [1] is useful.

Theorem 3 . *Let* $Q(\cdot)$ *be a LT-quasigroup:*

$$xy = \varphi x + \beta y,$$

$|\varphi| = m$, $m|n$. *Then* $Q(\cdot)$ *satisfies the following irreducible balanced identity of kind 2:*

$$(xy_0 y_1 \dots y_{n-1} y_n) = (xy_n y_1 \dots y_{n-1} y_0). \qquad (11)$$

Conversely, if a quasigroup $Q(\cdot)$ *satisfies the identity* (11), *then* $Q(\cdot)$ *is a LT-quasigroup:*

$$xy = \varphi x + \beta y,$$

and the order m *of the automorphism is a divisor of* n.

For the proof it is enough to observe that the identity (11) is (10) if $\theta = (0n)$, where $(0n)$ is a transposition (a cycle of the lenght two). Evidently, $\theta = (0n)$, satisfies each of conditions (1), (2), (3).

Remark, that the case $m = n$ corresponds to the identity (11) of a "minimal lenght".

The analogue of **Theorem 2** [1] is true for RT-quasigroups if we take the identity

$$[y_n y_{n-1} \dots y_1 y_0 x] = [y_{\theta n} y_{\theta(n-1)} \dots y_{\theta 1} y_{\theta 0} x]$$

instead of (10), but we shall formulate and prove the analog of **Theorem 3** changing a little the outline of the proof of the corresponding statement from [1].

Theorem 4. *Let* $Q(\cdot)$ *be a RT-quasigroup:*

$$xy = \alpha x + \psi y,$$

$|\psi| = k$, $k|l$. *Then the following irreducible balanced identity of kind 2:*

$$[y_l y_{l-1} \dots y_1 y_0 x] = [y_0 y_{l-1} \dots y_1 y_l x] \qquad (12)$$

is satisfied in $Q(\cdot)$.

Conversely, if the identity (12) *is satisfied in a quasigroup* $Q(\cdot)$ *for some* $l \geq 1$, *then* $Q(\cdot)$ *is a RT-quasigroup:*

$$xy = \alpha x + \psi y,$$

and the order k of the automorphism ψ is a divisor of l.

Proof. Let $Q(\cdot)$ be a RT-quasigroup:

$$xy = \alpha x + \psi y,$$

$|\psi| = k$, $k|l$. Then

$$[y_l y_{l-1} \dots y_1 y_0 x] = y_l(y_{l-1} \dots (y_1(y_0 x)) \dots) =$$
$$= \alpha y_l + \psi\alpha y_{l-1} + \psi^2 \alpha y_{l-2} + \dots + \psi^l \alpha y_0 + \psi^{l+1} x =$$
$$= \alpha y_l + \psi\alpha y_{l-1} + \psi^2 \alpha y_{l-2} + \dots + \alpha y_0 + \psi x =$$
$$= y_0(y_{l-1} \dots (y_1(y_l x)) \dots) = [y_0 y_{l-1} \dots y_1 y_l x].$$

Conversely, let the identity (12) be satisfied in a quasigroup $Q(\cdot)$ for some $l \geq 1$. By **Theorem 3** from [1] $Q(\cdot)$ is isotopic to a group $Q(+)$:

$$xy = \lambda x + \delta y \tag{13}$$

where $\lambda, \delta \in S_Q$. That is why from (12) we have

$$[y_l y_{l-1} \dots y_1 y_0 x] = y_l [y_{l-1} \dots y_1 y_0 x] =$$
$$= \lambda y_l + \delta[y_{l-1} \dots y_1 y_0 x] = \lambda y_0 + \delta[y_{l-1} \dots y_1 y_l x].$$

Fix x and all $y_j, j \neq 0, l$, in this equality:

$$\lambda y_l + \delta_1 y_0 = \lambda y_0 + \delta_1 y_l$$

for some $\delta_1 \in S_Q$. But by **Lemma 11** from [1] a group $Q(+)$ is abelian if the equality

$$\alpha x + \beta y = \gamma y + \delta x$$

is satisfied in $Q(+)$ for some $\alpha, \beta, \gamma, \delta \in S_Q$.

Next show that δ from (13) is a quasiautomorphism of the abelian group $Q(+)$. The identity (12) means that

$$y_l(y_{l-1} \dots (y_1(y_0 x)) \dots) = y_0(y_{l-1} \dots (y_1(y_l x)) \dots). \tag{14}$$

Let $l \geq 3$, then (14) can be written as follows

$$\lambda y_l + \delta(\lambda y_{l-1} + \delta[y_{l-2} \dots y_1 y_0 x]) =$$
$$= \lambda y_0 + \delta(\lambda y_{l-1} + \delta[y_{l-2} \dots y_1 y_l x]).$$

Put in this equality

$$x = \lambda y_0 = y_1 = y_{l-2} = 0,$$

where 0 is the identity element of $Q(+)$, then

$$\lambda y_l + \delta_1 y_{l-1} = \delta(\lambda y_{l-1} + \delta_2 y_l)$$

for the corresponding $\delta_1, \delta_2 \in S_Q$. Hence, δ is a quasiautomorphism of $Q(+)$.

Let now $l = 2$, then (14) implies

$$\lambda y_2 + \delta(\lambda y_1 + \delta(y_0 x)) = \lambda y_0 + \delta(\lambda y_1 + \delta(y_2 x)).$$

Put here $\lambda y_0 = x = 0$, then

$$\lambda y_2 + \delta_3 y_1 = \delta(\lambda y_1 + \delta_4 y_2)$$

for $\delta_3, \delta_4 \in S_Q$. At last, let $l=1$, then from (14) we have

$$\lambda y_1 + \delta(y_0 x) = \lambda y_0 + \delta(y_1 x),$$

or

$$\lambda y_1 + \delta' x = \delta(y_1 x),$$

if we put $\lambda y_0 = 0$.

Thus, in all cases we obtain that δ is a quasiautomorphism of $Q(+)$. According to **Lemma 2.5** [7]

$$\delta x = s + \psi x,$$

where ψ is an automorphism of $Q(+)$, $s \in Q$. Hence,

$$xy = \lambda x + \delta y = \alpha x + \psi y, \tag{15}$$

where

$$\alpha x = \lambda x + s.$$

Using (15) in (14) we have

$$\alpha y_l + \psi\alpha y_{l-1} + \psi^2 \alpha y_{l-2} + \ldots + \psi^{l-1}\alpha y_1 + \psi^l \alpha y_0 + \psi^{l+1} x =$$
$$= \alpha y_0 + \psi\alpha y_{l-1} + \psi^2 \alpha y_{l-2} + \ldots + \psi^{l-1}\alpha y_1 + \psi^l \alpha y_l + \psi^{l+1} x$$

whence

$$\alpha y_l + \psi^l \alpha y_0 = \alpha y_0 + \psi^l \alpha y_l,$$
$$\psi^l(\alpha y_0 - \alpha y_l) = \alpha y_0 - \alpha y_l.$$

Therefore, $\psi^l x = x$ for every $x \in Q$, so the order $|\psi|$ of the automorphism ψ is a divisor of l. This completes the proof.

Theorems 3 and **4** imply

Corollary 2. *Let $Q(\cdot)$ be a T-quasigroup:*

$$xy = \varphi x + c + \psi y,$$

$|\varphi|=m$, $|\psi|=k$, $m|n$, $k|l$. *Then the identities* (11),(12) *are satisfied in $Q(\cdot)$. Conversely, if the identities* (11) *and* (12) *hold for certain $n,l \geq 1$ in quasigroup $Q(\cdot)$, then $Q(\cdot)$ is a T-quasigroup:*

$$xy = \varphi x + c + \psi y,$$

$|\varphi| \mid n$ *and* $|\psi| \mid l$.

Proof. Since every T-quasigroup is a LT-quasigroup and a RT-quasigroup, the first statement follows at once from **Theorems 3** and **4.** Conversely, according to **Theorem 4** if (12) is satisfied in a quasigroup $Q(\cdot)$ for some $l \geq 1$, then $Q(\cdot)$ is a RT-quasigroup:

$$xy = \lambda x + \delta y = \alpha x + \psi y,$$

(see (15)) and $|\psi|$ is a divisor of l. Next, using the equalities (11) and (13), we can prove that λ is a quasiautomorphism of $Q(+)$:

$$\lambda x = \varphi x + t,$$

where $t \in Q$, $\varphi \in AutQ(+)$ and $|\varphi| \mid n$. The proof is similar to that of the case for in **Theorem 4**. Thus,

$$xy = \lambda x + \delta y = \varphi x + t + s + \psi y = \varphi x + c + \psi y,$$

where $c = t+s$, $|\varphi| \mid n$, $|\psi| \mid l$. This completes the proof.

3. Some subvarieties of the varieties of LT- (RT-) quasigroups and T-quasigroups.

The above proved results present the posibility to pick out some varieties of primitive LT-quasigroups, RT-quasigroups and T-quasigroups, which are characterized by irreducible balanced identities of kind 2 and depend on the orders of their determining automorphisms.

We begin with the following **Lemma** which means that the order of a determining automorphism φ (ψ) of a LT-quasigroup (RT-quasigroup) $Q(\cdot)$ is its invariant and does not depend on a group over which $Q(\cdot)$ is left (right) linear.

Lemma 1.

(i) *Let $Q(\cdot)$ be a LT-quasigroup and*

$$xy = \varphi x + \beta y = \bar{\varphi} x \circ \bar{\beta} y,$$

where φ ($\bar{\varphi}$) is an automorphism of the abelian group $Q(+)$ ($Q(\circ)$), $\beta, \bar{\beta} \in S_Q$. Then $\varphi x = R_a \bar{\varphi} R_a^{-1} x$ for certain $a \in Q$ ($R_a x = x + a$), i.e. $|\varphi| = |\bar{\varphi}|$.

(ii) *Let $Q(\cdot)$ be a RT-quasigroup and*

$$xy = \alpha x + \psi y = \bar{\alpha} x \circ \bar{\psi} y,$$

where $\psi \in AutQ(+)$, $\bar{\psi} \in AutQ(\circ)$. Then $\psi y = R_a \bar{\psi} R_a^{-1} y$ for some $a \in Q$, i.e. $|\psi| = |\bar{\psi}|$.

Proof. Let

$$xy = \varphi x + \beta y = \bar{\varphi} x \circ \bar{\beta} y,$$

$$\varphi \in AutQ(+), \quad \bar{\varphi} \in AutQ(\circ).$$

In this case the group $Q(\circ)$ is principally isotopic to the group $Q(+)$. By **Albert's Theorem** $Q(\circ)$ is isomorphic to $Q(+)$. Moreover, there exists such an element $a \in Q$ that

$$R_a(x \circ y) = R_a x + R_a y, \quad R_a x = x + a$$

(see the proof of **Albert's Theorem** in [7], p.17). Hence, using the equality

$$R_a^{-1} x = x - a,$$

we have

$$xy = \overline{\varphi} x \circ \overline{\beta} y = R_a^{-1}(R_a \overline{\varphi} x + R_a \overline{\beta} y) =$$
$$= R_a \overline{\varphi} R_a^{-1}(x + a) + \overline{\beta} y = R_a \overline{\varphi} R_a^{-1} x + \overline{\beta}_1 y$$

($\overline{\beta}_1 y = R_a \overline{\varphi} 0 + \overline{\beta} y$, **0** is the identity element of $Q(+)$), since

$$\varphi_1 = R_a \overline{\varphi} R_a^{-1}$$

is an automorphism of $Q(+)$. Thus,

$$xy = \varphi x + \beta y = \varphi_1 x + \overline{\beta}_1 y$$

whence by $x = 0$ have

$$\beta = \overline{\beta}_1, \varphi = \varphi_1, |\varphi| = |\varphi_1| = |\overline{\varphi}|.$$

The second part of **Lemma 1** is proved analogously.

Corollary 3. *If $Q(\cdot)$ is a T-quasigroup and*

$$xy = \varphi x + c + \psi y = \overline{\varphi} x \circ \overline{c} \circ \overline{\psi} y,$$

then

$$\varphi x = R_a \overline{\varphi} R_a^{-1},$$
$$\psi y = R_a \overline{\psi} R_a^{-1},$$

i.e. $|\varphi| = |\overline{\varphi}|, |\psi| = |\overline{\psi}|$.

The **proof** follows immediately from **Lemma 2.**

Now let m,n be natural numbers. Denote by $\mathfrak{N}_m^l$ ($\mathfrak{N}_n^r$) the class of all LT-quasigroups (RT-quasigroups) with determining automorphisms whose orders are devisors of m (of n). In other words, a LT-quasigroup (a RT-quasigroup) $Q(\cdot)$ lies in $\mathfrak{N}_m^l$ ($\mathfrak{N}_n^r$) iff $xy = \varphi x + \beta y$ ($xy = \alpha x + \psi y$) for certain abelian group $Q(+)$, its automorphism φ (ψ) such that $\varphi^m = \varepsilon$ ($\psi^n = \varepsilon$), i.e. $|\varphi| \mid m$ ($|\psi| \mid n$). Here ε is the identity mapping of Q.

By $\mathfrak{N}_{m,n}$ we denote the class of all T-quasigroups with a pair (φ,ψ) of the determining automorphisms such that

$$\varphi^m = \psi^n = \varepsilon.$$

Hence, a T-quasigroup $Q(\cdot)$ belongs to $\mathfrak{R}_{m,n}$ iff

$$xy = \varphi x + c + \psi y,$$
$$|\varphi| \mid m \quad \text{and} \quad |\psi| \mid n$$

for some abelian group $Q(+)$.

From **Lemma 1** it follows at once that

$$\mathfrak{R}^l_m \cap \mathfrak{R}^l_n = \mathfrak{R}^l_{(m,n)} \qquad (\mathfrak{R}^r_m \cap \mathfrak{R}^r_n = \mathfrak{R}^r_{(m,n)})$$

where (m,n) is the greatest common divisor of m,n. In particular, if p,q are prime numbers, then

$$\mathfrak{R}^l_p \cap \mathfrak{R}^l_q = \mathfrak{R}^l_1 \qquad (\mathfrak{R}^r_p \cap \mathfrak{R}^r_q = \mathfrak{R}^r_1).$$

Next we prove

Lemma 2. $\mathfrak{R}_{m,n} = \mathfrak{R}^l_m \cap \mathfrak{R}^r_n$.

Proof. It is clear, that

$$\mathfrak{R}_{m,n} \subseteq \mathfrak{R}^l_m \cap \mathfrak{R}^r_n.$$

Let $Q(\cdot)$ occurs in $\mathfrak{R}^l_m$ and $\mathfrak{R}^r_n$. Then there exists abelian groups $Q(+)$ and $Q(\circ)$, their automorphisms φ and $\overline{\psi}$, such that

$$\varphi^m = \overline{\psi}^n = \varepsilon$$

and

$$xy = \varphi x + \beta y = \alpha x \circ \overline{\psi} y \tag{16}$$

for some $\alpha, \beta \in S_Q$. In this case there exists such an element $a \in Q$ that

$$R_a(x \circ y) = R_a x + R_a y$$

(see the proof of **Lemma 1**). Hence, from (16) by $x = 0$ we have

$$\beta y = \alpha 0 \circ \overline{\psi} y = R_a^{-1}(R_a \alpha 0 + R_a \overline{\psi} y) =$$
$$= -a + a + \alpha 0 + R_a \overline{\psi} R_a^{-1}(a + y) = c + \psi y,$$

where

$$c = \alpha 0 + R_a \overline{\psi} 0,$$

since $\psi = R_a \overline{\psi} R_a^{-1}$ is an automorphism of $Q(+)$. Thus,

$$|\psi| = |\overline{\psi}|,$$
$$xy = \varphi x + c + \psi y,$$

and $Q(\cdot) \in \mathfrak{R}_{m,n}$, as required.

Now denote by $\overline{\mathfrak{R}}_m^l$, $\overline{\mathfrak{R}}_n^r$, $\overline{\mathfrak{R}}_{m,n}$ the classes of corresponding primitive LT-quasigroups, RT-quasigroups and T-quasigroups.

Theorem 5.

(i) $\overline{\mathfrak{R}}_m^l$ *is a variety of primitive LT-quasigroups characterized by the identity*

$$(xy_0y_1\cdots y_m)=(xy_my_1y_2\cdots y_{m-1}y_0). \tag{17}$$

(ii) $\overline{\mathfrak{R}}_n^r$ *is a variety of primitive RT-quasigroups characterized by the identity*

$$[y_ny_{n-1}\cdots y_1y_0x]=[y_0y_{n-1}\cdots y_1y_nx]. \tag{18}$$

(iii) $\overline{\mathfrak{R}}_{m,n}$ *is a variety of primitive T-quasigroups characterized by the identities* (17) *and* (18).

Proof.

(i) Let $Q(\cdot)\in\mathfrak{R}_m^l$:

$$xy=\varphi x+\beta y,\qquad |\varphi|\mid m,$$

then $Q(\cdot)$ satisfies (17) by the first part of **Theorem 2.** Conversely, if $Q(\cdot)$ satisfies (17), then it is a LT-quasigroup by the second part of **Theorem 2** and

$$xy=\varphi x+\beta y,\qquad |\varphi|\mid m,$$

i.e. $Q(\cdot)\in\mathfrak{R}_m^l$.

(ii) follows similarly from **Theorem 3.**

(iii) is a consequence of **Lemma 2,** (i) and (ii).

Next we consider some special cases of the above varieties.

The variety $\overline{\mathfrak{R}}_1^l$ $(\overline{\mathfrak{R}}_1^r)$ includes all quasigroups such that

$$xy=x+\beta y\quad (xy=\alpha x+y),\qquad \alpha,\beta\in S_Q$$

over all abelian groups $Q(+)$ (Q is a nonfixed set). These varieties are characterized by the identities

$$xy_0\cdot y_1=xy_1\cdot y_0\quad (y_1\cdot y_0x=y_0\cdot y_1x),$$

respectively.

The variety $\overline{\mathfrak{R}}_2^l$ $(\overline{\mathfrak{R}}_2^r)$ includes all quasigroups from $\overline{\mathfrak{R}}_1^l$ $(\overline{\mathfrak{R}}_1^r)$ and quasigroups of the form

$$xy=\varphi x+\beta y,\qquad |\varphi|=2$$

$$(xy=\alpha x+\psi y,\qquad |\psi|=2)$$

If $Q(\cdot)\in\overline{\mathfrak{R}}_2^l$ $(Q(\cdot)\in\overline{\mathfrak{R}}_2^r)$, then $Q(\cdot)$ satisfies the identity

$$(xy_0\cdot y_1)y_2=(xy_2\cdot y_1)y_0,$$

$$(y_2(y_1\cdot y_0x)=y_0(y_1\cdot y_2x)),$$

and conversely.

Let p,q be simple numbers. Then $\mathfrak{R}_p^l$ ($\mathfrak{R}_q^r$) contains all quasigroups from $\overline{\mathfrak{R}}_1^l$ ($\overline{\mathfrak{R}}_1^r$) and all LT-quasigroups (RT-quasigroups) with the determining automorphisms of the order p (of the order q). If $Q(\cdot)\in\overline{\mathfrak{R}}_{p,q}$, then it has one of the next forms:

$$xy = \varphi x + c + \psi y, \quad |\varphi| = p, \quad |\psi| = q,$$
$$xy = \varphi x + c + y, \quad |\varphi| = p,$$
$$xy = x + c + \psi y, \quad |\psi| = q,$$
$$xy = x + c + y.$$

Finally we note that the variety of all abelian groups is contained in every variety from $\overline{\mathfrak{R}}_m^l$, $\overline{\mathfrak{R}}_n^r$, $\overline{\mathfrak{R}}_{m,n}$ for any m,n.

References

1. *Belousov V.D.* Balanced identities in quasigroups (Russian). Matem. sbornik., v.**70**(**112**)(1966), N1, p.55-97.

2. *Belyavskaya G.B., Tabarov A.H.* Nuclei and the centre of linear quasigroups (Russian). Izvestija AN RM Matematika, N3(6)(1991), p.37-42.

3. *Belyavskaya G.B., Tabarov A.H.* Characterization of linear and alinear quasigroups (Russian). Diskretnaja matematica, Moscow., v.**4**(1992), p.42-147.

4. *Kepka T., Němec P.* T-quasigroups. 1. Acta Univ. Carol.math. et phys., v.**12**(1971), N1, p.39-49.

5. *Kepka T., Němec P.* T-quasigroups. 2. *Acta Univ. Carol.math. et phys.*, v.**12**(1971), N2, p.31-49.

6. *Belyavskaya G.B.* T-quasigroups and the centre of a quasigroup (Russian). Matem. Issled., vyp.111, Kishinev, "Stiintca", 1989, p.24-43.

7. *Belousov V.D.* Foundations of the theory of quasigroups and loops (Russian). Moscow, "Nauka", 1967.

8. *Sade A.* Entropic demosienne de multigroupoides et de quasigroupes. Ann. Sci. Bruxelles. Ser. 1, v.**73**(1959), p.302-309.

Belyavskaya G.B. **Ph.D.**
Tabarov A.H. **Ph.D.**
department of quasigroup theory,
Institute of Mathematics,
Academy of Sciences of Moldova,
5, Academiei str.,
Kishinau, 277028,
Moldova.

Received August 10, 1993

Quasigroups and related systems, vol. **1**, no. 1(1), 1994

TRANSVERSALS IN GROUPS.1. ELEMENTARY PROPERTIES

Evgenii A. Kuznetsov

Abstract

In this work the elementary properties of transversals in groups are studied.

1. Introduction. Necessary definitions and notations.

The present work deals with the properties of specific sets of representatives of left (right) cosets in groups to its subgroups. These sets are called left (right) transversals in groups to its subgroups. They were introduced in [1] and studied in [1,2,6] etc.

We shall use the following notations:

Λ is an index set (Λ contains a distinguished element 1); left (right) cosets in a group G to its subgroup H are numbered by the indexes from Λ;

${}_iH$ is the i-th left coset in a group G to its subgroup H;

H_i is the i-th right coset in a group G to its subgroup H;

e is the unit of group;

$Core_G(H)$ is the maximal subgroup contained in H and normal in G;

$St_a(K)$ is the stabilizor of an element a in a permutation group K.

Definition 1. Let G be a group and H a subgroup in G. A complete system T of representatives of the left (right) cosets in G to H ($e = t_1 \in T$) is called a *left* (*right*) *transversal in G to H*.

Definition 2. A left transversal T in G to H which is also a right transversal in G to H is called a *two-sided* transversal in G to H.

Remark. If we study a two-sided transversal T in G to H then we shall consider that

$$t_i \in {}_iH \cap H_i$$

for any $i \in \Lambda$ and $t_i \in T$. We can always succeed in this by a corresponding renumeration of cosets.

Let T be a transversal (left or right) in G to H. We can introduce correctly the following operations on Λ:

$$i * j = v \Leftrightarrow t_i t_j = t_v h, \quad h \in H \tag{1}$$

if T is a left transversal, and

$$i \circ j = w \Leftrightarrow t_i t_j = h t_w, \quad h \in H \tag{2}$$

if T is a right transversal.

Lemma 1. *The system* $< \Lambda, *, 1 >$ *is a right quasigroup with the unit* 1.

Proof. Let arbitrary elements $a, b \in \Lambda$ be given. Let us consider the following equation:

$$a * x = b. \tag{3}$$

We have from the **Definition 1**: there exists an element $u \in \Lambda$ such that

$$t_a^{-1} t_b = t_u h, \quad h \in H.$$

Then

$$t_a t_u = t_b h^{-1}, \tag{4}$$

i.e.

$$a * u = b.$$

So a solution of the equation (3) exists. Assume it is not unique. Then there exists an element $v \in \Lambda$ such that

$$a * v = b \quad \& \quad v \neq u. \tag{5}$$

Therefore we have

$$t_a t_v = t_b h_1, \quad h_1 \in H. \tag{6}$$

From (4) and (6) it follows that

$$t_a t_u h = t_a t_v h_1^{-1},$$
$$t_v = t_u h_2,$$

and then $v = u$, because only one element from T lies in every coset in G to H. We have a contradiction with (5). So u is the unique solution of the equation (3), i.e. the system $< \Lambda, * >$ is a right quasigroup.

We have for any $a \in \Lambda$

$$a*1=c,$$
$$t_a e = t_c h,\quad h\in H,$$
$$t_c = t_a h^{-1},\quad h\in H,$$

and then $c=a$, i.e. $a*1=a$. We can prove that $1*a=a$ for any $a\in\Lambda$ analogously. The proof is complete.

Lemma 1*. *The system* $<\Lambda,\mathrm{o},1>$ *is a left quasigroup with the unit* 1.

The **proof** is similar to the proof of **Lemma 1**.

Definition 3. Let T be a left (right) transversal in G to H. If the system $<\Lambda,*,1>$ ($<\Lambda,\mathrm{o},1>$) is a loop, then T is called a *left (right) loop transversal in G to H*. If $<\Lambda,*,1>$ (respectively, $<\Lambda,\mathrm{o},1>$) is a group, then T is called a *left (right) group transversal in G to H*.

The next **Lemma** reduces the investigation of transversals in groups to the case when $Core_G(H)=<e>$ (for loop transversals an analogous result was proved in [2]).

Lemma 2. *Let T be a left transversal in G to H and*

$$\varphi: G\to G' = G/Core_G(H)$$

the natural homomorphism. Then we have:

1. *The set*

$$T' = \{\varphi(t_x) | t_x \in T, x\in\Lambda\}$$

is a left transversal in G' *to* $H' = H/Core_G(H)$*;*

2. $$<\Lambda,\bullet,1> \cong <\Lambda,*,1>,$$

where "•" is the operation corresponding to the transversal T';

Proof.

1. Let us denote: $t_x' = \varphi(t_x)$. Then we have:

$$(t_x')^{-1} t_y' \in H',$$

$$(\varphi(t_x))^{-1}\varphi(t_y)\in\varphi(H),$$

$$\varphi(t_x^{-1}t_y)\in\varphi(H),$$

$$(t_x^{-1}t_y)\cdot Core_G(H) = h_0\cdot Core_G(H),\quad h_0\in H,$$

$$t_x^{-1}t_y\in H,$$

i.e. $x=y$, because $Core_G(H)\subseteq H$. Since for any $g'\in G'$ there exists $g\in G$ such that $g'=\varphi(g)$, then

$$g=t_u h_0,$$
$$g'=\varphi(g)=\varphi(t_u h_0)=\varphi(t_u)\varphi(h_0)=t_u' h_0',$$

where $h_0'\in H'$. It means T' is a left transversal in G' to H'.

2. We have:

$$x\bullet y=u,$$
$$t_x' t_y'=t_u' h',\quad h'\in H',$$
$$\varphi(t_x)\varphi(t_y)=t_u' h',\quad h'\in H',$$
$$t_u' h'=\varphi(t_x t_y)=\varphi(t_{x*y} h_1)=t_{x*y}'\cdot h_1',\quad h',h_1'\in H',$$
$$x*y=u,$$

i.e. for any $x,y\in\Lambda$

$$x*y=x\bullet y.$$

It means that

$$<\Lambda,\bullet,1>\equiv<\Lambda,*,1>.$$

Lemma 2*. *Let T be a right transversal in G to H and*

$$\varphi: G\to G'=G/Core_G(H)$$

the natural homomorphism. Then we have:

1. *The set*

$$T'=\{\varphi(t_x)\mid t_x\in T, x\in\Lambda\}$$

is a right transversal in G' to $H'=H/Core_G(H)$;

2. $$<\Lambda,\times,1>\equiv<\Lambda,o,1>,$$

where "$\times$" is the operation corresponding to transversal T'.

The **proof** is analogous to that of **Lemma 2**.

Lemma 3. *In notations of* **Lemma 2** *(or* **Lemma 2***):

$$Core_{G'}(H')=<e>.$$

Proof. Let us assume

$$Core_{G'}(H')=M_0\neq<e>.$$

The complete inverse-image $\varphi^{-1}(M_0)=M_1$ is a subgroup in G. We have:

$$e\in M_0\ \Rightarrow\ Core_G(H)=Ker\varphi=\varphi^{-1}(e)\subset\varphi^{-1}(M_0)=M_1, \qquad (*)$$
$$M_0\subseteq H'\ \Rightarrow\ M_1=\varphi^{-1}(M_0)\subseteq\varphi^{-1}(H')=H. \qquad (**)$$

Let g be an arbitrary element from G and

$$M_g = gM_1g^{-1}.$$

Then

$$\varphi(M_g) = \varphi(gM_1g^{-1}) = \varphi(g)\varphi(M_1)(\varphi(g))^{-1} = g'M_0g'^{-1} = M_0,$$

because M_0 is a normal subgroup in G'. Therefore we have for any element $g \in G$:

$$gM_1g^{-1} = M_g = \varphi^{-1}(M_0) = M_1,$$

i.e. M_1 is a normal subgroup in G. This fact is in a contradiction with (*) and (**) (see above); therefore we have:

$$Core_{G'}(H') = \langle e \rangle.$$

The proof is complete.

Let us consider the permutation representations $\hat{G}$ and $\check{G}$ of group G by the left and right cosets to subgroup H. Let T be a left transversal in G to H; then by the definition:

$$\hat{g}(x) = y \Leftrightarrow gt_xH = t_yH.$$

Analogously, if T is a right transversal in G to H, then by the definition:

$$\check{g}(x) = y \Leftrightarrow Ht_xg = Ht_y.$$

It is well known (see [4]) that

$$\hat{G} \cong \check{G} \cong G / Core_G(H).$$

Lemma 4. *If T is an arbitrary left transversal in G to H then:*

1. *For any* $h \in H$: $\hat{h}(1) = 1$;
2. *For any* $x, y \in \Lambda$:

$$\hat{t}_x(y) = x*y, \quad \hat{t}_x^{-1}(y) = x \backslash y,$$

$$\hat{t}_1(x) = \hat{t}_x(1) = x, \quad \hat{t}_x^{-1}(1) = x \backslash 1, \quad \hat{t}_x^{-1}(x) = 1,$$

(where $x*y = z \Leftrightarrow x \backslash z = y$*);*

3.[1] *The following conditions are equivalent:*

a. *T is a left loop transversal in G to H;*

b. *The set $\hat{T} = \{\hat{t}_x\}_{x \in \Lambda}$ is a sharply transitive set of permutations on Λ.*

Proof. **1.** It is trivial.

2. We have:

$$\hat{t}_x(y) = w \Leftrightarrow t_x t_y H = t_w H \Leftrightarrow w = x * y;$$

$$\hat{t}_x^{-1}(y) = z \Leftrightarrow t_x^{-1} t_y H = t_z H \Leftrightarrow t_y H = t_x t_z H \Leftrightarrow y = x * z \Leftrightarrow z = x \setminus y.$$

Therefore we have as a corollary:

$$\hat{t}_1(x) = 1 * x = x, \quad \hat{t}_x(1) = x * 1 = x,$$

$$\hat{t}_x^{-1}(1) = x \setminus 1, \quad \hat{t}_x^{-1}(x) = x \setminus x = 1,$$

3. We have the following sequence of equivalent assertions:

(T is a left loop transversal in G to H) $\Leftrightarrow$

(the system $<\Lambda, *, 1>$ is a loop) $\Leftrightarrow$

(T is a left transversal in G to H and the equation $x * a = b$ has the unique solution in Λ for any given $a, b \in \Lambda$) $\Leftrightarrow$

(the equation $\hat{t}_x(a) = b$ has the unique solution in Λ for any given $a, b \in \Lambda$) $\Leftrightarrow$

(the set $\{\hat{t}_x\}_{x \in \Lambda}$ is a sharply transitive set of permutations on Λ).

Lemma 4^*. *If T is an arbitrary right transversal in G to H then:*

1. *For any* $h \in H$: $\check{h}(1) = 1$;

2. *For any* $x, y \in \Lambda$:

$$\check{t}_x(y) = y \circ x, \quad \check{t}_x^{-1}(y) = y // x,$$

$$\check{t}_1(x) = \check{t}_x(1) = x, \quad \check{t}_x^{-1}(1) = 1 // x, \quad \check{t}_x^{-1}(x) = 1,$$

(where $y // x = z \Leftrightarrow z \circ x = y$*);*

3. *The following conditions are equivalent:*

a. *T is a right loop transversal in G to H;*

b. *The set* $\check{T} = \{\check{t}_x\}_{x \in \Lambda}$ *is a sharply transitive set of permutations on* Λ.

The **proof** is analogous to that of **Lemma 4**.

2. Two-sided transversals in groups.

Lemma 5. *Let T be a two-sided transversal in G to H. Then for any $x, y \in \Lambda$:*

1. $y \backslash (x \backslash 1) = (x \circ y) \backslash 1,$
   where "\" is the left inverse operation of "$*$";
2. $(1 // y) // x = 1 // (x * y),$
   where "//" is the right inverse operation of "$\circ$".

Proof. **1.** Using **Lemma 4** we have:

$$x \circ y = z \Leftrightarrow ht_x = t_x t_y, h \in H \Leftrightarrow t_y^{-1} t_x^{-1} h = t_z^{-1}, h \in H \Leftrightarrow$$

$$\Leftrightarrow \hat{t}_y^{-1} \hat{t}_x^{-1}(1) = \hat{t}_z^{-1}(1) \Leftrightarrow \hat{t}_y^{-1}(x \backslash 1) = z \backslash 1 \Leftrightarrow y \backslash (x \backslash 1) = z \backslash 1.$$

Therefore

$$y \backslash (x \backslash 1) = (x \circ y) \backslash 1.$$

2. It is proved analogously.

Corollary. *For any two-sided transversal in G to H*

$$x * y = 1 \Leftrightarrow x \circ y = 1.$$

The **proof** is obvious.

Lemma 6. *Let T be a two-sided transversal in G to H. Then the following conditions are equivalent:*

1. *For any $x, y \in \Lambda$:*

$$x * y = x \circ y;$$

2. *The system $< \Lambda, *, 1 >$ is a WIP-loop;*

3. *The system $< \Lambda, \circ, 1 >$ is a WIP-loop;*

Proof. The definition of *WIP*-loop one can find in [5].

1.$\Rightarrow$2. Let us have for any $x, y \in \Lambda$

$$x * y = x \circ y;$$

Then the system $< \Lambda, *, 1 >$ is a left and right quasigroup with the unit 1 simultaneously, i.e. $< \Lambda, *, 1 >$ is a loop. Moreover, using **Lemma 5** we have:

$$y \backslash (x \backslash 1) = (x * y) \backslash 1 \Leftrightarrow (x * y) * (y \backslash (x \backslash 1)) = 1. \qquad (7)$$

Let

$$(x*y)*z = 1.$$

Using the identity (7) we obtain

$$z = y\backslash(x\backslash 1) \Rightarrow x*(y*z) = 1.$$

Therefore using a characterization of *WIP*-loop (see [5], p.87) we get: system $<\Lambda, *, 1>$ is a *WIP*-loop.

2.⇒1. Let the system $<\Lambda, *, 1>$ be a *WIP*-loop. Then for any $x, y \in \Lambda$

$$(x*y)\backslash 1 = y\backslash(x\backslash 1).$$

Using **Lemma 5** we have for any $x, y \in \Lambda$

$$x*y = x \circ y.$$

1.⇔3. It is proved analogously.

Lemma 7. *Let T be a left transversal in G to H. Then following conditions are equivalent:*

1. *T is a two-sided transversal in G to H;*

2. *The equation $x*a = 1$ has the unique solution in Λ for any given $a \in \Lambda$.*

Proof. 1.⇒2. Let T be a two-sided transversal in G to H. Then using the **corollary** to **Lemma 5** we have for any given $a \in \Lambda$

$$x*a = 1 \Leftrightarrow x \circ a = 1.$$

The equation $x \circ a = 1$ has the unique solution in Λ for any given $a \in \Lambda$. Then the equation $x*a = 1$ satisfies the same property.

2.⇒1. Let the condition 2 holds. Then the mapping α which is defined by

$$\alpha : \Lambda \to \Lambda,$$
$$\alpha(x) = u \Leftrightarrow u*x = 1,$$

is a permutation on Λ. Then we have for any $x \in \Lambda$:

$$t_{\alpha(x)} t_x = e \cdot h \in H,$$

$$t_{\alpha(x)} = h t_x^{-1} \in H t_x^{-1},$$

$$H t_{\alpha(x)} = H t_x^{-1}.$$

Therefore we get: firstly

$$(H t_{\alpha(x)}) \cap (H t_{\alpha(y)}) \neq \varnothing,$$

$$(H t_x^{-1}) \cap (H t_y^{-1}) \neq \varnothing,$$

$$(t_x H) \cap (t_y H) \neq \varnothing \Rightarrow x = y,$$

secondly, for any $g \in G$ there exist $t_u \in T$ and $h_0 \in H$ such that:

$$g^{-1} = t_u h_0,$$

$$g = h_0^{-1}t_u^{-1} = h_0^{-1}h^{-1}t_{\alpha(u)} = h' t_{\alpha(u)}.$$

It means that the set

$$T_1 = \{t_{\alpha(x)} | x \in \Lambda\} \equiv T$$

is a right transversal in G to H; i.e. T is a two-sided transversal in G to H. The proof is complete.

Lemma 7*. *Let T be a right transversal in G to H. Then following conditions are equivalent:*

1. *T is a two-sided transversal in G to H;*

2. *The equation $a \circ x = 1$ has the unique solution in Λ for any given $a \in \Lambda$.*

The **proof** is analogous to that of **Lemma 7**.

Remark. O.Ore has proved in [3]: if the index *(G:H)* is finite, then there exists a two-sided transversal in G to H.

Lemma 8. *Let T be a two-sided transversal in G to H and $Core_G(H) = \langle e \rangle$. Then for any $h \in H$*

$$h = \bigcap_{u \in \Lambda} (t_{\hat{h}(u)} H t_u^{-1}),$$

$$h = \bigcap_{u \in \Lambda} (t_u^{-1} H t_{\check{h}(u)}).$$

Proof. We will prove the first equality; the second equality can be proved by the same way. For any $u \in \Lambda$ we get:

$$\hat{h}(u) = v \Leftrightarrow h t_u H = t_v H \Leftrightarrow h \in (t_v H t_u^{-1}),$$

$$h \in (t_{\hat{h}(u)} H t_u^{-1}).$$

Therefore we obtain

$$h \in \bigcap_{u \in \Lambda} (t_{\hat{h}(u)} H t_u^{-1}).$$

Let us assume that

$$h_1 \in \bigcap_{u \in \Lambda} (t_{\hat{h}(u)} H t_u^{-1}).$$

Then we have for any $u \in \Lambda$

$$h_1 \in (t_{\hat{h}(u)} H t_u^{-1}) \Leftrightarrow h_1 t_u H = t_{\hat{h}(u)} H \Leftrightarrow$$

$$\Leftrightarrow \hat{h}_1(u) = \hat{h}(u) \Leftrightarrow (h_1^{-1}h) \in Core_G(H) = \langle e \rangle \Rightarrow h_1 = h.$$

It means that

$$h = \bigcap_{u \in \Lambda} (t_{\hat{h}(u)} H t_u^{-1}).$$

The proof is complete.

3. Loop and group transversals in groups.

Lemma 9. *Let T be a left (right) transversal in G to H. Then the following conditions are equivalent:*

1. *The system $\langle \Lambda, *, 1 \rangle$ ($\langle \Lambda, \circ, 1 \rangle$) is a loop;*

2. *T is a left (right) transversal in G to $\pi H \pi^{-1}$ for any $\pi \in G$;*

3. *The set $\pi T \pi^{-1}$ is a left (right) transversal in G to H for any $\pi \in G$.*

The **proof** is contained in [1,2].

As we can see from the next **Lemma** the simplest example of two-sided transversals are loop transversals.

Lemma 10. *The following propositions are equivalent:*

1. *T is a left loop transversal in G to H;*

2. *T is a right loop transversal in G to H;*

Proof. 1.$\Rightarrow$2. Let T be a left loop transversal in G to H. Using **Lemma 9** we have for any $x, y \in \Lambda$ $(x \neq y)$:

$$(t_x^{-1} t_y) \notin (\pi H \pi^{-1}) \qquad (*)$$

for any $\pi \in G$. Assume that T is not a right loop transversal in G to H. Then by **Lemma 9** there exist $\pi_0 \in G$ and $x_0, y_0 \in \Lambda$ such that

$$t_{x_0} = \pi_0 h \pi_0^{-1} t_{y_0}, \quad h \in H, x_0 \neq y_0.$$

Then we get:

$$t_{x_0}^{-1} t_{y_0} = t_{y_0}^{-1} \pi_0 h^{-1} \pi_0^{-1} t_{y_0} = \pi_1 h^{-1} \pi_1^{-1},$$

where $\pi_1 = t_{y_0}^{-1}\pi_0$. The last equality contradicts (*). It means, that T is a right loop transversal in G to H.

2.⇒1. The proof is analogous.

Lemma 11. *Let T be a left (right) group transversal in G to H. Then for any $x, y \in \Lambda$*

$$x * y = x \circ y.$$

Proof. Let T be a left (right) group transversal in G to H. By **Lemma 10** T is a two-sided transversal in G to H. Then using **Lemma 6** we have for any $x, y \in \Lambda$

$$x * y = x \circ y,$$

because any group is a WIP-loop. The proof is complete.

Let us introduce the next notations:

$$h_{(x*y)} = t_{x*y}^{-1} t_x t_y,$$

if T be a left transversal; and

$$h_{(x \circ y)} = t_x t_y t_{x \circ y}^{-1},$$

if T be a right transversal.

Lemma 12. *Let $Core_G(H) = \langle e \rangle$ and T be a left (right) transversal in G to H. Then the following conditions are equivalent:*

1. *T is a group transversal in G to H;*

2. *For any $x, y \in \Lambda$*

$$h_{(x*y)} = e \quad (h_{(x \circ y)} = e).$$

3. *For any $x, y \in \Lambda$*

$$t_x t_y = t_{x*y} \quad (t_x t_y = t_{x \circ y}).$$

Proof. We shall prove these equivalences for a left transversal T in G to H. The proof in the case of a right transversal in G to H is analogous.

1.⇒2. Let T be a left group transversal in G to H. Using **Lemma 4** we have for any $x, y \in \Lambda$:

$$\hat{h}_{(x*y)}(u) = \hat{t}_{x*y}^{-1}\, \hat{t}_x\, \hat{t}_y(u) = \hat{t}_{x*y}^{-1}(x*(y*u)) =$$
$$= (x*y)\backslash(x*(y*u)) = (x*y)\backslash((x*y)*u) = u,$$

i.e. $\hat{h}_{(x*y)} = \mathbf{id}$. It means that

$$h_{(x*y)} \in Core_G(H) = \langle e \rangle \Rightarrow h_{(x*y)} = e.$$

2.⇒3. It is evident.

3.⇒1. Let us have

$$t_x t_y = t_{x*y}$$

for any $x, y \in \Lambda$. Then

$$t_{x*(y*u)} = t_x t_{y*u} = t_x t_y t_u = t_{x*y} t_u = t_{(x*y)*u},$$

i.e.

$$x*(y*u) = (x*y)*u,$$

and therefore the system $\langle \Lambda, *, 1 \rangle$ is a group. It means that T is a group transversal in G to H.

The proof is complete.

4. Connection between different transversals of the same subgroup in a group.

We shall consider below that $Core_G(H) = \langle e \rangle$.

Let T be an arbitrary two-sided transversal in G to H. It is obvious that any left transversal L in G to H may be represented by T in the following way:

$$l_{x'} = t_x h_x^{(1)}, \quad h_x^{(1)} \in H, \quad x \in \Lambda, \tag{8}$$

and any right transversal R in G to H may be represented by T in the following way:

$$r_{x''} = h_x^{(2)} t_x, \quad h_x^{(2)} \in H, \quad x \in \Lambda, \tag{9}$$

Remark 1. If we pass to the permutation representation $\hat{G}$ (in the case of a left transversal L) or $\check{G}$ (in a case of the right transversal R), we obtain

$$x' = \hat{l}_{x'}(1) = \hat{t}_x \hat{h}_x^{(1)}(1) = \hat{t}_x(1) = x,$$

$$x'' = \check{r}_{x''}(1) = (1)\check{h}_x^{(2)} \check{t}_x = \check{t}_x(1) = x.$$

Remark 2. If a two-sided transversal S may be represented by a transversal T by formulas (8) and (9), then

$$s_x = t_x h_x^{(1)} = h_{x'}^{(2)} t_{x'}. \tag{10}$$

Remark 3. The following equalities are obvious:

$$h_1^{(1)} = h_1^{(2)} = e, \quad \overset{\wedge(2)}{h_{x'}}(x') = x, \quad \overset{\vee(1)}{h_x}(x) = x'.$$

Let "$\otimes$" and "$\oplus$" be notations of the operations on Λ which correspond to the new transversals L and R.

Lemma 13. *The following assertions are true:*

1. $$x \otimes y = x * (\overset{\wedge(1)}{h_x}(y)).$$

2. $$x \oplus y = (\overset{\vee(2)}{h_y}(x)) o y.$$

Proof. 1. We have:

$$s_x s_y = s_{x\otimes y} h, \quad h \in H,$$

$$t_x h_x^{(1)} t_y h_y^{(1)} = t_{x\otimes y} h_{x\otimes y}^{(1)} h, \quad h \in H,$$

$$\hat{t}_x \overset{\wedge(1)}{h_x} \hat{t}_y \overset{\wedge(1)}{h_y}(1) = \hat{t}_{x\otimes y} \overset{\wedge(1)}{h_{x\otimes y}} \hat{h}(1),$$

$$x \otimes y = x * (\overset{\wedge(1)}{h_x}(y)).$$

2. The proof is analogous to that of **1.**

Lemma 14. *Let T be an arbitrary two-sided transversal in G to H. Then the following statements are true:*

1. *If a left transversal L can be represented by a transversal T by the formula* (8), *then*

$$t_x h_x^{(1)} t_x^{-1} = \bigcap_{u\in\Lambda} (t_{x\otimes u} H t_{x*u}^{-1}).$$

2. *If a right transversal R can be represented by a transversal T by the formula* (9), *then*

$$t_x^{-1} h_x^{(2)} t_x = \bigcap_{u\in\Lambda} (t_{uox}^{-1} H t_{u\oplus x}).$$

Proof. **1.** Using **Lemma 8** we have:

$$h_x^{(1)} = \bigcap_{u\in\Lambda} (t_{\hat{h}_x^{(1)}(u)} H t_u^{-1}).$$

Therefore by **Lemma 13**

$$t_x h_x^{(1)} t_x^{-1} = \bigcap_{u\in\Lambda} (t_x t_{\hat{h}_x^{(1)}(u)} H t_u^{-1} t_x^{-1}) =$$

$$= \bigcap_{u\in\Lambda} (t_{x*\hat{h}_x^{(1)}(u)} H t_{x*u}^{-1}) = \bigcap_{u\in\Lambda} (t_{x\otimes u} H t_{x*u}^{-1}).$$

2. The proof is analogous to that of **1.**

5. Structural theorem.

Lemma 15. *Let K be a subgroup in G and $H \subseteq K \subset G$. Then:*

1. *If T is a left (right) transversal in G to H, then there exists a right (left) subquasigroup $<\Lambda_1, *, 1>$ $(<\Lambda_1, \circ, 1>)$ in the right (left) quasigroup $<\Lambda, *, 1>$ $(<\Lambda, \circ, 1>)$; moreover, if $(G:H) = |\Lambda| < \infty$, then $|\Lambda_1|$ divides $|\Lambda|$;*

2. *If T is a two-sided transversal in G to H, then all assertions from* **1** *take place;*

3. *If T is a loop transversal in G to H then:*

$<\Lambda_1, *, 1>$ is a subloop in the loop $<\Lambda, *, 1>$;

$<\Lambda_1, \circ, 1>$ is a subloop in the loop $<\Lambda, \circ, 1>$,

and if $|\Lambda| < \infty$, then $|\Lambda_1|$ divides $|\Lambda|$.

Proof. **1.** Let us consider a partition of the subgroup K on the left cosets of the subgroup H:

$$K = \bigcup_{i\in\Lambda_1} {}_iH = \bigcup_{i\in\Lambda_1} k_i H.$$

It is evident that this partition can be completed to a partition of G on the left cosets of H:

$$G = \bigcup_{i\in\Lambda} {}_iH.$$

Therefore there exists a left subtransversal $T_1 \subset K$ in a left transversal T, which is indexed by elements of Λ_1. All products of elements from T_1 lie in K and so the system $<\Lambda_1,*,1>$ is a subsystem in $<\Lambda,*,1>$.

The proof for the system $<\Lambda_1,o,1>$ is analogous.

If $(G:H)=|\Lambda|=m_0<\infty$, then:

$$|\Lambda_1|=(K:H)=m_1<\infty,$$
$$(G:K)=m_2<\infty.$$

We obtain:

$$(G:H)=(G:K)\cdot(K:H),$$
$$m_0=m_2\cdot m_1,$$

i.e. $|\Lambda_1|$ divides $|\Lambda|$.

2. It is an easy corollary of **1.**

3. If T is a loop transversal in G to H then the system $<\Lambda,*,1>$ is a loop. By the point **1** of this **Lemma** the system $<\Lambda_1,*,1>$ is a subsystem in a loop $<\Lambda,*,1>$, i.e. $<\Lambda_1,*,1>$ is a subloop in $<\Lambda,*,1>$. Analogously for the system $<\Lambda_1,o,1>$.

Corollary. *Let a loop transversal in G to H does not exist. Then a loop transversal in G to H for any group $G^* \supseteq G$ does not exist too.*

Proof. It is an easy corollary of **Lemma 15.**

6. A criterion of loop transversal existence in a group.

Lemma 16. *Let $Core_G(H)=<e>$, $H^*=St_1(S_d)$, $d=|\Lambda|=(G:H)$. Then the following assertions are equivalent:*

1. *There exists a loop transversal in G to H;*
2. *There exists a set $\{h_x\}_{x\in\Lambda}$ satisfying the following conditions:*

a. $\hat{h}_1=$ **id** *and for any* $x\in\Lambda\setminus\{1\}$

$$\hat{h}_x\in((1x)\cdot\hat{G})\cap H^*;$$

b. *for any* $u\in\Lambda$

$$\bigcap_{x\in\Lambda}\{(1u)(1x)\hat{h}_x(1u)H^*(1x)\}\neq\varnothing.$$

3. *There exists a set* $\{h^{(u)}\}_{u\in\Lambda}$ *satisfying the following conditions:*

a. $\hat{h}^{(1)} = \mathbf{id}$ *and* $\hat{h}^{(u)} \in H^*$ *for any* $u \in \Lambda$;

b. *for any* $x \in \Lambda$

$$\bigcap_{u\in\Lambda}\{\hat{G}\cap((1u)\hat{h}^{(u)}(1x)H^*(1u))\}\neq\varnothing.$$

4.
$$K(G)\neq\varnothing,$$

where $\hat{h}^{(1)} = \mathbf{id}$ *and*

$$K(G)=\bigcup_{(h^{(1)},\dots,h^{(d)})\in(H^*)^d}\ \bigcup_{\alpha\in S_d}\prod_{x\in\Lambda}\{\hat{G}\cap(\bigcap_{u\in\Lambda}((1u)\hat{h}^{(u)}(1\alpha(x))H^*(1u)))\}.$$

Proof.

1.⇒2. Let T be a loop transversal in G to H, $Core_G(H) = <e>$ and $(G:H) = d$. Let us consider the loop $L = <\Lambda, *, 1>$ corresponding to the transversal T and take left and right translations of the loop L:

$$L_u(x) = u * x = \hat{t}_u(x),$$

$$R_u(x) = x * u = \hat{t}_x(u).$$

Since $Core_G(H) = <e>$, then $\hat{G} \cong G$ and the degree of permutations from $\hat{G}$ is equal d. Sets

$$L^* = \{L_u | u \in \Lambda\}, \qquad R^* = \{R_u | u \in \Lambda\}$$

are loop transversals in G to H, because L is a loop. By **Lemma 4,** L^* and R^* are sharply transitive sets of permutations on Λ. Therefore again by **Lemma 4** L^* and R^* are loop transversals in S_d to $H^* = St_1(S_d)$. Then for any $u \in \Lambda$ there exists an unique element $h_{(u)} \in H^*$ such that

$$L_u h_{(u)} = R_{\varphi(u)},$$

where φ is a permutation on Λ. Therefore for any $u \in \Lambda$ there exists an unique element $h_{(u)} \in H^*$ such that

$$L_u \hat{h}_{(u)}(x) = R_{\varphi(u)}(x) \qquad (*)$$

for any $x \in \Lambda$. If $x=1$, then we have from (*):

$$u = L_u(1) = R_{\varphi(u)}(1) = \varphi(u).$$

Therefore the identity (*) may be written in the following form

$$\hat{t}_u \hat{h}_{(u)}(x) = \hat{t}_x(u)$$

for any $x \in \Lambda$. Then we have for any $x \in \Lambda$:

$$t_u h_{(u)} t_x H^* = t_x t_u H^*,$$

$$h_{(u)} \in (t_u^{-1} t_x t_u H^* t_x^{-1}),$$

and therefore

$$h_{(u)} \in \bigcap_{x \in \Lambda} (t_u^{-1} t_x t_u H^* t_x^{-1}). \tag{11}$$

Let us consider the following two-sided transversal P_0 in S_d to H^*:

$$P_0 = \{(1x) | x \in \Lambda\},$$

where *(1x)* is a *transposition* of S_d. Since T is a two-sided transversal (see **Lemma 10**), then there exists a set $\{h_x\}_{x \in \Lambda}$ (see (8)), such that

$$\hat{h}_1 = \mathbf{id};$$

$$\hat{t}_x = (1x)\hat{h}_x, \quad x \neq 1. \tag{11'}$$

We have for any $x \in \Lambda \setminus \{1\}$:

$$H^* \supset \hat{h}_x = ((1x)\hat{t}_x) \in ((1x) \cdot \hat{G}),$$

$$\hat{h}_x \in ((1x) \cdot \hat{G}) \cap H^*.$$

Using this and (11)-(11') we have for any $u \in \Lambda$:

$$h_u' = (h_u h_{(u)}) \in \bigcap_{x \in \Lambda} ((1u)(1x)\hat{h}_x (1u) H^* (1x)). \tag{12}$$

By **Lemma 8** (since $Core_G(H) = \langle e \rangle$) the intersection in (12) consists of an unique element (if this intersection exists). Then the identity (12) may be written in a following form:

$$\bigcap_{x \in \Lambda} \{(1u)(1x)\hat{h}_x (1u) H^* (1x)\} \neq \varnothing.$$

2.⇒3. Let conditions of **2.** hold. Then by **2.b.** and (12) we have for any $u \in \Lambda$:

$$(1u)(1x)\hat{h}_x (1u) \hat{h}_1^{(x)} (1x) = \hat{h}^{(u)}$$

for any $x \in \Lambda \setminus \{1\}$ and some $\hat{h}_1^{(x)} \in H^*$. In particular, from **2.b.** we get:

$$\hat{h}^{(1)} = \bigcap_{x \in \Lambda} ((1x)\hat{h}_x H^* (1x)) = \{\mathbf{id}\}.$$

Therefore we obtain:

$$\hat{h}_x = ((1x)(1u)\hat{h}^{(u)} (1x)(\hat{h}_1^{(x)})^{-1}(1u)) \in ((1x)(1u)\hat{h}^{(u)} (1x) H^* (1u)).$$

Using **2.a.** we have for any $x \in \Lambda \setminus \{1\}$ and $u \in \Lambda$:

$$\hat{h}_x \in H^* \cap ((1x)\hat{G}) \cap ((1x)(1u)\hat{h}^{(u)}(1x)H^*(1u)),$$

and therefore

$$\hat{h}_x \in \bigcap_{u\in\Lambda} \{H^* \cap ((1x)\hat{G}) \cap ((1x)(1u)\hat{h}^{(u)}(1x)H^*(1u))\}. \tag{13}$$

Using **Lemma 8** and (13) we get

$$\hat{h}_x = \bigcap_{u\in\Lambda} \{((1x)\hat{G}) \cap ((1x)(1u)\hat{h}^{(u)}(1x)H^*(1u))\},$$

because $\hat{h}^{(1)} = \mathbf{id}$. Therefore we have for any $x \in \Lambda$:

$$\bigcap_{u\in\Lambda} \{\hat{G} \cap ((1u)\hat{h}^{(u)}(1x)H^*(1u))\} = ((1x)\hat{h}_x) \neq \varnothing.$$

3.⇒4. Let all conditions of **3.** hold. Then we have for any $\alpha \in S_d$ and $x \in \Lambda$:

$$\bigcap_{u\in\Lambda} \{\hat{G} \cap ((1u)\hat{h}^{(u)}(1\alpha(x))H^*(1u))\} \neq \varnothing.$$

Therefore for the set $\{\hat{h}^{(u)}\}_{u\in\Lambda}$ we obtain

$$\bigcup_{\alpha\in S_d} \prod_{x\in\Lambda} \{ \bigcap_{u\in\Lambda} (\hat{G} \cap ((1u)\hat{h}^{(u)}(1\alpha(x))H^*(1u)))\} \neq \varnothing.$$

Then

$$K(G) \neq \varnothing,$$

where $K(G)$ is the set defined in the condition **4.** of this **Lemma.**

4.⇒1. Let conditions of **4.** hold. We know (see **Lemma 8**) that the intersection

$$\bigcap_{u\in\Lambda} \{(1u)\hat{h}^{(u)}(1x)H^*(1u)\}$$

is either empty or contains an unique element g_x. Therefore we have:

$$g_x = \bigcap_{u\in\Lambda} \{(1u)\hat{h}^{(u)}(1x)H^*(1u)\},$$

$$g_x \in \{(1u)\hat{h}^{(u)}(1x)H^*(1u)\} \quad \text{for any } u \in \Lambda,$$

$$g_x(1u)H^* = (1u)\hat{h}^{(u)}(1x)H^* \quad \text{for any } u \in \Lambda,$$

$$\hat{g}_x(u) = u \bullet \hat{h}^{(u)}(x) \quad \text{for any } u \in \Lambda,$$

where operation "•" corresponds to the transversal

$$P_0 = \{(1x) | x \in \Lambda\}.$$

So the following two conditions are equivalent:

a) for any $\alpha \in S_d$

$$\prod_{x\in\Lambda} \{\hat{G} \cap (\bigcap_{u\in\Lambda} ((1u)\hat{h}^{(u)} (1\alpha(x))H^*(1u)))\} \neq \varnothing;$$

b) for any $x \in \Lambda$ the mapping

$$\gamma_x(u) = u \bullet \hat{h}^{(u)}(x)$$

is a permutation on Λ.

Let us define the following operation on Λ:

$$x \cdot y = \gamma_x(y) = y \bullet \hat{h}^{(y)}(x)$$

and prove that the system $<\Lambda,\cdot,1>$ is a loop.

We have for the operation "•" (see (1)):

$$x \bullet y = \begin{cases} x, & \text{if} \quad y = 1; \\ 1, & \text{if} \quad y = x; \\ y, & \text{if} \quad y \neq 1, x; \end{cases}$$

Therefore

$$x \cdot 1 = 1 \bullet \hat{h}^{(1)}(x) = 1 \bullet x = x;$$

$$1 \cdot x = x \bullet \hat{h}^{(x)}(1) = x \bullet 1 = x.$$

We have for given $a, b \in \Lambda$:

$$a \cdot x = b \Leftrightarrow \gamma_a(x) = b \Leftrightarrow x = \gamma_a^{-1}(b).$$

Since γ is a permutation on Λ, such an element x in Λ is unique. Finally, we get for arbitrary given $a, b \in \Lambda$:

$$x \cdot a = b,$$

$$a \bullet \hat{h}^{(a)}(x) = b,$$

$$\hat{h}^{(a)}(x) = \begin{cases} 1, & \text{if} \quad b = a; \\ a, & \text{if} \quad b = 1; \\ b, & \text{if} \quad \hat{h}^{(a)}(x) \neq 1, a; \end{cases}$$

$$x = \begin{cases} 1, & if \quad b = a; \\ (\hat{h}^{(a)})^{-1}(a), & if \quad b = 1; \\ (\hat{h}^{(a)})^{-1}(b), & if \quad b \neq 1, a; \end{cases}$$

So the system $<\Lambda, \cdot, 1>$ is a loop.

Finally we can see:

$$\hat{g}_a(x) = x \bullet \hat{h}^{(x)}(a) = a \cdot x = L_a(x),$$

where L_a is a left translation on $<\Lambda, \cdot, 1>$. Since $\hat{g}_a \in \hat{G}$, then $L_a \in \hat{G}$, i.e. the set

$$L = \{L_a | a \in \Lambda\}$$

is a loop transversal in G to H. The proof is complete.

Lemma 17. *In notations of* **Lemma 16** *the following assertions is true for any* $\pi \in S_d$

$$\pi K(G)\pi^{-1} = K(\pi G \pi^{-1}).$$

Proof. Using the proof of **Lemma 16** we have:

$$K(G) = \bigcup_{L} \bigcup_{\alpha \in S_d} \{\prod_{x \in \Lambda} (\hat{G} \cap L_{\alpha(x)})\},$$

where L is an arbitrary loop on Λ. Then we have for any $\pi \in S_d$:

$$\pi K(G)\pi^{-1} = \bigcup_{L} \bigcup_{\alpha \in S_d} \{\pi(\prod_{x \in \Lambda} (\hat{G} \cap L_{\alpha(x)}))\pi^{-1}\} =$$

$$= \bigcup_{L} \bigcup_{\alpha \in S_d} \{\prod_{x \in \Lambda} ((\pi \hat{G} \pi^{-1}) \cap (\pi L_{\alpha(x)} \pi^{-1}))\} =$$

$$= \bigcup_{L'} \bigcup_{\alpha' \in S_d} \{\prod_{x \in \Lambda} ((\pi \hat{G} \pi^{-1}) \cap L'_{\alpha'(x)})\} = K(\pi \hat{G} \pi^{-1}),$$

where L'_a is a left translation in a some loop L'. The last equality is based on the following sequence of statements:

T is a loop transversal in G to H $\Leftrightarrow$

for any $\alpha \in G$ the set $(\alpha T \alpha^{-1})$ is a left transversal in G to H $\Leftrightarrow$

$$\text{for any} \quad \pi \in S_d \quad \text{and} \quad \alpha \in G \quad \text{the set} \quad (\pi\alpha T(\pi\alpha)^{-1}) \quad \text{is}$$

$$\text{a left transversal in} \quad (\pi\hat{G}\pi^{-1}) \quad \text{to} \quad (\pi\hat{H}\pi^{-1}) \Leftrightarrow$$

$$\text{for any} \quad \pi \in S_d \quad \text{and} \quad \alpha_1 \in (\pi G\pi^{-1}) \quad \text{the set} \quad (\alpha_1(\pi T\pi^{-1})\alpha_1^{-1}) \quad \text{is}$$

$$\text{a left transversal in} \quad (\pi\hat{G}\pi^{-1}) \quad \text{to} \quad (\pi\hat{H}\pi^{-1}) \Leftrightarrow$$

$$T' = (\pi T\pi^{-1}) \quad \text{is a loop transversal in} \quad (\pi\hat{G}\pi^{-1}) \quad \text{to} \quad (\pi\hat{H}\pi^{-1}).$$

The proof is complete.

References

1. *Baer R.* Nets and groups. 1. Trans. Amer. Math. Soc., v.**46**(1939), p.110-141.

2. *Johnson K.W. S*-rings over loops, right mapping groups and transversals in permutation groups. Math. Proc. Camb. Phil. Soc., v.**89**(1981), p.433-443.

3. *Ore O.* On coset representatives in groups. Proc. Amer. Math. Soc., v.**9**(1958), p.665-670.

4. *Kargapolov M.I., Merzlyakov Y.I.* Foundations of group theory. (Russian), Ed. 3, Moscow, "Nauka", 1982.

5. *Belousov V.D.* Foundations of quasigroup and loop theory. (Russian), Moscow, "Nauka", 1967.

6. *Niemenmaa M., Kepka T.* On multiplication groups of loops. J. of Algebra, v.**135**(1990), p.112-122.

Kuznetsov E.A. **Ph.D.**
department of quasigroup theory,
Institute of Mathematics,
Academy of Sciences of Moldova,
5, Academiei str.,
Kishinau, 277028,
Moldova.

Received August 15, 1993

Quasigroups and related systems, vol. 1, no. 1(1), 1994

SHARPLY k-TRANSITIVE SETS OF PERMUTATIONS AND LOOP TRANSVERSALS IN S_n

Evgenii A. Kuznetsov

Abstract

The work is devoted to the investigation of sharply k-transitive sets of permutations which are a natural generalization of sharply k-transitive groups. Its main result is the establishment of the connection between such notions as sharply k-transitive sets of permutations, sharply k-transitive loops of permutations (introduced by F.Bonetti, G.Lunardon and K.Strambach) and loop transversals.

One special class of sets of permutations - sharply multiple transitive permutation sets - is studied in this work. These sets are the natural generalization of sharply multiple transitive permutation groups [3,4,5], but in contrast to the former are not described in the mathematical literature. On the other side, various known algebraical and geometrical problems are reduced to the research of conditions of existance and properties of sets mentioned above ([1], the end of §1.7; [2]).

To find the connection between the sets mentioned above, sharply k-transitive loops of permutations [9] and loop transversals in groups [6,7] is the main aim of this investigation. This connection allows us to describe the pure combinatorical objects - sharply multiple transitive sets of permutations - in terms of loop transversals of subgroups in groups. Moreover, since there exists a connection between finite projective planes and sharply 2-transitive sets of permutations (see [2,8]), the well-known problems of existence and of the number of projective planes of given order may be reformulated and studied in terms of loop transversals in the symmetric group S_n.

The main result of this work is

Theorem 1. *Let X be a set, $cardX=n$ and $1\le k\le n$. Then the following conditions are equivalent:*

1. *there exists a sharply k-transitive set of permutations on X;*
2. *there exists a sharply k-transitive loop of permutations on X;*
3. *there exists a loop transversal in S_n to $St_{1,\dots,k}(S_n)$;*

It is supposed that $1,2,\ldots\in X$.

Using the results from [2,8] and the **Theorem 1**, we have

Theorem 2. *The following conditions are equivalent:*

1. *there exists a finite projective plane of order n;*
2. *there exists a loop transversal in S_n to $St_{1,2}(S_n)$;*

Let us pass to the detailed description of the paper results with all necessary definitions and notations.

1. The necessary definitions.

Definition 1.[1] A set M of permutations on X is called *sharply (strongly) k-transitive* ($1\le k\le cardX$), if for any two k-tuples $(a_1,\ldots,a_k)$ and $(b_1,\ldots,b_k)$ of different elements from X there exist the unique permutation $\alpha\in M$ satisfying the following conditions:

$$\alpha(a_i)=b_i$$

for any $i=1,\ldots,k$. If the set M is closed relative to the multiplication of permutations, then M is a *sharply k-transitive group of permutations on* X.

Definition 2.[9] A loop G is called a *loop of permutations on the set X*, if there exists a map (action)

$$f:G\times X\to X,$$
$$f(g,x)=g(x),$$

which satisfies the following conditions:

1. $e(x)=x$ for any $x\in X$, where e is the unit of the loop G;
2. If b lies in the kernel of the loop G ([10], p.13), then
$$(ab)(x)=a(b(x))$$
for any $a\in G$ and $x\in X$;

3. There exists an element $x_0 \in X$ such that the set

$$G_{x_0} = \{a \in G | a(x_0) = x_0\}$$

is a subloop in G, and:

a) If $b \in G_{x_0}$ and $a \in G$, then

$$(ba)(x_0) = b(a(x_0));$$

b) If $a_1, a_2 \in G$ and $a_1(x_0) \neq x_0$, then

$$(a_2 a_1)(x_0) \neq a_2(x_0);$$

c) If $a_2 \notin G_{a_1(x_0)}$, then

$$(a_2 a_1)(x_0) \neq a_1(x_0);$$

If a loop of permutations on X is sharply k-transitive (as a set of permutations), then it is called a *sharply k-transitive loop of permutations on X.*

Definition 3. Let G be a group and H a subgroup of G. A complete system T of representatives of the left (right) cosets in G to H (unit $e \in T$) is called the *left (right) transversal in G to H.*

We can correctly introduce on T the following operation:

$$t_1 * t_2 = t_3 \Leftrightarrow t_1 t_2 = t_3 h, \quad h \in H. \tag{1}$$

If the system $< T, *, e >$ is a loop, then the transversal T in G to H is called the *loop transversal.*

In [6] it was proved

Lemma 1. *The following conditions are equivalent for left (right) transversal T in G to H:*

1. *T is a loop transversal;*
2. *T is a left (right) transversal in G to $\pi H \pi^{-1}$ for any $\pi \in G$;*
3. *$\pi H \pi^{-1}$ is a left (right) transversal in G to H for any $\pi \in G$.*

2. Proof of the Theorem 1.

Definition 4. Let M be a set of permutations on X. If **id**$\in M$ (where **id** is the identity permutation on X), then the set M is called a *reduced set* of permutations.

Lemma 2. *The following conditions are equivalent:*

1. *There exists a sharply k-transitive set of permutations on X;*
2. *There exists a reduced sharply k-transitive set of permutations on X.*

Proof. 2.⇒1. It is evident.

1.⇒2. Let M be a sharply k-transitive set of permutations on X. If $\mathbf{id} \in M$ then all is proved. Let $\mathbf{id} \notin M$. Let us take an arbitrary element $\alpha_0 \in M$ and introduce the following set:

$$M_0 = \{\alpha_0^{-1}\beta | \beta \in M\} = \alpha_0^{-1}M.$$

Since $\alpha_0 \in M$ then $\mathbf{id} \in M_0$, i.e. M_0 is a reduced set of permutations. Let $(a_1,\dots,a_k)$ and $(b_1,\dots,b_k)$ be any two k-tuples of different elements from X. Using the sharply k-transitivity of M we have that there exists the unique permutation $\beta_0 \in M$ such that

$$b_0(a_i) = a_0(b_i)$$

for any $i=1,\dots,k$, i.e.

$$(\alpha_0^{-1}\beta_0)(a_i) = b_i$$

for any $i=1,\dots,k$. Therefore there exists the unique permutation $\gamma_0 = \alpha_0^{-1}\beta_0 \in M$ such that

$$\gamma_0(a_i) = b_i$$

for any $i=1,\dots,k$, i.e. M_0 is a sharply k-transitive set of permutations.

Lemma 3. *The following conditions are equivalent:*

1. M_0 *is a reduced sharply k-transitive set of permutations on X;*
2. M_0 *is a loop transversal in* S_n *to* $St_{1,\dots,k}(S_n)$; $n = cardX$.

Proof. 1.⇒2. Let M_0 be a reduced sharply k-transitive set of permutations on X, $cardX=n$. The left (right) cosets in S_n to subgroup $H_0 = St_{1,\dots,k}(S_n)$ are sets of the following kind:

$$G_{a_1,\dots,a_k} = \{\alpha \in S_n | \alpha(i) = a_i, i = 1,\dots,k\},$$

where $(a_1,\dots,a_k)$ may be any k-tuples of different elements from X. Using the sharply k-transitivity of M_0, obtain that every coset of S_n to H_0 contains exactly one element from M_0, $\mathbf{id} \in M_0$ too. It means M_0 is the left transversal in S_n to H_0.

We must prove that M_0 is a loop transversal in S_n to H_0. It is sufficient (see **Lemma 1**) to prove that M_0 is a left transversal in S_n to $\pi H_0 \pi^{-1}$, where $\pi \in S_n$. Let π be an arbitrary element from S_n and

$$\pi(i) = a_i, \quad i = 1,\dots,k.$$

Then we have

$$(\pi h \pi^{-1})(a_i) = \pi h(i) = \pi(i) = a_i$$

for any $h \in H_0$, i.e.

$$\pi H_0 \pi^{-1} = St_{a_1,\dots,a_k}(S_n) = H_\pi.$$

Let us define the following sets:

$$G_\alpha = \alpha H_\pi,$$

where $\alpha \in M_0$. It is obvious that $G_{id} = H_\pi$. If we assume

$$\gamma \in (G_\alpha \cap G_\beta) \neq \varnothing, \quad \alpha \neq \beta,$$

then

$$\gamma = \alpha h_1 = \beta h_2, \quad h_1, h_2 \in H_\pi,$$

$$\alpha^{-1}\beta = h_1 h_2^{-1} \in H_\pi,$$

i.e.

$$\beta = \alpha H_\pi,$$

and

$$\alpha_2(a_i) = \alpha_1(a_i)$$

for any $i=1,\dots,k$. It's impossible, since M_0 is sharply k-transitive set. So

$$G_\alpha \cap G_\beta = \varnothing, \quad \text{if } \alpha \neq \beta.$$

Let g be an arbitrary element from S_n and

$$g(a_i) = c_i, \quad i = 1,\dots,k.$$

Then since M_0 is a k-transitive set of permutations, there exists an element $\alpha_0 \in M_0$ such that

$$\alpha_0(a_i) = c_i, \quad i = 1,\dots,k.$$

Therefore

$$(\alpha_0^{-1} g)(a_i) = \alpha_0^{-1}(c_i) = a_i$$

for any $i=1,\dots,k$, i.e.

$$(\alpha_0^{-1} g) \in H_\pi$$

and

$$g \in \alpha_0 H_\pi = G_{\alpha_0}.$$

It is proved that $\{G_\alpha\}_{\alpha \in M_0}$ is a complete system of left cosets in S_n to $St_{a_1,\dots,a_k}(S_n)$; therefore M_0 is a left transversal in S_n to $St_{a_1,\dots,a_k}(S_n)$.

2.⇒1. The reasoning is carried out in the opposite direction.

The proof is complete.

Lemma 4. *The following conditions are equivalent:*

1. *There exists a sharply k-transitive loop of permutations on X;*
2. *There exists a loop transversal in S_n to $St_{1,\dots,k}(S_n)$; n=cardX.*

Proof. 1.⇒2. A sharply k-transitive loop of permutations on **X** is a sharply k-transitive set of permutations on X. Therefore this implication is a corollary of **Lemma 3.**

2.⇒1. Let T be a loop transversal in S_n to $St_{1,\dots,k}(S_n)$. Then the system A=<T,*,**id**> is a loop, where "*" is defined in (1). We shall show that this loop is a sharply k-transitive loop of permutations on X.

The reflection f (see **Definition 2**) is defined naturally, because $T \subset S_n$. It is necessary to prove that the conditions **1.-3.** from **Definition 2** are satisfied. Let us denote $H = St_{1,\dots,k}(S_n)$.

The condition **1.** is satisfied, because **id**$\in T$ and **id** is the unit of the loop A.

Let us verify condition **2.** Let b_0 lie in the kernel of the loop A, i.e. for any $x, y \in A$:

$$(b_0 * x) * y = b_0 * (x * y),$$
$$(x * y) * b_0 = x * (y * b_0),$$
$$(x * b_0) * y = x * (b_0 * y).$$

From the last equality we have

$$x b_0 h_1^{-1} y h_2^{-1} = x b_0 y h_3^{-1} h_4^{-1},$$

where

$$x * b_0 = x b_0 h_1, \qquad b_0 * y = b_0 y h_3,$$
$$(x * b_0) * y = (x * b_0) y h_2, \quad x * (b_0 * y) = x (b_0 * y) h_4, \quad h_1, h_2, h_3, h_4 \in H.$$

Then for any $y \in A$

$$h_1^{-1} = (y h^* y^{-1}) \in (y H y^{-1}),$$

where $h^* = (h_3^{-1} h_4^{-1} h_2) \in H$. Therefore

$$h_1^{-1} \in \bigcap_{y \in A} (y H y^{-1}) = \bigcap_{g \in S_n} (g H g^{-1}) = Core_{S_n}(H) = <\mathbf{id}>,$$

because T is a transversal in S_n to H. Therefore $h_1 = \mathbf{id}$, and

$$x * b_0 = x b_0$$

for any $x \in A$. Then for any $x \in X$ and $a \in A$

$$(a * b_0)(x) = (a b_0)(x) = a(b_0(x)).$$

Let us show that condition **3.** from **Definition 2** is satisfied. We will take $x_0 = 1 \in X$. Then the set

$$G_1 = \{\alpha \in A | \alpha(1) = 1\}$$

is a subloop in A. Indeed, $\mathbf{id} \in G_1$, and if $\alpha, \beta \in G_1$ then we have for $\gamma = \alpha * \beta$:

$$\gamma(1) = (\alpha * \beta)(1) = (\alpha\beta h)(1) = (\alpha\beta)(1) = \alpha(1) = 1,$$

where $h \in H$; i.e. $\gamma \in G_1$, and G_1 is closed under the operation "*" in A.

If $b \in G_1$ and $a \in A$ then

$$(b * a)(1) = (bah)(1) = (ba)(1) = b(a(1)),$$

where $h \in H$, i.e. condition **3a.** is satisfied.

If $a_1, a_2 \in A$ and $a_1 \neq 1$ then

$$(a_2 * a_1)(1) = (a_2 a_1 h)(1) = (a_2 a_1)(1) = a_2(a_1(1)) \neq a_2(1),$$

because a_2 is a permutation from S_n, $h \in H$. Therefore the condition **3b.** is satisfied.

If

$$a_2 \notin G_{a_1(1)} = \{\alpha \in A | \alpha(a_1(1)) = a_1(1)\},$$

then

$$(a_2 * a_1)(1) = (a_2 a_1 h)(1) = (a_2 a_1)(1) = a_2(a_1(1)) \neq a_1(1),$$

where $h \in H$; i.e. condition **3c.** is satisfied.

It means that A is a loop of permutations on X. Using **Lemma 3** we have that A is a sharply k-transitive set of permutations on X. Therefore A is a sharply k-transitive loop of permutations on X. The proof is complete.

Theorem 1 is a simple corollary from **Lemmas 2-4**.

3. Proof of Theorem 2.

The author of this paper has proved in [8] the existence of correspondence between a projective plane of order n and the DK-ternar of order n coordinatizing this plane. Up to certain four fixed points in general position on the projective plane this is a 1-1 correspondence. In **Theorem 5** from [8] is proved that the cell permutations of a DK-ternar form a sharply 2-transitive set of permutations of degree n. It means that a projective plane of order n exists if and only if a sharply 2-transitive set of permutations of degree n exists (see [2] too). Using this reasonings we get **Theorem 2** from the **Theorem 1** when k=2.

References

1. *Bannai A., Ito T.* Algebraical combinatorics.1. Designs of relations (Russian). "Mir", Moscow, 1987.

2. *Lorimer P.* Finite projective planes and sharply 2-transitive subsets of finite groups. Springer Lect. Notes Series of Math., v.**372**(1973), p.432-436.

3. *Hall M.* Group theory (Russian). IL, Moscow, 1962.

4. *Wielandt H.* Finite permutation groups. Acad. Press, N.Y. 1964.

5. *Zassenhaus H.* Uberendliche Fastkorper. Abh. Mat. Sem. Hamburg, v.**11**(1936), p.187-220.

6. *Baer R.* Nets and groups.1. Trans. Amer. Math. Soc., v.**46**(1939), p.110-141.

7. *Johnson K.W.* *S*-rings over loops, right mapping groups and transversals in permutation groups. Math. Proc. Camb. Phil. Soc., v.**89**(1981), p.433-443.

8. *Kuznetsov E.A.* About of one class of ternary systems (Russian). In: "Kvazigruppi", vyp. 95, Kishinev, "Shtiintsa", 1987, p.71-85.

9. *Bonetti F., Lunardon G., Strambach K.* Cappi di permutazioni. Rend. Math., v.**12**(1979), No 3-4, p.383-395.

10. *Belousov V.D.* Foundations of the theory of Quasigroups and Loops (Russian), "Nauka", Moscow, 1967, 223 pp.

Kuznetsov E.A. **Ph.D.**
department of quasigroup theory,
Institute of Mathematics,
Academy of Sciences of Moldova,
5, Academiei str.,
Kishinau, 277028,
Moldova.

Received August 10, 1993.

Quasigroups and related systems, vol. **1**, no.1(1), 1994

OSBORN'S G-LOOPS

Alexandr S. Basarab

Abstract

It is proved, that if in a loop Q(·) the equality

$$(\cdot)_{I^{-1}x} = {}_{Ix}(\cdot)$$

holds for every $x \in Q$, then Q(·) is a G-loop. From this result it follows that:

a) An Osborn's loop Q(·) in which $x^2 \in N$ for every $x \in Q$ is a G-loop;
b) Every *i*-loop is a G-loop.

In the present work we continue the study of the class of *G*-loops which sprang from works [1], [2]. It is proved that if in the loop Q(·) the equality

$$(\cdot)_{I^{-1}x} = {}_{Ix}(\cdot)$$

holds for every $x \in Q$, then Q(·) is a *G*-loop.

Firstly we remind for some definitions and results which are necessary for proof of the main result of the present work.

The operation $(\cdot)_a$, defined by the equality

$$(\cdot)_a = (\cdot)^{(L_a, 1, L_a)}$$

is called the *right derivative operation of* (·). Analogously, the operation

$${}_a(\cdot) = (\cdot)^{(1, R_a, R_a)}$$

is called the *left derivative operation of* (·) (a is a fixed element of Q, $Q(\cdot)$ is a loop).

A loop $Q(\cdot)$ is called a *G-loop*, if all the right and left derivative operations of the loop $Q(\cdot)$ are isomorphic to the operation (·).

A loop Q(·) is a *G*-loop if and only if every loop $Q(\cdot)$ which is isotopic to Q(·) will be isomorphic to Q(·) (see [3]).

A loop $Q(\cdot)$ in which the equality

$$I(xy) \cdot I^2 x = Iy$$

holds is called an WIP_1-loop. In a WIP_1-loop translations L_x and R_x ar connected as follows:

$$IL_{I^{-1}x}I^{-1} = R_{Ix}^{-1}, \quad I^{-1}R_{Ix}I = L_{I^{-1}x}^{-1}. \qquad (1$$

If $T=(\alpha,\beta,\gamma)$ is an autotopy of an WIP_1-loop $Q(\cdot)$, then

$$T_1 = (I\gamma I^{-1}, I^2\alpha I^{-2}, I\beta I^{-1}) \quad \text{and} \quad T_2 = (I^{-2}\beta I^2, I^{-1}\gamma I, I^{-1}\alpha I) \qquad (2$$

are also autotopies of the loop $Q(\cdot)$.

Theorem 1. *A loop $Q(\cdot)$ in which the equality*

$$(\cdot)_{I^{-1}x} = {}_{Ix}(\cdot) \qquad (3$$

holds for every $x\in Q$ is a G-loop.

Proof. Let (3) be fulfilled in the loop $Q(\cdot)$, then

$$(\cdot)^{(L_{I^{-1}x},1,L_{I^{-1}x})} = (\cdot)^{(1,R_{Ix},R_{Ix})},$$

whence we get the autotopy

$$T = (L_{I^{-1}x}, R_{Ix}^{-1}, L_{I^{-1}x}R_{Ix}^{-1}).$$

From T the equality

$$(I^{-1}x\cdot y)\cdot R_{Ix}^{-1}z = I^{-1}x\cdot R_{Ix}^{-1}(y\cdot z) \qquad (4$$

follows. In (4) putting $R_{Ix}z$ instead of z and after that Ix instead of x we get

$$xy\cdot z = x\cdot R_{I^2x}^{-1}(y\cdot zI^2x). \qquad (5$$

Let $z = I(x\cdot y)$ in (5), then

$$1 = x\cdot R_{I^2x}^{-1}(y\cdot I(x\cdot y)\cdot I^2x),$$

whence

$$Ix = R_{I^2x}^{-1}(y\cdot I(xy)I^2x),$$

$$y\cdot I(xy)I^2x = R_{I^2x}Ix,$$

$$y\cdot I(xy)I^2x = 1,$$

$$I(x\cdot y)\cdot I^2x = Iy,$$

i.e. $Q(\cdot)$ is an WIP_1-loop. Applying (2) and (1) to T we obtain

$$T_1 = (IL_{I^{-1}x}R_{Ix}^{-1}I^{-1}, I^2L_{I^{-1}x}I^2, IR_{Ix}^{-1}I^{-1}) =$$

$$= (R_{Ix}^{-1}IR_{Ix}^{-1}I^{-1}, R_{Ix}R_{Ix}^{-1}IR_{Ix}^{-1}I^{-1}, R_{Ix}R_{Ix}^{-1}IR_{Ix}^{-1}I^{-1}) =$$

$$= (\alpha^{-1}, R_{Ix}\alpha^{-1}, R_{Ix}\alpha^{-1}),$$

$$\alpha^{-1}1 = 1,$$

whence it follows

$$ {}_{Ix}(\cdot) = (\cdot)^{\alpha} \qquad (6) $$

From (3) and (6) it follows

$$ (\cdot)_{I^{-1}x} = {}_{Ix}(\cdot) = (\cdot)^{\alpha}, $$

i.e. the loop $Q(\cdot)$ is a G-loop.

A loop in which the identity

$$ xy \cdot \theta_x zx = (x \cdot yz) \cdot x $$

is fulfilled, where θ_x is a substitution depending on x, is called *Osborn's loop*.

It is proved in [4], that a loop $Q(\cdot)$ is an Osborn's loop if and only if

$$ (\cdot)_x = {}_{Ix}(\cdot) \qquad (7) $$

for every $x \in Q$.

Statement 1. *A Osborn's loop $Q(\cdot)$ in which $x^2 \in N$ for every $x \in Q$ is a G-loop.*

Proof. Let in an Osborn's loop $x^2 \in N$ for every $x \in Q$, then $x^2 = n$, where $n \in N$ or $n^{-1}x \cdot x = 1$, whence

$$ n^{-1}x = I^{-1}x, $$
$$ x = nI^{-1}x, \qquad (8) $$

Using (8) in (7) we get

$$ {}_{Ix}(\cdot) = (\cdot)_x = (\cdot)_{nI^{-1}x} = ((\cdot)_n)_{I^{-1}x} = (\cdot)_{I^{-1}x}, $$

so

$$ (\cdot)_{I^{-1}x} = {}_{Ix}(\cdot), $$

i.e. we have got (3). By **Theorem 1** the loop $Q(\cdot)$ is a G-loop.

In the work [5] i-loops have been studied. A loop $Q(\cdot)$ in which the equality

$$ xy \backslash ((xy) \cdot u)v = u(v \cdot (y \cdot x)) / yx \qquad (9) $$

holds for arbitrary $x, y, u, v \in Q$ is called an *i-loop*. If $a \cdot b = c$, then $a \backslash c = b$, but $b = L_a^{-1}c$, so $a \backslash c = L_a^{-1}c$; similarly, if $ba = c$, then $c / a = R_a^{-1}c$. Now the equality (9) can be written as

$$ L_{xy}^{-1}((xy \cdot u) \cdot v) = R_{yx}^{-1}(u \cdot (v \cdot yx)) $$

or changing v by $R_{yx}^{-1}v$ as

$$ (xy \cdot u)R_{yx}^{-1}v = xy \cdot R_{yx}^{-1}(u \cdot v). \qquad (10) $$

At the end of [5] the author notes: "It seems to be difficult to answer the question, are i-loops G-loops".

Statement 2. *Every i-loop is a G-loop.*

Proof. Let $Q(\cdot)$ be an i-loop, then (10) holds, whence it follows that

$$T_3 = (L_{xy}, R_{yx}^{-1}, L_{xy}R_{yx}^{-1})$$

is an autotopy of the loop $Q(\cdot)$ and then

$$(\cdot)_{xy} = {}_{yx}(\cdot). \tag{11}$$

Put in (11) $y = e$, then

$$(\cdot)_x = {}_x(\cdot). \tag{12}$$

Using (12) in (11) we get

$$(\cdot)_{xy} = {}_{xy}(\cdot) = {}_{yx}(\cdot),$$

i.e.

$${}_{xy}(\cdot) = {}_{yx}(\cdot). \tag{13}$$

Let $y = Ix$ in (13), then

$$(\cdot) = {}_{Ix\cdot x}(\cdot),$$

then $Ix \cdot x = n$, where $n \in N$ or $n^{-1}Ix \cdot x = 1$, but $I^{-1}x \cdot x = 1$ and then $n^{-1}Ix = I^{-1}x$ or $nI^{-1}x = Ix$. Change in (12) x by Ix, then

$${}_{Ix}(\cdot) = (\cdot)_{Ix} = (\cdot)_{nI^{-1}x} = ((\cdot)_n)_{I^{-1}x} = (\cdot)_{I^{-1}x},$$

i.e.

$$(\cdot)_{I^{-1}x} = {}_{Ix}(\cdot),$$

and we again obtain (3). By **Theorem 1** $Q(\cdot)$ is a G-loop.

Statement 3. *If in an Osborn's loop $Q(\cdot)$ $x^2 = 1$ for every $x \in Q$, then $Q(\cdot)$ is an abelian group (1 is the identity element of the loop $Q(\cdot)$).*

Proof. If $Q(\cdot)$ is an Osborn's loop and $x^2 = 1$ for every $x \in Q$, then $x = x^{-1} = Ix$ and

$$R_{Ix} = R_x. \tag{14}$$

But in the Osborn's loop

$$R_{Ix}^{-1} = L_x^{-1}R_xL_x. \tag{15}$$

From (14) and (15) it follows

$$L_xR_x^{-1} = R_xL_x$$

and then the autotopy

$$T=(L_x,R_{Ix}^{-1},L_xR_{Ix}^{-1})$$

of the loop $Q(\cdot)$ takes the form:

$$T=(L_x,R_x^{-1},L_xR_x^{-1})=(L_x,R_x^{-1},R_xL_x),$$

whence

$$L_xy\cdot R_x^{-1}z=R_xL_x(y\cdot z). \tag{16}$$

Let $z=y$ in (16), then

$$L_xy\cdot R_x^{-1}y=1,$$
$$L_xy=R_x^{-1}y,$$
$$R_xL_xy=y,$$

and then (16) has the form:

$$L_xy\cdot z=y\cdot R_xz,$$
$$xy\cdot z=y\cdot zx. \tag{17}$$

Let $z=1$ in (17), then

$$xy=yx.$$

From (17) and (18) it follows that $Q(\cdot)$ is an abelian group.

Statement 4. *An Osborn's loop $Q(\cdot)$ in which $x^2\in N$ for every $x\in Q$ and $N\neq\{1\}$ is an extension of a group by means of an abelian group.*

Proof. The kernel N of the loop $Q(\cdot)$ is nontrivial and is a normal subloop of $Q(\cdot)$. The factor-loop $Q/N(\cdot)$ is an Osborn's loop in which $\bar{x}^2=\bar{1}$ for every $\bar{x}\in Q/N$ ($\bar{1}$ is the identity of the loop $Q/N(\cdot)$). By **Statement 3** the loop $Q/N(\cdot)$ is an abelian group.

References

1. *A.S.Basarab.* A certain class of G-loops (Russian), Mat. Issled., v.**3**(1968), vyp.2, p.72-77.

2. *A.S.Basarab.* A certain class of G-loops. 2. (Russian), Questions of the theory of Quasigroups and Loops, 1971, p.3-11.

3. *V.D.Belousov.* Foundations of the Theory of Quasigroups and Loops (Russian), Izdat."Nauka", Moscow, 1967, 223 pp.

4. *A.S.Basarab.* The Osborn loop (Russian), Studies in the theory of quasigroups and loops, "Shtiintsa", Kishinev, 1973, p.12-18.

5. *H.H.Buchteiner.* A certain class of binary loops (Russian), Nets and quasigroups, Mat. Issled., vyp. 39(1976), p.54-56.

Basarab A.S. **Ph.D.**
department of algebra,
Tiraspol pedaghogical state university,
5, Kubanskaya str.,
Kishinau, 277050,
Moldova.

Received August 12, 1993

Quasigroups and related systems, vol. **1**, no. 1(1), 1994

LOOPS WITH UNIVERSAL ELASTICITY

Paraskowya N. Syrbu

Abstract

An identity is called universal for a loop Q(·), if it holds in this loop and in each principal isotope of Q(·). Loops with universal law of elasticity, i.e.

$$xy \cdot x = x \cdot yx,$$

are investigated in this note.

Invariant properties on isotopy of quasigroups, i.e. universal properties of quasigroups, represent an important part in the theory of quasigroups and loops. The theory of algebraic nets gives, in particular, examples of such properties: all loops which coordinate the same net are isotopic between themselves and the identities which follow from the closure conditions of this net are universal for each of these loops. For example, Bol and Moufang identities are universal for loops. Our subject of investigations is the loop with universal law of elasticity (or symply, with universal elasticity), its properties and connections with some classes of well known loops such as Bol and Moufang loops.

Let $Q(\cdot)$ be a loop with universal elasticity, i.e. a loop for which the law of elasticity

$$x \cdot yx = xy \cdot x$$

is universal. Denote by $Q(*)$ a principal isotope of $Q(\cdot)$, i.e.

$$x * y = R_a^{-1}x \cdot L_b^{-1}y,$$

where

$$T = (R_a^{-1}, L_b^{-1}, 1)$$

is the isotopy, R_a (L_a) is the right (left) multiplication by the element a. The universality of the identity

$$x \cdot yx = xy \cdot x$$

for $Q(\cdot)$ involves the fact that the law of elasticity

$$(x*y)*x = x*(y*x)$$

holds in every LP-isotope $Q(*)$ of $Q(\cdot)$. Now, replace $(*)$ by $(\cdot)$ in the last identity. We get the following identity in $Q(\cdot)$:

$$R_a^{-1}(R_a^{-1}x \cdot L_b^{-1}y) \cdot L_b^{-1}x = R_a^{-1}x \cdot L_b^{-1}(R_a^{-1}y \cdot L_b^{-1}x)$$

or

$$(xy/z)(b\backslash xz) = x(b\backslash[(by/z)(b\backslash xz)]) \quad (1)$$

and

$$(bx/z)(b\backslash yx) = ([(bx/z)(b\backslash yz)]/z)x \quad (2)$$

where we replaced a by z.

Proposition 1. *The law of elasticity is universal for the loop $Q(\cdot)$ iff the identity* (1) ((2)) *holds in the primitive loop $Q(\cdot,/,\backslash)$.*

The following proposition gives some properties of loops with universal elasticity.

Proposition 2. *If $Q(\cdot)$ is a loop with universal elasticity, then*

(i) *$Q(\cdot)$ is strong power-associative (i.e. every its element generates an associative subloop);*

(ii) *$N_l = N_r$, where N_l is the left and N_r is the right nucleus of $Q(\cdot)$;*

(iii) *All (three) nuclei of $Q(\cdot)$ coincide iff each element of the middle nucleus is a Bol element.*

Proof. (i) It is known (see [1], pp.46-47) that if the identity

$$x \cdot x^2 = x^2 \cdot x$$

is universal for the loop $Q(\cdot)$, then $Q(\cdot)$ is strong power-associative.

(ii) To prove this we will need the following identity:

$$(x/z) \cdot yx = ([(x/z) \cdot yx]/z)x$$

(it follows from (2) taking b=e, where e is the unit of $Q(\cdot)$, $y \to yz, x \to bx$; here and below by "$x \to y$" we will mean "x is replased by y"). If $x \in N_r$ in the last identity, then

$$(x/z)y = [(x/z) \cdot yz]/z,$$

or

$$xy \cdot z = x \cdot yz,$$

i.e. $x \in N_l$ and $N_r \subseteq N_l$. Conversely, taking z=e in (1) we have:

$$xy \cdot (b\backslash x) = x(b\backslash[by \cdot (b\backslash x)]).$$

If $x \in N_l$ in the last identity, then

$$y(b\backslash x) = b\backslash[by\cdot(b\backslash x)],$$

or

$$b\cdot yx = by\cdot x,$$

i.e. $x \in N_r$, and so $N_r = N_l$.

(iii) Let us remind that an element a of the loop $Q(\cdot)$ is called a *Bol element* if the equality

$$a(x\cdot ay) = (a\cdot xa)y$$

is valid for every $x, y \in Q$. Suppose that a is a Bol element of the loop $Q(\cdot)$ and $a \in N_m$, where by N_m we denote the middle nucleus of $Q(\cdot)$:

$$N_m = \{a \in Q | xa\cdot y = x\cdot ay \text{ for every } x, y \in Q\}.$$

Then

$$a(xa\cdot y) = a(x\cdot ay) = (a\cdot xa)y = (ax\cdot a)y,$$

so

$$a(xa\cdot y) = (a\cdot xa)y,$$

or, after replacing $x \to xa$,

$$a\cdot xy = ax\cdot y,$$

i.e. $a \in N_l = N_r$, and $N_m \subseteq N_l = N_r$. Further, if a is a Bol element of $Q(\cdot)$ and $a \in N_l = N_r$, then

$$ax\cdot ay = a(x\cdot ay) = (a\cdot xa)y = (ax\cdot a)y.$$

So

$$ax\cdot ay = (ax\cdot a)y,$$

or after replacing $x \to a\backslash x$,

$$x\cdot ay = xa\cdot y,$$

i.e. $a \in N_m$ and

$$N_l = N_r \subseteq N_m.$$

Now this proposition follows from the next result of Florea (see [3]): all (three) nuclei of a loop coincide if and only if each element of these nuclei is a Moufang and Bol element at the same time.

Remark 1. A loop with universal elasticity satisfies the equality

$$x^p y\cdot x^q = x^p\cdot yx^q$$

for every $x, y \in Q$, where p and q are arbitrary integers (for the proof of this proposition see [2]).

A loop $Q(\cdot)$ is called a *middle Bol loop* if it satisfies the identity

$$(z/x)(y\backslash z) = z(yx\backslash z).$$

Proposition 3. *A loop $Q(\cdot)$ with universal elasticity and such that*

$$yb \cdot b = yz \cdot z$$

for all $y,b,z \in Q$, is a middle Bol loop.

Proof. Make the replacement $y \to x \backslash y$ in (1), then

$$[b(x \backslash y)/z](b \backslash xz) = b(x \backslash [(y/z)(b \backslash xz)]).$$

Now replace $y \to yz$ in the last identity:

$$[b(x \backslash yz)/z](b \backslash xz) = b(x \backslash [y(b \backslash xz)]),$$

or, if $x = yz$:

$$(b/z)(b \backslash (yz \cdot z)) = b(yz \backslash [y(b \backslash (yz \cdot z))]).$$

Suppose that

$$yb \cdot b = yz \cdot z,$$

for all $y,b,z \in Q$. Then

$$yb = (yz \cdot z)/b,$$

or

$$b = (yz \cdot z)/(y \backslash b),$$

if we replace $b \to y \backslash b$. So,

$$b \backslash (yz \cdot z) = y \backslash b,$$

and

$$(b/z)(y \backslash b) = b(yz \backslash b)$$

for all $b,y,z \in Q$, i.e. $Q(\cdot)$ is a middle Bol loop.

Remark 2. We will see in what follows that the loop $Q(\cdot)$ under the conditions of **Proposition 3** is associative and so is an abelian group.

A loop $Q(\cdot)$ is called a *LIP-loop* (a *RIP-loop*), i.e. a *loop with left inverse property* (*right inverse property*) if

$$x^{-1} \cdot xy = y \quad (yx \cdot x^{-1} = y)$$

holds for every $x,y \in Q$. A loop is called an *IP-loop* if it is a *LIP*-loop and a *RIP*-loop at the same time.

Proposition 4. *A loop with universal elasticity satisfies the left alternative law*

$$x \cdot xy = x^2 \cdot y$$

iff it has the right inverse property.

Proof. Denote by e the unit element of the loop $Q(\cdot)$ and replace in (1) $z \to x^{-1}$ and $y \to e$. As $Q(\cdot)$ is strong power-associative, we get

$$x^2b^{-1} = x(b\backslash[(b/x^{-1})b^{-1}]). \tag{3}$$

If $Q(\cdot)$ satisfies the left alternative law, then

$$x^2b^{-1} = x\cdot xb^{-1}$$

and from (3) we get

$$xb^{-1} = b\backslash[(b/x^{-1})b^{-1}],$$

that is

$$b/x^{-1} = bx$$

or

$$bx\cdot x^{-1} = b$$

for every $x,b \in Q$ (see **Remark 1**). Conversely, if $Q(\cdot)$ has the right inverse property, then

$$b/x^{-1} = bx$$

and using **Remark 1** and the identity (3), we have:

$$x^2b^{-1} = x[b\backslash(bx\cdot b^{-1})] = x[b\backslash(b\cdot xb^{-1})] = x\cdot xb^{-1},$$

i.e. $Q(\cdot)$ satisfies the left alternative law.

Analogously, but begining with (2), we can prove the following

Proposition 5. *A loop with universal elasticity satisfies the right alternative law*

$$yx\cdot x = yx^2,$$

iff it has the left inverse property.

Corollary. *A loop with universal elasticity is a IP-loop iff it satisfies the left and right alternative laws.*

Proposition 6. *A loop with universal elasticity has the left inverse property iff it has the right inverse property.*

Proof. Let $Q(\cdot)$ be a *LIP*-loop with universal elasticity. From the identity

$$bx\cdot(b\backslash(by\cdot x)) = (bx\cdot y)x \tag{4}$$

(this identity follows from (2) when $y\to by, z=e$), if $y=(bx)^{-1}$, we get

$$b[(bx)^{-1}x] = b(bx)^{-1}x \tag{5}$$

(the elasticity involvs ${}^{-1}a = a^{-1}$). Now let us make the replacement $y\to yz$ and $b=e$ in (1):

$$x(y\cdot xz) = [(x\cdot yz)/z]\cdot xz \tag{6}$$

and suppose that $y=(xz)^{-1}$ in (6). Then

$$[x / xz]z = x((xz)^{-1} z),$$

and if $x = b, z = x$:

$$[b / bx]x = b[(bx)^{-1} x]. \qquad (7)$$

From (5) and (7) we have

$$b / bx = b(bx)^{-1}$$

and so

$$bx^{-1} \cdot x = b$$

for every $x, b \in Q$, i.e. $Q(\cdot)$ is a RIP-loop. Conversely, let $Q(\cdot)$ be a RIP-loop with universal elasticity. Substitute $y \to (xz)^{-1}$ in the identity (6):

$$[x(xz)^{-1}]z = x((xz)^{-1} z). \qquad (8)$$

Take in (4) $y = (bx)^{-1}$:

$$b(bx \backslash x) = b(bx)^{-1} \cdot x.$$

Now, because of the last identity and (8) we get:

$$b(bx \backslash x) = b((bx)^{-1} x),$$

or

$$b(b^{-1} x) = x,$$

for all $x, b \in Q$, i.e. $Q(\cdot)$ is a LIP-loop.

Corollary. *If $Q(\cdot)$ is a loop with universal elasticity, then the following properties are equivalent in $Q(\cdot)$:*

right inverse property;

left inverse property;

right alternative law;

left alternative law.

Now, let us consider IP-loops with universal elasticity. Each of the identities (1) and (2) is equivalent in such a loop to the following identity:

$$(xz \cdot by)z \cdot bx = xz \cdot b(yz \cdot bx) \qquad (9)$$

(Indeed, in a IP-loop are valid the equalities:

$$x \backslash y = x^{-1} y$$

and

$$x / y = xy^{-1}$$

for every $x, y \in Q$. Now, to prove this use the last two equalities in (1) and (2) and make the replacements $x \to xz^{-1}, y \to b^{-1} y, z^{-1} \to z, b^{-1} \to b$ in (1) and $x \to b^{-1} x, y \to yz^{-1}$ in (2)).

It is known (see [4]) that in a IP-loop all (three) nuclei coincide. Denote by N the nucleus of the IP-loop $Q(\cdot)$.

Proposition 7. *The commutative IP-loop $Q(\cdot)$ with universal elasticity and $x^2 \in N$ for all $x \in Q$, is associative.*

Proof. To prove this, make the replacement $z \to xz$ and $b \to bx$ in (9) and use **Propositions 4,5** and the fact that $x^2 \in N$, for all $x \in Q$:

$$[z(bx \cdot y) \cdot xz]b = z[bx \cdot (y \cdot xz)b].$$

Now, if $y=z$ in the last identity then

$$(bx \cdot xz)b = z(bx)^2,$$

or, using the commutativity of $Q(\cdot)$ and substituting $x \to b^{-1}x$:

$$x(b^{-1}x \cdot z) \cdot b = zx^2,$$

$$x(b^{-1}x \cdot z) = zx^2 \cdot b^{-1} = x^2 z \cdot b^{-1} = x^2 \cdot zb^{-1} = x(x \cdot zb^{-1}),$$

$$b^{-1}x \cdot z = x \cdot zb^{-1},$$

$$xb^{-1} \cdot z = x \cdot b^{-1}z,$$

so, the loop $Q(\cdot)$ is an abelian group.

Corollary. *A IP-loop $Q(\cdot)$ with universal elasticity and such that $x^2 = 1$ for all $x \in Q$ is associative.*

Proposition 8. *The identity (9) involves both inverse properties in the loop.*

Proof. Substitute $b = e$ and $y = z^{-1}$ in (9). Then we have:

$$(xz \cdot z^{-1})z \cdot x = xz \cdot x,$$

or

$$xz \cdot z^{-1} = x$$

for all $x,z \in Q$, i.e. $Q(\cdot)$ is a RIP-loop. Analogously, from (9) (making the replacement $z = e, y = b^{-1}$) we have

$$x \cdot bx = x \cdot b(b^{-1} \cdot bx),$$

or

$$x = b^{-1} \cdot bx$$

for every $x,b \in Q$; hence, $Q(\cdot)$ is a LIP-loop.

Corollary 1. *The loop which satisfies the identity (9) is a loop with universal elasticity.*

Corollary 2. *The identity (9) is universal for $Q(\cdot)$ iff $Q(\cdot)$ is a Moufang loop.*

Indeed, according to the information given up, the identities (1) and (9) are equivalent in an *IP*-loop.

Remark 3. The identity (1) follows from the identity (9) but, in general, these two identities are not equivalent. For instance, the loop from the example given below satisfies the identity (1) but it is not an *IP*-loop, hence it does not satisfy (9).

	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	1	4	3	6	5	8	7
3	3	4	1	2	7	8	6	5
4	4	3	2	1	8	7	5	6
5	5	6	7	8	1	2	3	4
6	6	5	8	7	2	1	4	3
7	7	8	6	5	3	4	1	2
8	8	7	5	6	4	3	2	1

Using the computer the author proved that in loops of order n, where $n \le 6$, the identity (1) and Bol's middle law

$$(z/x)(y\backslash z) = z(yx\backslash z)$$

are equivalent. For other loop orders this question is open.

References

1. *Belousov V.D.* Algebraic nets and quasigroups. (Russian), Kishinev, "Shtiintsa", 1971.

2. *Shelekhov A.M., Shestakova M.A.* About identities in weakly associative loops. (Russian), Probl. teorii tkanei i kvazigrupp. Kalinin, 1985, p.115-121.

3. *Florea I.A.* Loops with one of the inverse properties. (Russian), Izv. AN MSSR, v.7(1965), p.68-79.

4. *Belousov V.D.* Foundations of the theory of quasigroups and loops. (Russian), Moskow, "Nauka", 1967.

Syrbu P.N. **Ph.D.**
department of quasigroup theory,
Institute of Mathematics,
Academy of Sciences of Moldova,
5, Academiei str.,
Kishinau, 277028,
Moldova.

Received August 10, 1993

Quasigroups and related systems, vol. 1, no. 1(1), 1994

ON LINEAR ISOTOPES OF CYCLIC GROUPS

Sokhatskyj Fedir, Syvakivskyj Petro

Abstract

A description of all cyclic group n-ary linear isotopes is found to within isomorphism. Some results on their automorphism group and endomorphism semigroup are given.

An operative *(G;f)* will be called a multiplace isotope of the group *(Q;+)* iff there exists a sequence $(\gamma_1,...,\gamma_n,\gamma)$, named isotopy, of one-to-one mappings from G onto Q such that

$$f(x_1,x_2,...,x_n)=\gamma^{-1}(\gamma_1 x_1+\gamma_2 x_2+...+\gamma_n x_n)$$

holds for all $x_1,x_2,...,x_n$ in G. If all isotopy components are linear transformations of the group, then it will be called linear one. (Here and henceforth a linear transformation α of a group *(Q;+)* is a mapping from Q into Q such that $\alpha x=\theta x+c$, where θ is an automorphism and c is an arbitrary element of the group). According to **Albert's theorem** isomorphism of group isotopes implies isomorphism of the corresponding groups. So, it is enough to find an isomorphical test for isotopes of the same arbitrary fixed group. In this article we do it for a cyclic group, describe all its linear isotopes up to isomorphism, consider their automorphism groups and endomorphism semigroups. In the next works we shall consider the general case, but the main results one may find in [1].

Let Z be the integer ring and $C=Z$ or $C=Z_m=Z/mZ$. It is easy to verify that any n-ary linear isotope of a cyclic group is isomorphic to *(C;f)* defined by the equality

$$f(x_1,x_2,...,x_n)=h_1x_1+h_2x_2+...+h_nx_n+a, \tag{1}$$

where $h_1,h_2,...,h_n$ are invertible elements in the ring C (denote by C^* the group of ones). In this case the elements $h_1,h_2,...,h_n$ will be called *coefficients of (C;f)* and a will be its free member. Let *(C;g)* be defined by equality

$$g(x_1,x_2,...,x_n)=k_1x_1+k_2x_2+...+k_nx_n+b \tag{2}$$

and α be a homomorphism from *(C;g)* into *(Q;f)*, i.e. the equality

$$\alpha(k_1x_1+k_2x_2+\ldots+k_nx_n+b)=h_1\alpha x_1+h_2\alpha x_2+\ldots+h_n\alpha x_n+a \tag{3}$$

holds for all $x_1,x_2,\ldots,x_n$ in C. In particular, replacing $x_3,\ldots,x_n$ by 0 and x_1,x_2 by the suitable expressions we have the equality

$$\alpha(x+y)=\beta x+\gamma y$$

for some transformations β,γ of the set C. Applying **Lemma 2.5** from [2] we get

$$\alpha x=kx+c$$

for some k,c of the set C. It is clear the element k is invertible together with the transformation α, i.e. when these isotopes are isomorphic. The relationship (3) with $x_1=x_2=\ldots=x_n=0$ gives the dependence

$$kb=(h_1+h_2+\ldots+h_n-1)c+a \tag{4}$$

and with $x_j=0$ for all $j\neq i$ and $x_i=1$ it gives

$$kk_i=h_ik,\quad i=1,\ldots,n, \tag{5}$$

in the ring C. The last equalities in the infinite ring for homomorphic isotopes mean that the corresponding sequenses of the coeffitients coincide. If the ring C is finite the relation (5) is equivalent to congruence

$$k_i\equiv h_i(\bmod\frac{m}{s}),\quad i=1,\ldots,n,$$

i.e.

$$k_i\in\frac{m}{s}Z_m+h_i,\quad i=1,\ldots,n, \tag{6}$$

where $s=GCD(k,m)$. Hence, we can make the following conclusions.

Lemma 1. *A transformation α of the set Z_m is a homomorphism of the isotope $(Z_m;g)$ into $(Z_m;f)$ defined by (2) and (1) respectively if and only if there exist elements k,c in Z_m such that*

$$\alpha x=kx+c$$

and the relationships (4) and (6) hold.

Lemma 2. *A transposition α of the set Z is a homomorphic mapping from the isotope $(Z;g)$ into $(Z;f)$ defined by (2) and (1) if and only if there exist elements k,c such that the equalities*

$$\alpha x=kx+c,\quad k_i=h_i,\quad i=1,\ldots,n,$$

and (4) hold.

Corollary. *Different sequences of invertible elements of the ring C define nonisomorphic linear isotopes of the cyclic group $(C,+)$.*

Lemma 3. *Let $(C;f)$ and $(C;g)$ be linear isotopes defined by the equalities* (1) *and*

$$g(x_1,x_2,\dots,x_n)=h_1x_1+h_2x_2+\dots+h_nx_n+b.$$

Then a substitution α of the set C will be an isomorphism between them if and only if

$$\alpha x=kx+c \quad \text{and} \quad kb=\mu c+a$$

for some element c and invertible element k of the ring C, where

$$\mu=h_1+h_2+\dots+h_n-1.$$

To establish an isomorphical test for the linear isotopes we need the following.

Lemma 4. *For every integer a there exists a number r which is relatively prime to m and*

$$d\equiv ra(\operatorname{mod} m),$$

where $d=GCD(a,m)$.

Proof. Let a_1 and m_1 be integers defined by the equalities $a=a_1d$ and $m=m_1d$, and t be a product of all prime integers having the same exponent in the factorizations a and b into prime numbers. We can take r such that

$$(a_1-tm_1)r\equiv 1(\operatorname{mod} m).$$

Theorem 1. *Any linear isotope $(Z_m;f)$ defined by* (1) *is isomorphic to the isotope $(Z_m;g)$ defined by the following equality*

$$g(x_1,x_2,\dots,x_n)=h_1x_1+h_2x_2+\dots+h_nx_n+d, \tag{7}$$

where $d=GCD(\mu,m,a)$ and $\mu=h_1+h_2+\dots+h_n-1$.

Proof. We adopt the notations $a_0=GCD(a,m)$, $\mu_0=GCD(\mu,m)$, then $d=GCD(a_0,\mu_0)$ and the **lemma 4** implies the existence of a number x which is relatively prime to μ_0 and

$$d\equiv xa_0(\operatorname{mod}\mu_0). \tag{8}$$

Let us denote by z the product of all prime divisors of the number m not dividing the number x. Since every prime divisor of the integer m divides exactly one of the numbers x,μ_0,z, then the integers $r=x+\mu_0z$ and m are relatively prime. **Lemma 4** implies the existence of numbers r_1 and r_2 which are relatively prime to m and

$$a_0\equiv ar_1(\operatorname{mod} m),$$
$$\mu_0\equiv \mu r_2(\operatorname{mod} m),$$

and the relationship (8) implies the equality

$$d=a_0x+\mu_0y$$

for some integer y. For this reason

$$d = a_0(x+\mu_0 z-\mu_0 z)+\mu_0 y = a_0 r-\mu_0(a_0 z-y) \equiv$$
$$\equiv (ar_1 r-\mu r_2(a_0 z-y))(\mathrm{mod}\, m).$$

So, after the notations $k=r_1 r$ and $c=r_2(a_0 z-y)$ we get the relationship

$$ka \equiv (\mu c+d)(\mathrm{mod}\, m),$$

which completes the proof according to **lemma 3**.

Theorem 2. *Any linear isotope of a cyclic* m *order group is isomorphic to exactly one isotope* $(Z_m;g)$ *defined by the equality* (7), *where* $h_1,h_2,\dots,h_n$ *is a sequence of invertible elements of the ring* Z_m *and* d *is a common divisor of* $\mu=h_1+h_2+\dots+h_n-1$ *and* m.

Proof. Any linear isotope of a cyclic group G is isomorphic to a linear isotope of the group Z_m. According to **theorem 1**, it is isomorphic to the isotope $(Z_m;g)$ satisfying to the conditions of this theorem. Let us consider two different isotopes $(Z_m;g_1)$ and $(Z_m;g_2)$. If they have the different sequences of their coefficients, then by the **corollary** of **lemma 1** these isotopes are not isomorphic. When the isotopes differ from each other only by their free members named a,b and taken $a<b$, then by **lemma 3** the existence of an isomorphism of the isotopes is equivalent to the existence of numbers k,c such that

$$kb \equiv \mu c+a(\mathrm{mod}\, m)$$

holds. Under the conditions of the theorem the numbers a,b are common divisors of the integers μ,m and k is relatively prime to a, so b is divided by a. A contradiction.

If we consider group isotopes of a prime order, we can give more exact information following from the **theorem 2**.

Corollary 1. *Any n-ary linear group isotope of the prime order* p *is isomorphic:*

1) *one to the other, if the sum of the coeffitients is not the identity transformation;*

2) *to exactly one of the isotopes* (Z_p,g_0) *or* (Z_p,g_1) *defined by* (1) *with* $a=0$ *and* $a=1$, *respectively, in contrary case.*

Define $F(n,m)$ as the number of all pairwise nonisomorphic n-ary linear isotopes of the m order cyclic groups. According to **theorem 2**, $F(n,m)$ is the cardinal number of the set

$$\{(h_1,h_2,\dots,h_n,d) | h_1,h_2,\dots,h_n \in Z_m^{**}, d \in D(h_1+h_2+\dots+h_n-1,m)\},$$

where Z_m^{**} denotes a set of all pairwise noncongruent by modulo m integers, which are relatively prime to m and $D(k,m)$ is the set of all common divisors of the integers k and m. We put the following problem:

what is the analytical expression of the number function $F(n,m)$?

Here we shall give a solution of this problem for prime m.

Corollary 2. *There exist exactly*

$$F(n,p)=\frac{(p+1)(p-1)^n+(-1)^{n+1}}{p}$$

n-ary linear group isotopes of a prime order p up to isomorphism.

Proof. Let us denote by $k_{n,i}$ the number of all sequences $(h_1,h_2,\dots,h_n)$ with

$$h_1+h_2+\dots+h_n\equiv i(\mathrm{mod}\,p)$$

and

$$0<h_1,h_2,\dots,h_n<p.$$

It is easy to see that

$$k_{n,0}+k_{n,1}+\dots+k_{n,p-1}=(p-1)^n, \tag{9}$$

Let

$$h_1+h_2+\dots+h_n\equiv j(\mathrm{mod}\,p),$$

then there exists exactly one number h_{n+1} with conditions

$$h_1+h_2+\dots+h_n+h_{n+1}\equiv i(\mathrm{mod}\,p),$$
$$0<h_{n+1}<p$$

if and only if $j\neq i$. So, the equalities

$$k_{n+1,i}=(p-1)^n-k_{n,i},\quad i=0,1,\dots,n,$$

hold. Since $k_{1,0}=0$ and

$$k_{1,1}=k_{1,2}=\dots=k_{1,p-1}=1,$$

then

$$k_{n,1}=k_{n,2}=\dots=k_{n,p-1}=k_{n,0}-(-1)^n$$

for every $n=1,2,\dots$. From (9) we have

$$k_{n,1}+(-1)^n+(p-1)k_{n,1}=(p-1)^n,$$

and

$$k_{n,1}=\frac{(p-1)^n-(-1)^n}{p}.$$

Hence, by **corollary 1** we get

$$F(n,p)=\frac{(p-1)^n-(-1)^n}{p}+(p-1)^n=\frac{(p+1)(p-1)^n+(-1)^{n+1}}{p}.$$

A description of all linear isotopes of infinite cyclic groups is given by the following theorem.

Theorem 3. *Any linear isotope of an infinite cyclic group is isomorphic to exactly one linear isotope (Z;f) defined by* (1), *where*

1) $a=0,1,2,\ldots,$ *if* $\mu=0$;
2) $a=0,$ *if* $\mu=-1,1$;
3) $a=0,1,\ldots,[|\frac{\mu}{2}|],$ *if* $\mu\neq-1,0,1,$

where $\mu=h_1+h_2+\ldots+h_n-1.$

Proof. An isomorphical test of such isotopes is given by **lemma 2** and is expressed by the relationship (4). Since in this case k=1 or k=-1, then the isomorphism of the isotopes means that one of the equalities

$$b=\mu c+a \quad \text{or} \quad -b=\mu c+a \tag{10}$$

is true. Let $\mu=0$, then the isomorphism is possible iff $b=\pm a$. Hence all isotopes with $a>0$ are pairwise nonisomorphic. If $\mu=\pm1$, then $c=b\pm a$ give an isomorphism of any pair of linear isotopes with the same coeffitient sequence. Finally, let $\mu\neq-1,0,1$, then the equalities (10) mean that

$$b\equiv a(\mathrm{mod}\,\mu).$$

So, in this case any linear isotope is isomorphic to exactly one isotope defined by (1) with $a=0,1,\ldots,[|\frac{\mu}{2}|]$. The proof has been completed.

The immediate corollary of the lemmas **1,2** is

Lemma 5. *A transformation* α *of the set* C *is an endomorphism of the isotope* $(C;f)$ *defined by* (1) *if and only if there exist elements* k *and* c *of* C *such that*

$$\alpha x=kx+c, \qquad (k-1)a=\mu c,$$

where $\mu=h_1+h_2+\ldots+h_n-1.$

The next statements is obvious (we denote the semidirect product by "♦").

Corollary. *If the isotope (C;f) is defined by* (1) *and* $a=0$, *then the relations*

$$End(C;f) \cong Ker\mu \blacklozenge C, \quad Aut(C;f) \cong Ker\mu \blacklozenge C$$

hold. In particular, $End(C;f)$ *is a subnearing of the linear transformation nearing of the group (C;+).*

Theorem 3, lemma 5 and its **corollary** permit to calculate the endomorphism semigroup and the automorphism group of the arbitrary linear isotope of the infinite cyclic group. We shall express these results in the following theorem.

Theorem 4. *Let (Z;f) be an arbitrary isotope of the infinite cyclic group (Z;+), where Z is the ring of integers, and* (1) *be its decomposition. If we denote* $\mu = h_1 + h_2 + \ldots + h_n - 1$ *and* $d = GCD(a,\mu)$, *then the following conditions are fulfilled:*

1) $End(Z;f) \cong Z \blacklozenge Z, Aut(Z;f) \cong Z_2 \blacklozenge Z,$ *when* $a=\mu=0$;
2) $End(Z;f) \cong Z, Aut(Z;f) \cong Z_2,$ *when* $a=0$ *and* $\mu \neq 0$;
3) $End(Z;f) \cong Aut(Z;f) \cong (Z;+),$ *when* $a \neq 0$ *and* $\mu = 0$;
4) $End(Z;f) \cong (Z;\cdot), Aut(Z;f) \cong Z_2,$ *when* $a \neq 0$ *and* $\mu = \pm 1$;
5) $End(Z;f) \cong (\frac{\mu}{d}Z+1;\cdot), Aut(Z;f) \cong Z_2,$ *when* $a \neq 0$ *and* $\mu = \pm 2a$;
6) $End(Z;f) \cong (\frac{\mu}{d}Z+1;\cdot), Aut(Z;f) \cong \{1\},$ *when* $a \neq 0$ *and* $\mu \neq 0, \pm 1, \pm 2a$.

Proof. We consider the case $\mu \neq 0, \pm 1$, $a \neq 0$ only because other ones are obvious. By the **lemma 5** we have the equality

$$(k-1)\frac{a}{d} = \frac{\mu}{d}c.$$

It implies the existence of an integer t such that

$$k-1 = \frac{\mu}{d}t \quad \text{and} \quad c = \frac{a}{d}t,$$

i.e. any endomorphism has the expression

$$\alpha(x) = (\frac{\mu}{d}t+1)x + \frac{a}{d}t$$

for some integer t. It is easy to see that the converse statement is true as well. Thus, we have established an one-to-one correspondence between semigroups

$$End(Q;f) \quad \text{and} \quad (\frac{\mu}{d}Z+1).$$

It is easy to verify that it is an isomorphism. In particular, the group of all invertible elements of the semigroup $(\frac{\mu}{d}Z+1)$ is isomorphic to the automorphism group of the linear isotope *(Z;f)*. If an integer is invertible, then it belongs to {-1,1}. Let

$$\frac{\mu}{d}t+1=-1,$$

i.e. $\frac{\mu}{d}t=-2$. Then $t=\pm1,\pm2$ and the numbers t,μ have different signs. Since $a\le[|\frac{\mu}{2}|]$, then $d\le a<|\mu|$, so $t=1$ if $\mu<0$ and $t=-1$ if $\mu>0$. Moreover, the relationships both $|\mu|=2d$ and $d\le a<|\mu|$ hold only if $a=d$.

A problem of description of endomorphism semigroup and automorphism group of a finite linear isotope is still open. We shall single out some relationships only.

Denote by $M(f)$ ($M^*(f)$) the set of all coefficients of endomorphisms (respectively isomorphisms), i.e.

$$M(f)=\{k|(\exists c)\alpha\in End(Q;f),\text{ where }\alpha x=kx+c\},$$

$$M^*(f)=\{k|(\exists c)\alpha\in Aut(Q;f),\text{ where }\alpha x=kx+c\},$$

It is easy to verify that $(M(f);\cdot)$ is a monoid and $(M^*(f);\cdot)$ is a subgroup of all its invertible elements. The **lemma 5** implies

Corollary. *A transformation* α *of the set* Z_m *is an endomorphism of the isotope* $(Z_m;f)$ *defined by* (1) *if and only if* $\alpha x=kx+c$ *and*

$$(k-1)c=\mu c(\bmod m), \tag{11}$$

where $\mu=h_1+h_2+\ldots+h_n-1$.

After the **theorem 2** and the corollary of the **lemma 5** we shall only consider the case

$$a\not\equiv 0(\bmod m)$$

and a is a common divisor of μ and m. The relationship (11) means that

$$k\equiv\frac{\mu}{a}c+1(\bmod\frac{m}{a}),$$

i.e.

$$k \equiv \frac{m}{a}t + \frac{\mu}{a}c + 1 (\bmod m)$$

for some integer t. So,

$$k \in \frac{m}{a}Z_m + \frac{\mu}{a}Z_m + 1.$$

It is easy to verify that the converse statement is true as well. Thus

$$M(f) = \frac{m}{a}Z_m + \frac{\mu}{a}Z_m + 1$$

and

$$M^*(f) = Z_m^* \cap (\frac{m}{a}Z_m + \frac{\mu}{a}Z_m + 1). \qquad (12)$$

It is easy to make sure that

1) the transformations α and β defined by

$$\alpha x \equiv kx + c (\bmod m),$$
$$\beta x \equiv k_1 x + c (\bmod m)$$

are endomorphisms of $(Z_m; f)$ if and only if

$$k_1 \in \frac{m}{a}Z_m + k.$$

2) the transformations α and β defined by

$$\alpha x \equiv kx + c (\bmod m),$$
$$\beta x \equiv kx + c_1 (\bmod m)$$

are endomorphisms of $(Z_m; f)$ if and only if

$$c_1 \in \frac{m}{d}Z_m + c,$$

where $d = GCD(\mu, m)$.

These assertions imply the following relationships for the sets $End(Z_m; f)$ and $Aut(Z_m; f)$:

$$End(Z_m; f) = \bigcup_{c \in Z_m} (\frac{m}{a}Z_m + \frac{\mu}{a}c + 1) \times (\frac{m}{d}Z_m + c), \qquad (13)$$

$$End(Z_m; f) = \bigcup_{k \in M(f)} (\frac{m}{a}Z_m + k) \times (\frac{m}{d}Z_m + (\frac{\mu}{d})^{\varphi(\frac{\mu}{d})-1} \frac{(k-a)}{d}),$$

$$Aut(Z_m;f)=\bigcup_{c\in Z_m}((\frac{m}{a}Z_m+\frac{\mu}{a}c+1)\cap Z_m^*)\times(\frac{m}{d}Z_m+c), \qquad (14)$$

$$Aut(Z_m;f)=\bigcup_{k\in M^*(f)}((\frac{m}{a}Z_m+k)\cap Z_m)\times((\frac{m}{d}Z_m+(\frac{m}{d})^{\varphi(\frac{\mu}{d})-1}\frac{(k-1)a}{d}),$$

where φ is the *Euler's phi-function*. From (13) and (14) it follows

Proposition 1. *In the linear isotope* $(Z_m;f)$ *defined by* (1) *with*

$$h_1+h_2+\ldots+h_n\equiv 1(\mathrm{mod}\, m)$$

the following relationships

$$End(Z_m;f)\cong Z_m\times(\frac{m}{a}Z_m+1),$$

$$Aut(Z_m;f)\cong Z_m\times((\frac{m}{a}Z_m+1)\cap Z_m^*)$$

hold. If in addition $a=1$, *then the endomorphism semigroup coincides with the automorphism group and is isomorphic to* Z_m.

Proposition 2. *An automorphism group of a linear isotope of prime order* p *is isomorphic to* $Z_p, HolZ_p$ *or* Z_{p-1}.

References

1. *Sokhatskii F.N.* About isomorphism of linear quasigroups., International algebraic conference, Barnaul, 20-25 august 1991, p.138.

2. *Belousov V.D.* Foundations of the theory of quasigroups and loops.(Russian), Moscow, "Nauka", 1967.

3. *Sokhatskii F.N.* About the *M*-associative operatives. (Russian), Third All-union symposium on semigroup theory (Sverdlovsk), 1988, p.88.

4. *Sokhatskii F.N., Sivakovskii P.V.* Quasigroups which are linear on a cyclic group. International algebraic conference, Barnaul, 20-25 august 1991, p.140.

5. *Izbash V.I.* About quasigroups which are group isotopes. (Russian), IM VC AN MSSR, Kishinev, 1989, 21p., Dep. VINITI 29.06.89, N 4298-B89.

Sokhatskyj Fedir **Ph.D.**
Syvakivskyj Petro
department of algebra,
Vinnytsa State Pedagogical Institute,
32, Chervonopraporna str.,
Vinnytsa, 287100,
Ukraine.

Received August 15, 1993

Quasigroups and related systems, vol. 1, no. 1(1), 1994

A COMMON FORM FOR AUTOTOPIES OF n-ARY GROUP WITH THE INVERSE PROPERTY

Leonid A. Ursu

Abstract

In this article it is proved that every component of an autotopy of n-*IP*-group is its quasiautomorphism and a common form of quasiautomorphisms and autotopies of such groups is also established.

A quasigroup *Q(A)* of arity n is called a n-group [1] if the following identities

$$A(x_1^{i-1}, A(x_i^{i+n-1}), x_{i+1}^{2n-1}) = A(x_1^{j-1}, A(x_j^{j+n-1}), x_{j+1}^{2n-1})$$

hold in it for all $x_1^{2n-1} \in Q^{2n-1}$ and all $i, j \in \overline{1,n}$, $i \neq j$.

There exist n-ary groups without an identity element and n-ary groups with more than one identity elements [1].

A group *Q(A)* of arity n is called *symmetric* [1] if

$$A(x_{\alpha 1}^{\alpha n}) = A(x_1^n)$$

for every $x_1^n \in Q^n$ and every $\alpha \in S_n$, where S_n is the symmetric group of the degree n.

According to the **Gluskin-Hosszu theorem** [1] each n-group *Q(A)* is reduced to a binary group $Q(\cdot)$:

$$A(x_1^n) = x_1 \cdot \varphi x_2 \cdot \varphi^2 x_3 \cdot \ldots \cdot \varphi^{n-1} x_n \cdot k,$$

where φ is an automorphism of $Q(\cdot)$, k is a fixed element of Q and

$$\varphi k = k, \quad \varphi^{n-1} x = k \cdot x \cdot k^{-1}.$$

If *Q(A)* is a symmetric n-group without an identity element, then

$$A(x_1^n) = x_1 \cdot x_2 \cdot x_3 \cdot \ldots \cdot x_n \cdot k. \tag{1}$$

If *Q(A)* is a symmetric n-group with an identity element, then

$$A(x_1^n) = x_1 \cdot x_2 \cdot x_3 \cdot \ldots \cdot x_n, \tag{2}$$

where $Q(\cdot)$ is an abelian group.

A quasigroup $Q(A)$ of arity n is called a *quasigroup with the inverse property* (briefly a *n-IP-quasigroup*) [1] if there exist such substitutions ν_{ij} of Q, $i,j \in \overline{1,n}$, $\nu_{ii} = \varepsilon$ (ε is the identity substitution) that the identities

$$A(\{\nu_{ij}x_j\}_{j=1}^{i-1}, A(x_1^n), \{\nu_{ij}x_j\}_{j=i+1}^{n}) = x_i$$

hold for every $x_1^n \in Q^n$, $i \in \overline{1,n}$.

The matrix

$$(\nu_{ij}) = \begin{bmatrix} \varepsilon & \nu_{12} & \nu_{13} & \dots & \nu_{1n} & \varepsilon \\ \nu_{21} & \varepsilon & \nu_{23} & \dots & \nu_{2n} & \varepsilon \\ \nu_{31} & \nu_{32} & \varepsilon & \dots & \nu_{3n} & \varepsilon \\ \dots & \dots & \dots & \dots & \dots & \dots \\ \nu_{n1} & \nu_{n2} & \nu_{n3} & \dots & \varepsilon & \varepsilon \end{bmatrix}$$

is called an *inverse matrix* of $Q(A)$.

It is known [2], that the inverse property holds only in the following n-groups:

a) all symmetric n-groups with an identity element. For such a group the inverse matrix is

$$(O) = \begin{bmatrix} \varepsilon & I & I & \dots & I & \varepsilon \\ I & \varepsilon & I & \dots & I & \varepsilon \\ I & I & \varepsilon & \dots & I & \varepsilon \\ \dots & \dots & \dots & \dots & \dots & \dots \\ I & I & I & \dots & \varepsilon & \varepsilon \end{bmatrix}; \tag{3}$$

b) all symmetric n-groups without an identity element. For them

$$(O) = \begin{bmatrix} \varepsilon & IL_k & IL_k & I & I & \dots & I & \varepsilon \\ IL_k & \varepsilon & IL_k & I & I & \dots & I & \varepsilon \\ IL_k & IL_k & \varepsilon & I & I & \dots & I & \varepsilon \\ IL_k & IL_k & I & \varepsilon & I & \dots & I & \varepsilon \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ IL_k & IL_k & I & I & I & \dots & \varepsilon & \varepsilon \end{bmatrix}; \tag{4}$$

c) all nonsymmetric n-groups without an identity element which are reduced to binary abelian groups. For such n-groups

$$\varphi^2=\varepsilon,\quad k^2=e,$$

where e is the identity element of $Q(\cdot)$, i.e.

$$A(x_1^n)=x_1\cdot\varphi x_2\cdot x_3\cdot\varphi x_4\cdot\ldots\cdot\varphi x_{n-1}\cdot x_n\cdot k. \tag{5}$$

In this case $Q(A)$ has an odd arity and

$$(O)=\begin{pmatrix} \varepsilon & I & I & I & \ldots & I & \varepsilon \\ I\varphi & \varepsilon & I\varphi & I\varphi & \ldots & I\varphi & \varepsilon \\ I & I & \varepsilon & I & \ldots & I & \varepsilon \\ I\varphi & I\varphi & I\varphi & \varepsilon & \ldots & I\varphi & \varepsilon \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ I & I & I & I & \ldots & \varepsilon & \varepsilon \end{pmatrix}; \tag{6}$$

An ordered $(n+1)$-tuple $T=(\alpha_1^{n+1})$ of subtitutions of Q is called an *autotopy of a n-group $Q(A)$* if

$$\alpha_{n+1}^{-1}A(\{\alpha_i x_i\}_{i=1}^n)=A(x_i^n).$$

In particular, $(\overset{n+1}{\alpha})=\alpha$ is called an *automorphism* of $Q(A)$.

The set of all autotopies of $Q(A)$ forms a group with respect to the multiplication of substitutions. This group is denoted by $\mathfrak{J}_A$.

The chief component α_{n+1} of an autotopy $T=(\alpha_1^{n+1})$ of a n-group is called a *quasiautomorphism* of this group [1].

All quasiautomorphisms of a n-group form the group [1].

In this article it is proved that every component of an autotopy of n-IP-group is its quasiautomorphism and a common form of quasiautomorphisms and autotopies of such groups is also established.

Let $T=(\alpha_1^n,\delta)$ be an autotopy of a nonsymmetric n-*IP*-group $Q(A)$:

$$\delta A(x_1^n)=A(\{\alpha_i x_i\}_{i=1}^n).$$

Denote

$$(\bar{a})=A(\{\alpha_i e\}_{i=1}^n).$$

Then, according to (5),

$$\delta A(x_1^n)=\delta(x_1\cdot\varphi x_2\cdot x_3\cdot\varphi x_4\cdot\ldots\cdot\varphi x_{n-1}\cdot x_n\cdot k)=A(\{\alpha_i x_i\}_{i=1}^n).$$

By

$$x_1=x_2=\ldots=x_{i-1}=x_{i+1}=\ldots=x_n=e$$

we obtain

$$\delta R_k x_i = L_i(\bar{a})\alpha_i x_i,$$

whence

$$\alpha_i = L_i^{-1}(\bar{a})\delta R_k \qquad (7)$$

for each odd i, and

$$\alpha_i = L_i^{-1}(\bar{a})\delta R_k \varphi \qquad (8)$$

for each even i, $i \in \overline{1,n}$, where $R_k x = x \cdot k$.

Thus,

$$T = (L_1^{-1}(\bar{a}), L_2^{-1}(\bar{a})\delta\varphi\delta^{-1}, L_3^{-1}(\bar{a}), L_4^{-1}(\bar{a})\delta\varphi\delta^{-1}, \ldots, \delta R_k^{-1}\delta^{-1})\delta R_k, \qquad (9)$$

since

$$R_k\varphi = \varphi R_k: \quad R_k \varphi x = \varphi x \cdot k = \varphi(x \cdot \varphi k) = \varphi(x \cdot k) = \varphi R_k x.$$

If $Q(A)$ is a symmetric n-group without an identity element, according to (1) we put $\varphi = \varepsilon$ in (9). In the case when $Q(A)$ is a symmetric n-group with an identity element we put $\varphi = R_k = \varepsilon$ in (9) according to (2).

Lemma 1. *All components of an autotopy* $T = (\alpha_1^n, \delta)$ *of a* n*-IP-group* $Q(A)$ *are quasiautomorphisms if* $L_i(\bar{a})$, φ, R_k, $(i \in \overline{1,n})$, *are quasiautomorphisms of* $Q(A)$.

The **proof** follows from (7), (8) and the fact that the set of all quasiautomorphisms of $Q(A)$ forms a group.

Proposition. *All components of any autotopy of a* n*-group* $Q(A)$ *of the form*

$$A(x_1^n) = x_1 \cdot \varphi x_2 \cdot x_3 \cdot \varphi x_4 \cdot \ldots \cdot \varphi x_{n-1} \cdot x_n \cdot k,$$

where $Q(\cdot)$ *is an abelian group, are its quasiautomorphisms.*

Proof. We have for each odd i:

$$L_i(\bar{a})A(x_1^n) = A(\{\alpha_j e\}_{j=1}^{i-1}, A(x_1^n), \{\alpha_j e\}_{j=i+1}^{n}) =$$
$$= \alpha_1 e \cdot \varphi\alpha_2 e \cdot \alpha_3 e \cdot \varphi\alpha_4 e \cdot \ldots \cdot \varphi\alpha_{i-1} e \cdot x_1 \cdot \varphi x_2 \cdot x_3 \cdot \varphi x_4 \cdot \ldots \cdot \varphi x_{i-1} \cdot$$
$$\cdot x_i \cdot \varphi x_{i+1} \cdot x_{i+2} \cdot \ldots \cdot \varphi x_{n-1} \cdot x_n \cdot k \cdot \varphi\alpha_{i+1} e \cdot \alpha_{i+2} e \cdot \ldots \cdot \varphi\alpha_{n-1} e \cdot \alpha_n e \cdot k =$$
$$= x_1 \cdot \varphi x_2 \cdot x_3 \cdot \varphi x_4 \cdot \ldots \cdot \varphi x_{i-1} \cdot (\alpha_1 e \cdot \varphi\alpha_2 e \cdot \alpha_3 e \cdot \varphi\alpha_4 e \cdot \ldots \cdot \varphi\alpha_{i-1} e \cdot x_i \cdot$$
$$\cdot \varphi\alpha_{i+1} e \cdot \alpha_{i+2} e \cdot \ldots \cdot \varphi\alpha_{n-1} e \cdot \alpha_n e \cdot k) \cdot \varphi x_{i+1} \cdot x_{i+2} \cdot \ldots \cdot \varphi x_{n-1} \cdot x_n \cdot k =$$
$$= A(x_1^{i-1}, A(\{\alpha_j e\}_{j=1}^{i-1}, x_i, \{\alpha_j e\}_{i+1}^{n}), x_{i+1}^n) = A(x_1^{i-1}, L_i(\bar{a})x_i, x_{i+1}^n),$$

i.e. $L_i(\bar{a})$ is a quasiautomorphism of $Q(A)$.

For each even i

$$L_i(\bar{a})A(x_1^n) = A(\{\alpha_j e\}_{j=1}^{i-1}, A(x_1^n), \{\alpha_j e\}_{j=i+1}^n) =$$
$$= \alpha_1 e \cdot \varphi\alpha_2 e \cdot \alpha_3 e \cdot \varphi\alpha_4 e \cdot \ldots \cdot \varphi\alpha_{i-1} e \cdot \varphi x_1 \cdot x_2 \cdot \varphi x_3 \cdot x_4 \cdot \ldots \cdot \varphi x_{i-1} \cdot$$
$$\cdot x_i \cdot \varphi x_{i+1} \cdot \ldots \cdot x_{n-1} \cdot \varphi x_n \cdot k \cdot \alpha_{i+1} e \cdot \varphi\alpha_{i+2} e \cdot \ldots \cdot \varphi\alpha_{n-1} e \cdot \alpha_n e \cdot k =$$
$$= \varphi x_1 \cdot x_2 \cdot \varphi x_3 \cdot x_4 \cdot \ldots \cdot x_{i-2} \cdot (\alpha_1 e \cdot \varphi\alpha_2 e \cdot \alpha_3 e \cdot \varphi\alpha_4 e \cdot \ldots \cdot \alpha_{i-1} e \cdot \varphi x_{i-1} \cdot$$
$$\cdot \alpha_{i+1} e \cdot \varphi\alpha_{i+2} e \cdot \ldots \cdot \varphi\alpha_{n-1} e \cdot \alpha_n e \cdot k) \cdot x_i \cdot \varphi x_{i+1} \cdot x_{i+2} \cdot \ldots \cdot x_{n-1} \cdot \varphi x_n \cdot k =$$
$$= A(\{\varphi x_j\}_{j=1}^{i-2}, L_i(\bar{a})x_{i-1}, \{\varphi x_j\}_{j=i}^n),$$

i.e. $L_i(\bar{a})$ is a quasiautomorphism of $Q(A)$.

We also have

$$R_k A(x_1^n) = R_k(x_1 \cdot \varphi x_2 \cdot x_3 \cdot \varphi x_4 \cdot \ldots \cdot \varphi x_{n-1} \cdot x_n \cdot k) =$$
$$= x_1 \cdot \varphi x_2 \cdot x_3 \cdot \varphi x_4 \cdot \ldots \cdot \varphi x_{n-1} \cdot R_k x_n \cdot k = A(x_1^{n-1}, R_k x_n),$$

i.e. $(\overset{n-1}{\varepsilon}, R_k, R_k) \in \mathfrak{I}_A$.

Note that φ is an automorphism of $Q(A)$. Indeed,

$$\varphi A(x_1^n) = \varphi(x_1 \cdot \varphi x_2 \cdot x_3 \cdot \varphi x_4 \cdot \ldots \cdot \varphi x_{n-1} \cdot x_n \cdot k) =$$
$$= \varphi x_1 \cdot x_2 \cdot \varphi x_3 \cdot x_4 \cdot \ldots \cdot x_{n-1} \cdot \varphi x_n \cdot k = A(\{\varphi x_i\}_{i=1}^n).$$

If $Q(A)$ is a symmetric n-group without an identity element, then in the proof we put $\varphi = \varepsilon$ according (1). If $Q(A)$ is a symmetric n-group with an identity element, then put $\varphi = R_k = \varepsilon$. Using **Lemma 1** we complete the proof.

Lemma 2. *Each quasiautomorphism δ of a n-IP-group $Q(A)$*

$$A(x_1^n) = x_1 \cdot \varphi x_2 \cdot x_3 \cdot \varphi x_4 \cdot \ldots \cdot \varphi x_{n-1} \cdot x_n \cdot k$$

has the form

$$\delta = R_{\delta k}\theta_0 R_k^{-1}, \tag{10}$$

where θ_0 is some automorphism of $Q(\cdot)$.

Proof. Let $T = (\alpha_1^n, \delta)$ be an autotopy of a nonsymmetric n-IP-group $Q(A)$ without an identity element, which is reduced to a binary abelian group $Q(\cdot)$:

$$A(x_1^n) = x_1 \cdot \varphi x_2 \cdot x_3 \cdot \varphi x_4 \cdot \ldots \cdot \varphi x_{n-1} \cdot x_n \cdot k.$$

Transforming (7) and (8) we receive

$$\alpha_i = L_i^{-1}(\bar{a})\delta R_k = L_i(\overline{Ia})\delta R_k$$

for each odd i and

$$\alpha_i = L_i^{-1}(\bar{a})\delta R_k \varphi = L_i(\overline{I\varphi a})\delta R_k \varphi$$

for each even i, where

$$(\overline{Ia}) = A(\{I\alpha_i e\}_{i=1}^n),$$

$$(\overline{I\varphi a}) = A(\{I\varphi\alpha_i e\}_{i=1}^n).$$

Indeed, according to (6), by odd i it follows from

$$A(\{I\alpha_j e\}_{j=1}^{i-1}, A(\{\alpha_j e\}_{j=1}^{i-1}, x, \{\alpha_j e\}_{j=i+1}^n), \{I\alpha_j e\}_{j=i+1}^n) = x$$

that

$$L_i(\overline{Ia})L_i(\bar{a})x = x, \quad L_i^{-1}(\bar{a})x = L_i(\overline{Ia})x.$$

By even i from

$$A(\{I\varphi\alpha_j e\}_{j=1}^{i-1}, A(\{\alpha_j e\}_{j=1}^{i-1}, x, \{\alpha_j e\}_{j=i+1}^n), \{I\varphi\alpha_j e\}_{j=i+1}^n) = x$$

it follows that

$$L_i(\overline{I\varphi a})L_i(\bar{a})x = x, \quad L_i^{-1}(\bar{a})x = L_i(\overline{I\varphi a})x.$$

Hence,

$$T = (L_1(\overline{Ia})\delta R_k, L_2(\overline{I\varphi a})\delta R_k\varphi, L_3(\overline{Ia})\delta R_k, L_4(\overline{I\varphi a})\delta R_k\varphi, \ldots, L_n(\overline{Ia})\delta R_k, \delta),$$

i.e.

$$\begin{aligned}\delta A(x_1^n) &= A(L_1(\overline{Ia})\delta R_k x_1, L_2(\overline{I\varphi a})\delta R_k \varphi x_2, L_3(\overline{Ia})\delta R_k x_3, \ldots, L_n(\overline{Ia})\delta R_k x_n) = \\ &= A(A(\delta R_k x_1, I\alpha_2 e, \ldots, I\alpha_n e), A(I\varphi\alpha_1 e, \delta R_k\varphi x_2, I\varphi\alpha_3 e, \ldots, I\varphi\alpha_n e), \\ &\ldots, A(I\alpha_1 e, \ldots, I\alpha_{n-1}e, \delta R_k x_n)) = \delta R_k x_1 \cdot I\varphi\alpha_2 e \cdot \ldots \cdot I\alpha_n e \cdot k \cdot \\ &\cdot \varphi(I\varphi\alpha_1 e \cdot \varphi\delta R_k \varphi x_2 \cdot I\varphi\alpha_3 e \cdot I\alpha_4 e \cdot \ldots \cdot I\varphi\alpha_n e \cdot k) \cdot \ldots \cdot I\alpha_1 e \cdot I\varphi\alpha_2 e \cdot \ldots \cdot \delta R_k x_n \cdot k \cdot k = \\ &= \delta R_k x_1 \cdot I\alpha_1 e \cdot I\varphi\alpha_2 e \cdot I\alpha_3 e \cdot I\varphi\alpha_4 e \cdot \ldots \cdot I\alpha_n e \cdot k \cdot \delta R_k \varphi x_2 \cdot I\alpha_1 e \cdot I\varphi\alpha_2 e \cdot I\alpha_3 e \cdot I\varphi\alpha_4 e \cdot \ldots \cdot I\alpha_n e \cdot \\ &\cdot k \cdot \ldots \delta R_k \varphi x_{n-1} \cdot I\alpha_1 e \cdot I\varphi\alpha_2 e \cdot I\alpha_3 e \cdot I\varphi\alpha_4 e \cdot \ldots \cdot I\alpha_n e \cdot k \cdot \delta R_k x_n,\end{aligned}$$

since $I\varphi x = \varphi I x$. But

$$\delta A(x_1^n) = \delta(x_1 \cdot \varphi x_2 \cdot x_3 \cdot \varphi x_4 \cdot \ldots \cdot x_n \cdot k) = \delta R_k(x_1 \cdot \varphi x_2 \cdot x_3 \cdot \varphi x_4 \cdot \ldots \cdot x_n),$$

and

$$\begin{aligned}I\alpha_1 e \cdot I\varphi\alpha_2 e \cdot I\alpha_3 e \cdot I\varphi\alpha_4 e \cdot \ldots \cdot I\alpha_n e \cdot k &= I(\alpha_1 e \cdot \varphi\alpha_2 e \cdot \alpha_3 e \cdot \varphi\alpha_4 e \cdot \ldots \cdot \alpha_n e \cdot k) = \\ = IA(\{\alpha_i e\}_{i=1}^n) = I\delta A(\overset{n}{e}) &= I\delta(e \cdot \varphi e \cdot e \cdot \varphi e \cdot \ldots \cdot e \cdot k) = I\delta k,\end{aligned}$$

therefore

$$\delta R_k(x_1 \cdot \varphi x_2 \cdot x_3 \cdot \varphi x_4 \cdot \ldots \cdot x_n) = (\delta R_k x_1 \cdot I\delta k) \cdot (\delta R_k \varphi x_2 \cdot I\delta k) \cdot \ldots \cdot (\delta R_k \varphi x_{n-1} \cdot I\delta k) \cdot \delta R_k x_n.$$

Changing x_{2i} for φx_{2i} ($2i<n$), and multiplying both parts of the last equality by $I\delta k$ we get

$$\delta R_k^*(x_1 \cdot x_2 \cdot \ldots \cdot x_n) I\delta k = (\delta R_k x_1 \cdot I\delta k) \cdot (\delta R_k x_2 \cdot I\delta k) \cdot \ldots \cdot (\delta R_k x_n \cdot I\delta k).$$

Let

$$\delta R_k x \cdot I\delta k = \theta_0 x. \tag{11}$$

Then

$$\theta_0(x_1 \cdot x_2 \cdot \ldots \cdot x_n) = \theta_0 x_1 \cdot \theta_0 x_2 \cdot \ldots \cdot \theta_0 x_n,$$

i.e. θ_0 is an automorphism of $Q(\cdot)$. It follows from (11) that

$$\delta R_k x = R_{\delta k}\theta_0 x$$

whence (10) follows.

Note, that if $Q(A)$ is a symmetric n-IP-group without an identity element, then $\varphi = \varepsilon$, i.e.

$$A(x_1^n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot k,$$

and according to (1) and (4)

$$\alpha_i = L_i^1(\bar{a})\delta R_k = L_i(\overline{IL_k a})\delta R_k, \quad i \in \overline{1,n},$$

where

$$L_1(\overline{IL_k a})x = A(x, IL_k\alpha_2 e, IL_k\alpha_3 e, I\alpha_4 e, \ldots, I\alpha_n e),$$
$$L_2(\overline{IL_k a})x = A(IL_k\alpha_1 e, x, IL_k\alpha_3 e, I\alpha_4 e, \ldots, I\alpha_n e),$$
$$L_3(\overline{IL_k a})x = A(IL_k\alpha_1 e, IL_k\alpha_2 e, x, I\alpha_4 e, \ldots, I\alpha_n e),$$
$$L_4(\overline{IL_k a})x = A(IL_k\alpha_1 e, IL_k\alpha_2 e, I\alpha_3 e, x, I\alpha_5 e, \ldots, I\alpha_n e),$$

....

$$L_n(\overline{IL_k a})x = A(IL_k\alpha_1 e, IL_k\alpha_2 e, I\alpha_3 e, \ldots, I\alpha_{n-1} e, x).$$

Thus,

$$T = (\{L_i(\overline{IL_k a})\delta R_k\}_{i=1}^n, \delta),$$

i.e.

$$\begin{aligned}
\delta A(x_1^n) = A(&A(\delta R_k x_1, IL_k\alpha_2 e, IL_k\alpha_3 e, I\alpha_4 e, \ldots, I\alpha_n e),\\
&A(IL_k\alpha_1 e, \delta R_k x_2, IL_k\alpha_3 e, I\alpha_4 e, \ldots, I\alpha_n e),\\
&A(IL_k\alpha_1 e, IL_k\alpha_2 e, \delta R_k x_3, I\alpha_4 e, \ldots, I\alpha_n e),\\
&A(IL_k\alpha_1 e, IL_k\alpha_2 e, I\alpha_3 e, \delta R_k x_4, I\alpha_5 e, \ldots, I\alpha_n e),\\
&\ldots, A(IL_k\alpha_1 e, IL_k\alpha_2 e, I\alpha_3 e, \ldots, I\alpha_{n-1} e, \delta R_k x_n)) =\\
&= \delta R_k x_1 \cdot I\alpha_2 e \cdot Ik \cdot I\alpha_3 e \cdot Ik \cdot I\alpha_4 e \cdot \ldots \cdot I\alpha_n e \cdot k \cdot\\
&\cdot I\alpha_1 e \cdot Ik \cdot \delta R_k x_2 \cdot I\alpha_3 e \cdot Ik \cdot I\alpha_4 e \cdot \ldots \cdot I\alpha_n e \cdot k \cdot\\
&\cdot I\alpha_1 e \cdot Ik \cdot I\alpha_2 e \cdot Ik \cdot \delta R_k x_3 \cdot I\alpha_4 e \cdot \ldots \cdot I\alpha_n e \cdot k \cdot\\
&\cdot I\alpha_1 e \cdot Ik \cdot I\alpha_2 e \cdot Ik \cdot I\alpha_3 e \cdot \delta R_k x_4 \cdot I\alpha_5 e \cdot \ldots \cdot I\alpha_n e \cdot k \cdot\\
&\ldots \cdot I\alpha_1 e \cdot Ik \cdot I\alpha_2 e \cdot Ik \cdot I\alpha_3 e \cdot \ldots \cdot I\alpha_{n-1} e \cdot \delta R_k x_n \cdot k \cdot k =\\
&= (\delta R_k x_1 \cdot I\alpha_1 e \cdot I\alpha_2 e \cdot \ldots \cdot I\alpha_n e \cdot Ik) \cdot (\delta R_k x_2 \cdot I\alpha_1 e \cdot I\alpha_2 e \cdot \ldots \cdot I\alpha_n e \cdot Ik) \cdot\\
&\ldots \cdot \delta R_k x_{n-1} \cdot I\alpha_1 e \cdot I\alpha_2 e \cdot \ldots \cdot I\alpha_n e \cdot Ik) \cdot \delta R_k x_n.
\end{aligned}$$

Next, since

$$\delta A(x_1^n) = \delta R_k(x_1 \cdot x_2 \cdot \ldots \cdot x_n),$$
$$I\alpha_1 e \cdot I\alpha_2 e \cdot \ldots \cdot I\alpha_n e \cdot Ik = I(\alpha_1 e \cdot \alpha_2 e \cdot \ldots \cdot \alpha_n e \cdot k) =$$

$$= IA(\{\alpha_i e\}_{i=1}^{n}) = I\delta A(\overset{n}{e}) = I\delta(e \cdot e \cdot \ldots \cdot e \cdot k) = I\delta k,$$

then, multiplying both parts of this equality by $I\delta k$, we have

$$\delta R_k(x_1 \cdot x_2 \cdot \ldots \cdot x_n) = (\delta R_k x_1 \cdot I\delta k) \cdot (\delta R_k x_2 \cdot I\delta k) \cdot \ldots \cdot (\delta R_k x_n \cdot I\delta k).$$

Let

$$\delta R_k x \cdot I\delta k = \theta_0 x.$$

Then

$$\theta_0(x_1 \cdot x_2 \cdot \ldots \cdot x_n) = \theta_0 x_1 \cdot \theta_0 x_2 \cdot \ldots \cdot \theta_0 x_n,$$

i.e. θ_0 is an automorphism of $Q(\cdot)$ and (10) is true.

If $Q(A)$ is a symmetric n-group with an identity element, then the proof is analogous to that of a nonsymmetric n-IP-group when $\varphi = \varepsilon$, $k = e$. Note that in this case the automorphism $\theta_0 = R_{\delta e}^{-1}\delta$ of $Q(\cdot)$ is also an automorphism of $Q(A)$, since

$$\theta_0 A(x_1^n) = \theta_0(x_1 \cdot x_2 \cdot \ldots \cdot x_n) = \theta_0 x_1 \cdot \theta_0 x_2 \cdot \ldots \cdot \theta_0 x_n = A(\theta_0 x_1, \theta_0 x_2, \ldots, \theta_0 x_n).$$

Now we can easy prove the following

Theorem. *Every autotopy $T = (\alpha_1^n, \delta)$ of a n-IP-group $Q(A)$:*

$$A(x_1^n) = x_1 \cdot \varphi x_2 \cdot x_3 \cdot \varphi x_4 \cdot \ldots \cdot \varphi x_{n-1} \cdot x_n \cdot k$$

has the form

$$\begin{aligned} T = (&L_1^{-1}(\bar{a})R_{\delta k}, L_2^{-1}(\bar{a})\delta\varphi\delta^{-1}R_{\delta k}, L_3^{-1}(\bar{a})R_{\delta k}, \\ &L_4^{-1}(\bar{a})\delta\varphi\delta^{-1}R_{\delta k}, \ldots, L_n^{-1}(\bar{a})R_{\delta k}, \delta R_k^{-1}\delta^{-1}R_{\delta k})\theta_0, \end{aligned} \tag{12}$$

where $\theta_0 = R_{\delta k}^{-1}\delta R_k$ is an automorphism of the binary abelian group $Q(\cdot)$.

Proof. Let $T = (\alpha_1^n, \delta)$ be an autotopy of a n-IP-group $Q(A)$. Then according to (9) this autotopy has the form

$$\begin{aligned} T = (&L_1^{-1}(\bar{a})R_{\delta k}, L_2^{-1}(\bar{a})\delta\varphi\delta^{-1}R_{\delta k}, L_3^{-1}(\bar{a})R_{\delta k}, \\ &L_4^{-1}(\bar{a})\delta\varphi\delta^{-1}R_{\delta k}, \ldots, L_n^{-1}(\bar{a})R_{\delta k}, \delta R_k^{-1}\delta^{-1}R_{\delta k})R_{\delta k}^{-1}\delta R_k. \end{aligned}$$

But, by **Lemma 2**,

$$R_{\delta k}^{-1}\delta R_k = \theta_0$$

is an automorphism of $Q(\cdot)$ in all cases. The theorem is proved.

From this **theorem** it follows that

1) if $Q(A)$ is a symmetric n-IP-group without an identity element, then according (1) with $\varphi = \varepsilon$ we have

$$T = (L_1^{-1}(\bar{a})R_{\delta k}, L_2^{-1}(\bar{a})R_{\delta k}, \ldots, L_n^{-1}(\bar{a})R_{\delta k}, \delta R_k^{-1}\delta^{-1}R_{\delta k})\theta_0.$$

2) if $Q(A)$ is a symmetric n-IP-group with an identity element, then in accord with (2), where $\varphi = \varepsilon$ and $k = e$, (12) takes on the form

$$T = (\{L_i^{-1}(\bar{a})R_{\delta e}\}_{i=1}^{n}, R_{\delta e})\theta_0, \tag{13}$$

where $\theta_0 = R_{\delta e}^{-1}\delta$ is an automorphism of $Q(\cdot)$ and $Q(A)$. In this case the form of an autotopy can be simplified. Really, since for each $i \in \overline{1,n}$

$$L_i^{-1}(\bar{a})R_{\delta e}x = L_i(\overline{Ia})R_{\delta e}x = A(\{I\alpha_j e\}_{j=1}^{i-1}, x\cdot\delta e, \{I\alpha_j e\}_{j=i+1}^{n}) =$$

$$= I\alpha_1 e\cdot I\alpha_2 e\cdot\ldots\cdot I\alpha_{i-1}e\cdot x\cdot \delta \overset{n}{A(e)}\cdot I\alpha_{i+1}e\cdot\ldots\cdot I\alpha_n e =$$

$$= I\alpha_1 e\cdot I\alpha_2 e\cdot\ldots\cdot I\alpha_{i-1}e\cdot x\cdot\alpha_1 e\cdot\alpha_2 e\cdot\ldots\cdot\alpha_{i-1}e\cdot\alpha_i e\cdot\alpha_{i+1}e\cdot\ldots\cdot\alpha_n e\cdot I\alpha_{i+1}e\cdot\ldots\cdot I\alpha_n e =$$

$$= x\cdot\alpha_i e = R_{\alpha_i e}x,$$

$$\theta_0 x = R_{\delta e}^{-1}\delta x = R_{I\delta e}\delta x = \delta x\cdot I\delta e = \delta A(\overset{i-1}{e}, x, \overset{n-i}{e})\cdot I\delta A(e) =$$

$$= \alpha_1 e\cdot\ldots\cdot\alpha_{i-1}e\cdot\alpha_i x\cdot\alpha_{i+1}e\cdot\ldots\cdot\alpha_n e\cdot I\alpha_1 e\cdot\ldots\cdot I\alpha_{i-1}e\cdot I\alpha_i e\cdot I\alpha_{i+1}e\cdot\ldots\cdot I\alpha_n e =$$

$$= \alpha_i x\cdot I\alpha_i e = R_{I\alpha_i e}\alpha_i x = R_{\alpha_i e}^{-1}\alpha_i x,$$

then (13) takes on the form

$$T = (\{R_{\alpha_i e}\}_{i=1}^{n}, R_{\delta e})\theta_0, \tag{14}$$

where $\theta_0 = R_{\alpha_i e}^{-1}\alpha_i$ is an automorphism of $Q(\cdot)$ and $Q(A)$.

Note that when n=2 the known result from [3] for abelian groups follows.

References

1. *Belousov V.D.* n-ary quasigroups. Kishinev, "Shtiintsa", 1972.

2. *Ursu L.A.* About the inverse property of n-ary groups. (Russian). Issled. po teorii binarnyh i n-arnyh qvazigrup. Kishinev, "Shtiintsa", 1985, p.124-133.

3. *Belousov V.D.* Foundations of theory of quasigroups and loops. (Russian). Moscow, "Nauka", 1967.

Ursu L.A. **Ph.D**
department of higher mathematica,
Technical state university,
41, Dachia str.,
Kishinau, 277060,
Moldova.

Received August 15, 1993