Quasigroups and Related Systems **5** (1998), 1 – 12

Centrally isotopic quasigroups

Galina B. Belyavskaya

Abstract

Relation of central isotopy between usual quasigroups is considered. The connection of this relation with central isotopy relation of equasigroups and with the abelian subgroup of the multiplication group of a quasigroup corresponding to the centre congruence of this quasigroup is established.

1. Introduction

In the work [10] and in Chapter III of [8] J.D.H.Smith has considered the relation of central isotopy between equasigroups (i.e. primitive quasigroups). This relation is tighter than isotopy but looser than isomorphism. In the base of this relation lies the concept of the centre congruence of an equasigroup $Q(\cdot,\backslash,/)$, introduced in the same works. In the articles [2, 3] the concept of the h-centre Z_h for an usual quasigroup $Q(\cdot)$ where h is an arbitrary fixed element of Q was introduced and it was proved that the h-centre defines a normal congruence which is called the centre congruence of $Q(\cdot)$ and does not depend on the element h. Finally, in article [5] a proof was given that the centre congruence of a quasigroup $Q(\cdot)$ coincides with the centre congruence of the equasigroup $Q(\cdot,\backslash,/)$, corresponding to $Q(\cdot)$. Thus, it was established that the h -centre is an inner characterization of the centre congruence of an equasigroup.

1991 Mathematics Subject Classification: 20N05

Keywords: quasigroup, equasigroup, centre congruence, central isotopy, multiplication group

In this article we consider the relation of central isotopy between usual quasigroups, establish its connection with the relation of central isotopy of the corresponding equasigroups and also with the abelian subgroup Γ of the multiplication group of a quasigroup $Q(\cdot)$. This subgroup was picked out in [4] and corresponds to the centre congruence of a quasigroup ($\Gamma h = Z_h$ for any $h \in Q$).

2. Preliminaries

An algebra $Q(\cdot, \backslash, /)$ with the three binary operations $\cdot, \backslash, /$ satisfying the identities

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

is called an *equasigroup* [6] (or a *primitive quasigroup* [1]).

A groupoid $Q(\cdot)$ is called a *quasigroup* if each of the equations $ax = b$, $xa = b$ has a unique solution for any $a, b \in Q$. The equasigroup $Q(\cdot, \backslash, /)$ corresponds to quasigroup $Q(\cdot)$ where

$$x \backslash y = z \Longleftrightarrow xz = y, \quad x/y = z \Longleftrightarrow zy = x.$$

The quasigroups $Q(\backslash)$ and $Q(/)$ are called the *right inverse* and the *left inverse* quasigroups for $Q(\cdot)$ respectively.

A quasigroup $Q(\cdot)$ is said to be *isotopic* to a quasigroup $P(\circ)$ if there exist three bijections $\alpha, \beta, \gamma : Q \to P$ such that $\alpha a \circ \beta b = \gamma(ab)$ for all $a, b \in Q$. The ordered triple $T = (\alpha, \beta, \gamma)$ is called an *isotopy.*

According to [10], two equasigroups $Q(\cdot, \backslash, /)$ and $P(\circ, \backslash\backslash, //)$ are called *isotopic* if for each operation ω from $\circ, \backslash\backslash, //$ ($\cdot, \backslash, /$, respectively) there exist bijections θ_1, θ_2 and $\theta_3 : Q \to P$ such that

$$\theta_1 a \omega \theta_2 b = \theta_3(a \omega b)$$

for all $a, b \in Q$.

It is easy to see that if equasigroups $Q(\cdot, \backslash, /)$ and $P(\circ, \backslash\backslash, //)$ are isotopic then the pairs of the quasigroups $Q(\cdot)$ and $P(\circ)$, $Q(\backslash)$ and $P(\backslash\backslash)$, $Q(/)$ and $P(//)$ are isotopic, and conversely, isotopy of any such pair implies isotopy of corresponding equasigroups (it suffices to make the suitable permutation in the triplet of bijections).

According to [8], a congruence α of an equasigroup $Q(\cdot,\backslash,/)$ is central iff the diagonal $\hat{Q}=\{(q,q)\mid q\in Q\}$ is a normal subquasigroup on α, i.e. if it is a class of some congruence V on α. In his case the congruence α is considered as a subquasigroup of the direct product $(Q\times Q)(\cdot,\backslash,/)$ containing the diagonal $\hat{Q}$. This congruence V on α is said to centre α [6].

By Theorem III.3.10 from [8] an equasigroup $Q(\cdot,\backslash,/)$ has a unique maximal central congruence called the *centre congruence* $\zeta(Q)$ (or $\zeta(\cdot,\backslash,/)$) of $Q(\cdot,\backslash,/)$. Thus, the centre congruence $\zeta(Q)$ of an equasigroup $Q(\cdot,\backslash,/)$ is the (unique) maximal subquasigroup in $(Q\times Q)(\cdot,\backslash,/)$ containing the diagonal $\hat{Q}$ as a normal subquasigroup.

Let V be the congruence centering the centre congruence of an equasigroup $P(\circ,\backslash\backslash,//)$.

Definition 1. An equasigroup $Q(\cdot,\backslash,/)$ is said *to be a central isotope of an equasigroup* $P(\circ,\backslash\backslash,//)$ iff there is a bijection $\theta:Q\to P$, called a *central shift*, such that for each of the operations $\circ,\backslash\backslash,//$ (correspondingly, $\cdot,\backslash,/$) denoted ω, there is an element $(p_\omega,\bar{p}_\omega)$ of $\zeta(P)$ such that

$$(p_\omega,\bar{p}_\omega)V(\theta(q_1\omega q_2),\theta q_1\omega\theta q_2) \tag{1}$$

for each pair q_1,q_2 of elements of Q.

In [8] the following properties of central isotopy were proved.

- Centrally isotopic equasigroups are isotopic (Proposition III.4.2.).
- Isomorphic equasigroups are centrally isotopic (Proposition III.4.3).
- A central shift $\theta:Q\to P$ mapping an idempotent of Q to an idempotent of P is an isomorphism (Proposition III.4.4).
- Central isotopy is an equivalence relation. Further, if $\theta:Q\to P$ is a central shift and the centre congruence $\zeta(Q)$ of Q is centered by W, then $\hat{\theta}\zeta(Q)=\zeta(P)$ and $\overline{\theta}W$ center $\zeta(P)$, where

$$\hat{\theta}:Q\times Q\to P\times P;\quad (q_1,q_2)\mapsto(\theta q_1,\theta q_2)$$

and

$$\begin{gathered}\overline{\theta}:(Q\times Q)\times(Q\times Q)\to(P\times P)\times(P\times P)\,;\\ ((q_1,q_2),(q_3,q_4))\mapsto((\theta q_1,\theta q_2),(\theta q_3,\theta q_4))\,.\end{gathered}$$

(Theorem III.4.5).

- Centrally isotopic quasigroups have isomorphic multiplication groups (Proposition III.4.6).

In articles [2, 3] the concept of h-centre Z_h of a quasigroup $Q(\cdot)$ where h is an arbitrary fixed element in Q was introduced. It was also proved that the h-centre Z_h defines the same normal congruence $\theta_z(\cdot)$ on $Q(\cdot)$ by any $h \in Q$. This congruence is called the centre congruence of the quasigroup $Q(\cdot)$. Remind that each congruence of an equasigroup $Q(\cdot, \backslash, /)$ is a normal congruence in $Q(\cdot)$ and conversely.

Let the centre congruence $\zeta(Q)$ of an equasigroup $Q(\cdot, \backslash, /)$ be denoted by $\zeta(\cdot, \backslash, /)$. By Theorem 1 from [5]

$$\zeta(\cdot, \backslash, /) = \theta_z(\cdot) = \theta_z(\backslash) = \theta_z(/),$$

where $Q(\backslash)$ and $Q(/)$ are the right inverse and the left inverse quasigroups for $Q(\cdot)$. Thus, the h-centre Z_h is the $\zeta(\cdot, \backslash, /)$-class containing the element h.

Let $G_{(\cdot)}$ be the multiplication group of a quasigroup $Q(\cdot)$, i.e. the group generated by its translations L_a, R_a ($L_a x = ax$, $R_a x = xa$) for all $a \in Q$. In [4] it was picked out an abelian normal subgroup Γ in $G_{(\cdot)}$ corresponding to the centre congruence and acting sharply transitively on each h-centre, $h \in Q$. The subgroup Γ is characterized by means of the groups of left and right regular mappings of a quasigroup $Q(\cdot)$, in the sense of [9]. Recall these concepts.

Let $Q(\cdot)$ be a quasigroup. A mapping λ (ρ) of the set Q onto Q is called left (right) regular if there is a mapping λ^* (ρ^*) such that

$$\lambda x \cdot y = \lambda^*(xy), \quad x \cdot \rho y = \rho^*(xy) \tag{2}$$

for each $x, y \in Q$. The mappings λ, λ^*, ρ, ρ^* are permutations on Q and λ^* (ρ^*) is called a conjugate to λ (ρ). The set of all left (right) regular mappings of a quasigroup (the set of all mappings conjugate to them) forms the group Λ, respectively Λ^* (R, correspondingly, R^*). These groups are subgroups of the multiplication group $G_{(\cdot)}$ of $Q(\cdot)$ since

$$\lambda^* = R_x^{-1} \lambda R_x = L_{\lambda x} L_x^{-1}, \quad \rho^* = L_x \rho L_x^{-1} = R_{\rho x} R_x^{-1} \tag{3}$$

for each $x \in Q$.

Let $Core_G(H)$ be the maximal normal subgroup of a group G which lies in a subgroup H. By Theorem 1 from [4] $Z_h = \Gamma h$ where

$$\Gamma = Core_G(\Lambda \cap R) = Core_G(\Lambda^* \cap R^*),$$

Z_h is the h-centre of a quasigroup $Q(\cdot)$, G is the multiplication group of $Q(\cdot)$.

In view of Corollary 3 from [4]

$$\Gamma = \{R_x R_y^{-1} \mid (x,y) \in \theta_z(\cdot)\} = \{L_x L_y^{-1} \mid (x,y) \in \theta_z(\cdot)\}$$
$$= \{R_x R_h^{-1} \mid x \in Z_h\} = \{L_x L_h^{-1} \mid x \in Z_h\}$$

for any arbitrary fixed h in Q.

3. Isotopic quasigroups and the subgroup Γ

Let an equasigroup $Q(\cdot, \backslash, /)$ be a central isotope of $P(\circ, \backslash\backslash, //)$. Then condition (1) means that for all q_1, q_2 of Q the pairs of the form $(\theta(q_1q_2), \theta q_1 \circ \theta q_2)$ lie in the same class of the congruence V centering the centre congruence $\zeta(P)$ of the equasigroup $P(\circ, \backslash\backslash, //)$. Analogously, in the same class by V all pairs $(\theta(q_1/q_2), \theta q_1 // \theta q_2)$ (all pairs $(\theta(q_1 \backslash q_2), \theta q_1 \backslash\backslash \theta q_2)$) are contained. But, as it was noted above, the diagonal $\hat{P}$ is one of the classes of the congruence V, so all classes of V have the form

$$\hat{P}(a_1, b_1) = \{(p,p)(a_1,b_1) \mid p \in P, (a_1,b_1) \in \zeta(P)\}.$$

Thus

$$(\theta(q_1q_2), \theta q_1 \circ \theta q_2) = (p,p) \circ (a_1, b_1)$$

and

$$\theta(q_1q_2) = p \circ a_1, \quad \theta q_1 \circ \theta q_2 = p \circ b_1$$

for all $q_1, q_2 \in Q$. From these equalities it follows that

$$R_{b_1}^{-1}(\theta q_1 \circ \theta q_2) = R_{a_1}^{-1}\theta(q_1q_2) = p,$$

or

$$(\theta q_1 \circ \theta q_2) = R_{b_1} R_{a_1}^{-1} \theta(q_1q_2) \tag{4}$$

where $R_a x = x \circ a$, i.e.

$$T_1 = (\theta, \theta, R_{b_1} R_{a_1}^{-1}\theta) \tag{5}$$

is an isotopy of the quasigroups $Q(\cdot)$ and $P(\circ)$. In the same way we establish that

$$T_2 = (\theta, \theta, R_{b_2} R_{a_2}^{-1}\theta) \tag{6}$$

is an isotopy of $Q(\backslash)$ and $P(\backslash\backslash)$, $R_a x = x \backslash\backslash a$, and

$$T_3 = (\theta, \theta, R_{b_3} R_{a_3}^{-1} \theta) \tag{7}$$

is an isotopy of $Q(/)$ and $P(//)$, $R_a x = x//a$, for some (a_2, b_2), (a_3, b_3) in $\zeta(P)$. Therefore, if an equasigroup $Q(\cdot, \backslash, /)$ is a central isotope of $P(\circ, \backslash\backslash, //)$ and θ is a central shift of this central isotopy, then there are the three isotopies (5), (6), (7) of the quasigroups $Q(\cdot)$ and $P(\circ)$ ($Q(\backslash)$ and $P(\backslash\backslash)$, $Q(/)$ and $P(//)$ correspondingly) for some (a_1, b_1), (a_2, b_2), (a_3, b_3) in $\zeta(P)$.

Let θ_z^P denote the centre congruence of a quasigroup $P(\circ)$. It is natural to give the following

Definition 2. A quasigroup $Q(\cdot)$ is said *to be a central isotope of a quasigroup* $P(\circ)$ iff there are a bijection $\theta : Q \to P$, a pair $(a, b) \in \theta_z^P$ such that

$$R_b R_a^{-1} \theta(q_1 q_2) = \theta q_1 \circ \theta q_2 \tag{8}$$

for all $q_1, q_2 \in Q$, where $R_a x = x \circ a$.

In this case $T = (\theta, \theta, R_b R_a^{-1} \theta)$ is an isotopy between $Q(\cdot)$ and $P(\circ)$.

Let $\Gamma_{(\circ)}$ be the subgroup of the multiplication group $G_{(\circ)}$ of a quasigroup $P(\circ)$ corresponding to the centre congruence θ_z^P of $P(\circ)$ (in the sense of Theorem 1 from [4]). Then we can give the following statement that is equivalent to Definition 2 (see also Corollary 3 in [4]).

Proposition 1. *A quasigroup $Q(\cdot)$ is a central isotope of a quasigroup $P(\circ)$ iff there are a bijection $\theta : Q \to P$ and $\alpha \in \Gamma_{(\circ)}$ such that*

$$\alpha\theta(q_1 q_2) = \theta q_1 \circ \theta q_2 \tag{9}$$

for all $q_1, q_2 \in Q$. □

A substitution α on P (a bijection θ) we shall call a *central torsion* (a *central shift*) of the central isotopy defined by (9). By a *central torsion* of a quasigroup $P(\circ)$ we mean its isotope $P(*)$, where $x * y = \alpha^{-1}(x \circ y)$ for all $x, y \in P$, $\alpha \in \Gamma_{(\circ)}$.

From Proposition 1 we have

Corollary 1. *If a quasigroup $Q(\cdot)$ is a central isotope of $P(\circ)$, then $Q(\cdot) \cong P(*)$, where $P(*)$ is a central torsion of $P(\circ)$.*

Proof. Indeed, let $x * y = \alpha^{-1}(x \circ y)$, $\alpha \in \Gamma_{(\circ)}$, for all $x, y \in P$. From (9) it follows that

$$q_1 q_2 = \theta^{-1}\alpha^{-1}(\theta q_1 \circ \theta q_2) = \theta^{-1}(\theta q_1 * \theta q_2)$$

i.e. $Q(\cdot) \cong P(*)$. □

Thus, a central isotopy is a sequential taking of a central torsion and an isomorphism.

Now we shall prove the following

Theorem 1. *An equasigroup $Q(\cdot, \backslash, /)$ is centrally isotopic to an equasigroup $P(\circ, \backslash\backslash, //)$ iff the quasigroup $Q(\cdot)$ is centrally isotopic to $P(\circ)$.*

Proof. Let an equasigroup $Q(\cdot, \backslash, /)$ be a central isotope of $P(\circ, \backslash\backslash, //)$, then as it was shown above, the quasigroup $Q(\cdot)$ is a central isotope of $P(\circ)$ (see (4)).

Conversely, let a quasigroup $Q(\cdot)$ be centrally isotopic to a quasigroup $P(\circ)$, i.e.

$$\theta q_1 \circ \theta q_2 = R_b R_a^{-1} \theta(q_1 q_2) \tag{10}$$

for all $q_1, q_2 \in Q$ where θ is a central shift, $(a, b) \in \theta_z^P$. But then for all $q_1, q_2 \in Q$

$$R_a^{-1}\theta(q_1 q_2) = R_b^{-1}(\theta q_1 \circ \theta q_2) = p \in P$$

and

$$\theta(q_1 q_2) = p \circ a, \quad \theta q_1 \circ \theta q_2 = p \circ b.$$

Whence,

$$(\theta(q_1 q_2), \theta q_1 \circ \theta q_2) = (p, p) \circ (a, b) \in \hat{P} \circ (a, b).$$

It means that all pairs of such form lie in the same class of the congruence V centering the centre congruence of the equasigroup $P(\circ, \backslash\backslash, //)$ since from $(a, b) \in \theta_z^P$ it follows that $(a, b) \in \zeta(\cdot, \backslash, /)$ (see Theorem 1 in [5]). Hence, the condition of Definition 1 is satisfied for the operations $(\cdot)$ and $(\circ)$.We shall show that this condition holds for the operations $(/)$ and $(//)$ $((\backslash)$ and $(\backslash\backslash))$.

From (10) it follows that

$$R_a R_b^{-1}(\theta q_1 \circ \theta q_2) = \theta(q_1 q_2) \tag{11}$$

for all $q_1, q_2 \in Q$. But $(a,b) \in \theta_z^P$, so by Theorem 1 from [4]

$$R_a R_b^{-1} \in \Gamma_{(\circ)} \subseteq \Lambda^* \cap R^*.$$

If $\lambda^* \in \Gamma_{(\circ)}$, then by (3)

$$\lambda = R_x^{-1} \lambda^* R_x \in \Gamma_{(\circ)}$$

for any $x \in P$ since $\Gamma_{(\circ)}$ is a normal subgroup in the multiplication group $G_{(\circ)}$ of $P(\circ)$. So $\lambda = R_c R_d^{-1}$ for some pair $(c,d) \in \theta_z^P$ by Corollary 3 in [4]. Now by the definition of a left regular mapping (see (2)) we get

$$R_a R_b^{-1}(\theta q_1 \circ \theta q_2) = R_c R_d^{-1} \theta q_1 \circ \theta q_2$$

for all $q_1, q_2 \in Q$. Taking into account (11), we have

$$\theta(q_1 q_2) = R_c R_d^{-1} \theta q_1 \circ \theta q_2,$$

i.e. $T_1 = (R_c R_d^{-1}\theta, \theta, \theta)$ is an isotopy between $Q(\cdot)$ and $P(\circ)$. But then $T_1' = (\theta, \theta, R_c R_d^{-1})$ is an isotopy between $Q(/)$ and $P(//)$.

Indeed, if $\alpha x \circ \beta y = \gamma(xy) = \gamma z$, then $\gamma z // \beta y = \alpha x = \alpha(z/y)$, i.e.

$$(\alpha, \beta, \gamma) \to (\gamma, \beta, \alpha).$$

Therefore,

$$R_c R_d^{-1} \theta(q_1/q_2) = \theta q_1 // \theta q_2$$

and, as in the first case, we receive that

$$(\theta(q_1/q_2), \theta q_1 // \theta q_2) = (p_1 \circ d, p_1 \circ c) \in \hat{P} \circ (d,c)$$

for $(d,c) \in \theta_z^P$ and for all $q_1, q_2 \in Q$, i.e. all pairs $(\theta(q_1/q_2), \theta q_1 // \theta q_2)$ lie in the same class. This means that the condition of Definition 1 holds for the operations $(/)$ and $(//)$.

It remains to check this condition for the operations $(\backslash)$ and $(\backslash\backslash)$. Since $\Gamma_{(\circ)}$ is a normal subgroup in $G_{(\circ)}$ and $R_a R_b^{-1} \in \Gamma_{(\circ)} \subseteq R^*$, then $R_a R_b^{-1} = \rho^*$ and $\rho = L_x^{-1} \rho^* L_x \in \Gamma_{(\circ)}$ for any $x \in P$ (see (3)). By Corollary 3 from [4] there exists a pair $(s,t) \in \theta_z^P$ such that $\rho = R_s R_t^{-1}$ and so

$$R_a R_b^{-1}(\theta q_1 \circ \theta q_2) = \theta q_1 \circ R_s R_t^{-1} \theta q_2$$

by the definition of a right regular mapping (see (2)). Taking into account (11), we get

$$\theta(q_1q_2) = \theta q_1 \circ R_s R_t^{-1} \theta q_2$$

and $T_2 = (\theta, R_s R_t^{-1}\theta, \theta)$ is an isotopy between $Q(\cdot)$ and $P(\circ)$. But then $T_2' = (\theta, \theta, R_s R_t^{-1}\theta)$ is an isotopy between $Q(\backslash)$ and $P(\backslash\backslash)$ and so

$$R_t^{-1}\theta(q_1 \backslash q_2) = R_s^{-1}(\theta q_1 \backslash\backslash \theta q_2).$$

From this equality it follows that

$$(\theta(q_1 \backslash q_2), \theta q_1 \backslash\backslash \theta q_2) \in \hat{P} \circ (t, s), \quad (t, s) \in \theta_z^P.$$

This proves that $Q(\cdot, \backslash, /)$ is an isotope of $P(\circ, \backslash\backslash, //)$ with the central shift θ in the sense of Definition 1. □

From this proof and Proposition 1 the following result follows.

Corollary 2 *The transformation of central isotopy of quasigroups is invariant with respect to parastrophy of quasigroups (i.e. with respect to passage to a conjugate quasigroup).* □

Corollary 3. *If a quasigroup $Q(\cdot)$ is a central isotope of a quasigroup $P(\circ)$, then there exist substitutions $\alpha, \alpha_1, \alpha_2$ from $\Gamma_{(\circ)}$ such that*

$$\alpha\theta(q_1q_2) = \theta q_1 \circ \theta q_2,$$
$$\theta(q_1q_2) = \alpha_1\theta q_1 \circ \theta q_2,$$
$$\theta(q_1q_2) = \theta q_1 \circ \alpha_2\theta q_2$$

for all $q_1, q_2 \in Q$. □

Using now Theorem III.4.5 from [8], we get

Corollary 4. *Central isotopy of quasigroups is an equivalence relation.*

Theorem III.4.5 in [8] describes how a central shift acts at the centre congruence. The following statement shows how a central shift and a central torsion act at the Z_h-centres, i.e. at the classes of the centre congruence.

Proposition 2. *Let a quasigroup $Q(\cdot)$ be a central isotope of $P(\circ)$ with a central shift θ and a central torsion α, $Z_h(\cdot), h \in Q$ ($Z_h(\circ), h \in P$) be the h-centre of $Q(\cdot)$ (of $P(\circ)$). Then*

$$\alpha Z_h(\circ) = Z_h(\circ), \quad \theta Z_h(\cdot) = Z_{\theta h}(\circ).$$

Proof. Let $\alpha \in \Gamma_{(\circ)}$. Taking into account Theorem 1 in [4], we get

$$\alpha Z_h(\circ) = \alpha(\Gamma_{(\circ)} h) = \Gamma_{(\circ)} h = Z_h(\circ),$$

since $\alpha \in \Gamma_{(\circ)}$. Comparing Theorem 1 from [4] and Theorem III.4.5 from [8], we get $\hat{\theta}\theta_z(\cdot) = \theta_z(\circ)$, where

$$\hat{\theta} \ : \ Q \times Q \to P \times P; \quad (q_1, q_2) \mapsto (\theta q_1, \theta q_2).$$

Then for any $h \in Q$

$$\hat{\theta}(Z_h(\cdot), h) = (\theta Z_h(\cdot), \theta h) \in \theta_z(\circ)$$

and so $\theta Z_h(\cdot) \subseteq Z_{\theta h}(\circ)$. But $\theta_z(\cdot) = \hat{\theta}^{-1}\theta_z(\circ)$, $(Z_{\theta h}(\circ), \theta h) \subseteq \theta_z(\circ)$. From these equalities it follows that $\theta^{-1} Z_{\theta h}(\circ) \subseteq Z_h(\cdot)$. Hence, $\theta Z_h(\cdot) = Z_{\theta h}(\circ)$. □

According to Proposition III.4.6 from [8], centrally isotopic equasigroups have isomorphic multiplication groups. It is found that an analogous result is true for subgroups $\Gamma_{(\cdot)}$ and $\Gamma_{(\circ)}$.

Proposition 3. *If a quasigroup $Q(\cdot)$ is centrally isotopic to a quasigroup $P(\circ)$ with a central shift θ, then $\Gamma_{(\cdot)} \cong \Gamma_{(\circ)}$, namely, $\Gamma_{(\cdot)} = \theta^{-1}\Gamma_{(\circ)}\theta$.*

Proof. Let $x \cdot y = \theta^{-1}\alpha^{-1}(\theta x \circ \theta y)$, $\alpha \in \Gamma_{(\circ)}$. Then $R_a = \theta^{-1}\alpha^{-1}\tilde{R}_{\theta a}\theta$ for all $a \in Q$, where R_a ($\tilde{R}_{\theta a}$) is a right translation in $Q(\cdot)$ (in $P(\circ)$). From the last equality we get

$$R_a R_b^{-1} = \theta^{-1}\alpha^{-1}\tilde{R}_{\theta a}\tilde{R}_{\theta b}^{-1}\alpha\theta, \quad a, b \in Q.$$

Using this equality, Corollary 3 from [4] and Theorem III.4.5 from [8], we obtain

$$\Gamma_{(\cdot)} = \theta^{-1}\alpha^{-1}\Gamma_{(\circ)}\alpha\theta = \theta^{-1}\Gamma_{(\circ)}\theta,$$

since $\alpha \in \Gamma_{(\circ)}$. □

The centre $Z_{(\cdot)}$ of a loop $Q(\cdot)$, i.e. the set of $a \in Q$ such that

$$ax \cdot y = a \cdot xy, \quad x \cdot ya = xy \cdot a, \quad ax = xa$$

for all $x, y \in Q$ is a subloop of $Q(\cdot)$ (cf. [7]). Note that $Z_{(\cdot)}$ is also the h-centre for $h = e$, where e is the unit of the loop $Q(\cdot)$ (cf. [2]).

It is known that every quasigroup is isotopic to a loop. This result is not true in the case of central isotopy.

Theorem 2. *A quasigroup $P(\circ)$ is centrally isotopic to a loop iff there exists an element $a \in P$ such that $\tilde{R}_a = \tilde{L}_a \in \Gamma_{(\circ)}$ where $\tilde{R}_a x = x \circ a$, $\tilde{L}_a x = a \circ x$.*

Proof. By Corollary 1 it suffices to consider the case when a central shift is equal to the identity mapping. Let a quasigroup $P(\circ)$ be centrally isotopic to a loop $P(\cdot)$ with a central torsion α. Then $P(\cdot)$ is centrally isotopic to the quasigroup $P(\circ)$ with the central torsion α^{-1}: $xy = \alpha(x \circ y)$, $\alpha \in \Gamma_{(\cdot)}$, since by Proposition 3 $\Gamma_{(\cdot)} = \Gamma_{(\circ)}$. Let e be the unit of the loop $P(\cdot)$, then

$$e \cdot x = x \cdot e = \alpha(e \circ x) = \alpha(x \circ e) = x,$$

i.e. $\tilde{R}_e = \tilde{L}_e = \alpha^{-1} \in \Gamma_{(\circ)}$. Conversely, let there exist an element $a \in P$ in quasigroup $P(\circ)$ such that $\tilde{R}_a = \tilde{L}_a = \alpha \in \Gamma_{(\circ)}$. Then the quasigroup $P(\cdot)$: $xy = \alpha^{-1}(x \circ y)$ is a loop with the unit a. □

Corollary 5. *Every loop $Q(\circ)$ with nontrivial centre $Z_{(\circ)}$ is centrally isotopic to a loop with a nonidentical central torsion.*

Proof. Indeed, if $a \in Z_{(\circ)} \neq \emptyset$, then $R_a = L_a \in \Gamma_{(\circ)}$ since by Corollary 3 from [4] $\Gamma_{(\circ)} = \{R_a R_e^{-1} = R_a,\ a \in Z_{(\circ)} = Z_e\}$ where e is the unit of $Q(\circ)$ and the quasigroup $Q(\cdot)$: $x \cdot y = R_a^{-1}(x \circ y)$ is a loop with the unit a , centrally isotopic to the loop $Q(\circ)$. It means that $Q(\circ)$ is a central isotope of $Q(\cdot)$ with the central torsion $R_a^{-1} \in \Gamma_{(\circ)}$, since in this case $\Gamma_{(\cdot)} = \Gamma_{(\circ)}$ by Proposition 3. □

References

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

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

[3] **G. B. Belyavskaya**: *T-Quasigroups and the centre of a quasigroup*, (Russian), Math. Issled. **111** (1989), $24 - 43$.

[4] **G. B. Belyavskaya**: *Centre and multiplication groups of quasigroups*, Izv. AN Resp. Moldova, Matematica, **2** (1992), $81 - 89$.

[5] **G. B. Belyavskaya**: *On concept of centre in quasigroups*, Demonstratio Mathematica, **26** (1993), $75 - 84$.

[6] **G. Birkhoff**: *Lattice Theory*, (Russian), Nauka, Moscow, 1984.

[7] **R. H. Bruck**: *A survey of binary systems*, Springer-Verlag, Berlin, 1964.

[8] **O. Chein, H. O. Pflugfelder, J. D. H. Smith**: *Quasigroups and loops: Theory and Applications*, Heldermann, Berlin, 1990.

[9] **T. Kepka**: *Regular mappings of groupoids*, Acta Univ. Carol., Math., Phys., **12** (1971), $25 - 37$.

[10] **J. D. H. Smith**: *Mal'cev varieties*, Lecture Notes in Math., **554** (1976).

Department of Quasigroup Theory
Institute of Mathematics and Informatics
Academy of Sciences of Republic of Moldova
Str. Academiei 5
MD-2028 Chishinau
Moldova

Received November 19, 1998

Quasigroups and Related Systems **5** (1998), 35 – 52

Incidence systems over groups that can be supplemented up to projective planes

Eugene A. Kuznetsov

Abstract

In the present article incidence systems over groups, which can be supplemented up to the projective planes by two lines, are studied. All such groups and projective planes are described.

1. Introduction

At present different methods of determination of projective planes over some algebraic systems are known. Algorithms of constructing projective planes over fields, near-fields, semifields [3, 4], complete systems of orthogonal Latin squares [4, 1], ternary systems [3, 4, 1, 6], loop transversals in groups [10] etc. are described. In process of finding the new projective planes researchers more often abandon traditional methods of describing projective planes, and use construction of such incidence systems over universal algebras [2, 5, 11, 13] (in particular, over groups [14, 12]), that can be supplemented up to projective planes in some natural way.

One of the most natural methods of constructing the incidence system over group, that can be supplemented up to projective plane, consists of the following:

"points" of incidence system are all elements of group G,
"lines" of incidence system are left (right) cosets by some

1991 Mathematics Subject Classification: 20N15
Keywords: group, projective plane, incidence system

collection of subgroups of group G, and incidence relation is a belonging relation. This incidence system is supplemented up to projective plane π by the addition of all points of l lines.

It is shown in [14] that if $l = 1$ then the group G is an elementary abelian group and projective plane π is the desarguesian plane. It is shown in [12] that if $l = 2$ then over group G_K of linear transformations of a field K a projective plane can be constructed (by the method mentioned above), which is the desarguesian plane. In general case, if $l = 2$, the problem of describing all groups, that can be supplemented up to projective planes by the method mentioned above, is open. The solution of this problem will be given in the present article.

2. Necessary definitions and notations

Definition 1. A *DK-ternar* is a system $< E, (x, t, y), 0, 1 >$ (where (x, t, y) is a ternary operation on the set E and $0, 1$ are the distinguished elements in E), if the following conditions hold:

1. $(x, 0, y) = x$,
2. $(x, 1, y) = y$,
3. $(x, t, x) = x$,
4. $(0, t, 1) = t$,
5. if a, b, c, d are arbitrary elements from E and $a \neq b$, then the system
$$\begin{cases} (x, a, y) = c \\ (x, b, y) = d \end{cases}$$
has a unique solution in $E \times E$.
6. E is finite or

(*a*) if a, b, c are arbitrary elements from E and $c \neq 0, (c, a, 0) \neq b$, then the system
$$\begin{cases} (x, a, y) = b \\ (x, t, y) \neq (c, t, 0) \qquad \forall t \in E \end{cases}$$
has a unique solution in $E \times E$.

(*b*) if a, b are arbitrary elements from E and $b \neq 0$, then the inequality $(a, t, b) \neq (x, t, 0) \quad \forall t \in E$ has a unique solution in E.

Definition 2. A group G is called *sharply double transitive permutation group* on a set E, if the following conditions hold:

1. For any two pairs (a, b) and (c, d) (where $a \neq b, c \neq d$) of elements from E there exists an unique permutation $\alpha \in G$ such that $\alpha(a) = c, \alpha(b) = d$.

2. Set E is finite, or for any elements $a, b \in E$ (where $a \neq b$) there exists an unique fixed-point-free permutation $\alpha \in G$ such that $\alpha(a) = b$.

Definition 3. An *incidence system* $\Sigma(G)$ *of left (right) cosets over the system* Σ *of some subgroups of a group* G is an incidence system $< A, L, I >$ such that:

1. "Points" from A (ΣG-*points*) are all elements of the group G.
2. "Lines" from L (ΣG-*lines*) are left (right) cosets by the subgroups from Σ.
3. An incidence relation is a belonging relation.

3. Main theorems

The main results of the present article are contained in the following two theorems.

Theorem 1. *Let G be a group and Σ be a such system of subgroups of the group G that system $\Sigma(G)$ can be supplemented up to some projective plane π by all points of two lines. Then the following statements are true:*

1. *Group G is isomorphic to a sharply double transitive permutation group on some set E.*
2. *Plane π is a plane dual to the translations plane.*

Theorem 2. *Let conditions of Theorem 1 hold and all subgroups from Σ are centralizators of non-identity elements of group G. Then the following statements are true:*

1. *Group G is isomorphic to the group G_K of linear transformations of some field K.*
2. *Plane π is the desarguesian plane.*

Theorem 2 gives a negative answer to the problem 4.70 from [7].

4. Preliminary statements

Lemma 3. *Let π be an arbitrary projective plane. On plane π coordinates $(a,b),(m),(\infty)$ for points and $[a,b],[m],[\infty]$ for lines (where set E is some set with the distinguished elements $0,1$ and $a,b,m\in E$) can be introduced such that if we define a ternary operation (x,t,y) on the set E by the formula*

$$(x,t,y)=z \quad \stackrel{def}{\Longleftrightarrow} \quad (x,y)\in[t,z],$$

then system $< E,(x,t,y),0,1 >$ is a DK-ternar.

Proof. See Lemma 1 in [9]. □

Define the following binary operation (x,∞,y) on the set E:

$$(x,\infty,0)\stackrel{def}{=}x,$$

$$\begin{cases}(x,\infty,y)=u\\(x,y)\neq(u,0)\end{cases} \quad \stackrel{def}{\Longleftrightarrow} \quad (x,t,y)\neq(u,t,0) \quad \forall t\in E.$$

According to condition 6(b) of Definition 1, the operation (x,∞,y) is defined correctly.

Lemma 4. *Operation (x,∞,y) satisfies the following conditions:*

1. $\begin{cases}(x,\infty,y)=(u,\infty,v)\\(x,y)\neq(u,v)\end{cases} \quad \Longleftrightarrow \quad (x,t,y)\neq(u,t,v) \quad \forall t\in E.$
2. $(x,\infty,x)=0.$
3. *if a,b,c are an arbitrary elements from E, then system*

$$\begin{cases}(x,a,y)=b\\(x,\infty,y)=c\end{cases}$$

has a unique solution in $E\times E$.

Proof. See Lemma 4 in [9]. □

Let $< E,(x,t,y),0,1 >$ be a DK-ternar. Let $(a,b),(m),(\infty)$ be points and $[a,b],[m],[\infty]$ (where $a,b,m\in E$) be lines. We define the following incidence relation I between points and lines:

$$\begin{array}{c}
(a,b)\ I\ [c,d] \iff (a,c,b)=d \\
(a,b)\ I\ [d] \iff (a,\infty,b)=d \\
(a)\ I\ [c,d] \iff a=c \\
(a)\ I\ [\infty], \qquad (\infty)\ I\ [d], \qquad (\infty)\ I\ [\infty] \\
(a,b)\ I\ [\infty] \iff (a)\ I\ [d] \iff (\infty)\ I\ [c,d] \iff false.
\end{array} \tag{1}$$

Lemma 5. *The incidence system* $< X, L, I >$, *where*

$X = \{(a,b),(m),(\infty) \mid a,b,m \in E\}$,
$L = \{[a,b],[m],[\infty] \mid a,b,m \in E\}$,
I *- incidence relation defined in* (1),

is a projective plane.

Proof. See Lemma 5 in [9]. □

5. Proof of Theorem 1

Let conditions of Theorem 1 hold.

Lemma 6. *All subgroups from the set* Σ *of subgroups of a group* G *are exactly all* ΣG*-lines on a projective plane* π*, which are incident to* ΣG*-point* E *(*E *is the unit of* G*).*

Proof. Since the unit of a group is included to any of its subgroup, ΣG-point E is incident to all ΣG-lines-subgroups of the plane π, i.e. it is incident to all subgroups from Σ. Because cosets by the same subgroup in the group G are not intersected, ΣG-point E can not be incident to some ΣG-line, which differs from ΣG-lines-subgroups. □

Define on the plane π coordinates such that the following conditions hold:

1. ΣG-point E has coordinates $(0,1)$.

2. Supplementary lines L_1 and L_2 of the plane π (which is not ΣG-lines) have coordinates $[0]$ and $[\infty]$.

It can be done in the following way, assuming by definition:

$$L_1 = [0], \quad L_2 = [\infty], \quad L_1 \cap L_2 = (\infty).$$

Let M_1, M_2 be arbitrary lines on plane π, which are incident to the ΣG-point E and are not incident to the point (∞). Let

$$O = M_1 \cap L_1, \quad I = M_2 \cap L_1, \quad X = M_1 \cap L_2, \quad Y = M_2 \cap L_2.$$

Points X, Y, O, I are four points in a general position on the plane π (this means that any line contains at most two of these points). Introducing coordinates on π according to Lemma 1 from [9] (see also Lemma 3), we obtain the necessary coordinatization.

According to coordinatization introduced above, we obtain

$$M_1 = [0,0], \qquad M_2 = [1,1],$$

and ΣG-lines M_1 and M_2 contain exactly by two supplemented points (i.e. points, which are incident to supplemented lines of the plane π) - points $(0,0)$ and (0), $(1,1)$ and (1), correspondingly.

We examine the following two classes of "parallel" lines on the plane π - cosets by subgroups M_1 and M_2:

$$\begin{array}{cccc} M_1^{(0)} = M_1, & M_1^{(1)}, & \ldots \; M_1^{(k)}, & \ldots \\ M_2^{(0)}, & M_2^{(1)} = M_2, & \ldots \; M_2^{(m)}, & \ldots \end{array}$$

Since cosets $M_1^{(i)}$ $(M_2^{(j)})$ either don't intersect or coincide, then as lines of π, they can intersect only in supplemented points of the plane π.

Lemma 7. *All lines $M_1^{(i)}$ $(M_2^{(j)})$ intersect in the same supplemented point of the plane π.*

Proof. Assume the contrary, i.e. there exist two different lines $M_1^{(i)}$ and $M_1^{(j)}$ such that

$$M_1 \cap M_1^{(i)} = (0,0), \quad M_1 \cap M_1^{(j)} = (0).$$

But lines $M_1^{(i)}$ and $M_1^{(j)}$ must intersect in a supplemented point of the plane π too. We have:

$$\begin{array}{rcl} (0,0) & \in & M_1^{(i)} \implies M_1^{(i)} = [i,0], \\ (0) & \in & M_1^{(j)} \implies M_1^{(j)} = [0,j]. \end{array}$$

But the line $[i,0]$ is incident to only two supplemented points of π: the point $(0,0)=[i,0]\cap[0]$ and the point $(i)=[i,0]\cap[\infty]$. Analogously, line $[0,j]$ is incident to only two supplemented points of π: the point $(0)=[0,j]\cap[\infty]$ and the point $(j,j)=[0,j]\cap[0]$. Since

$$(0,0)=M_1\cap M_1^{(i)}\neq M_1^{(j)}\cap M_1^{(i)}\neq M_1\cap M_1^{(j)}=(0),$$

then $(i)=M_1^{(j)}\cap M_1^{(i)}=(j,j)$, which is a contradiction.

For the class of lines $M_2^{(j)}$ the proof is analogous. □

We will suppose below that cosets by subgroups from the set Σ are left cosets. Proof of Theorem 1 in the case of right cosets by subgroups from the set Σ is analogous.

According to Lemma 5, only following four cases may take place:

Case 1. $\bigcap\limits_i M_1^{(i)}=(0),\qquad \bigcap\limits_j M_2^{(j)}=(1).$

Case 2. $\bigcap\limits_i M_1^{(i)}=(0,0),\quad \bigcap\limits_j M_2^{(j)}=(1,1).$

Case 3. $\bigcap\limits_i M_1^{(i)}=(0),\qquad \bigcap\limits_j M_2^{(j)}=(1,1).$

Case 4. $\bigcap\limits_i M_1^{(i)}=(0,0),\quad \bigcap\limits_j M_2^{(j)}=(1).$

Case 2 is reduced to Case 1 by rearrangement of supplemented lines $L_1=[0]$ and $L_2=[\infty]$ before coordinatization of the plane π. Cases 3 and 4 are impossible. Indeed, if Case 3 holds, then

$$\bigcap_i M_1^{(i)}=(0)\implies M_1^{(i)}=[0,i],$$
$$\bigcap_j M_2^{(j)}=(1,1)\implies M_2^{(j)}=[j,1].$$

So we obtain $M_1^{(1)}=[0,1]=M_2^{(0)}$, i.e. for some $g_1,g_2\in G$

$$g_1\cdot[0,0]=g_1\cdot M_1^{(0)}=g_2\cdot M_2^{(1)}=g_2\cdot[1,1].$$

Whence we obtain $[1,1]=(g_2^{-1}g_1)\cdot[0,0]$.

Because $[0,0] \neq [1,1]$, then $(g_2^{-1}g_1) \notin [0,0]$. So we have

$$e \notin (g_2^{-1}g_1) \notin [0,0] = [1,1] \ni e.$$

That is a contradiction. Impossibility of Case 4 is shown analogously.

In Case 1 we have:

$$\begin{aligned} (0) \in M_1^{(i)} &\implies M_1^{(i)} = [0,i], \\ (1) \in M_2^{(j)} &\implies M_2^{(j)} = [1,j]. \end{aligned}$$

For $M_1^{(i)} = [0,i] \doteq A_i$ and $M_2^{(j)} = [1,j] \doteq B_j$ we have

$$A_0 \cap B_1 = [0,0] \cap [1,1] = (0,1)$$

$$A_i \cap B_j = \begin{cases} [0,i] \cap [1,j], & if \quad i \neq j \\ [0,i] \cap [1,i], & if \quad i = j \end{cases} = \begin{cases} (i,j) \in G, & if \quad i \neq j \\ (i,i) \notin G, & if \quad i = j. \end{cases}$$

Now let

$$a_t = \begin{cases} A_0 \cap B_t, & if \quad t \neq 0 \\ c_0 = B_0 \cap A_1, & if \quad t = 0 \end{cases}$$

$$b_t = \begin{cases} B_1 \cap A_t, & if \quad t \neq 1 \\ c_0 = B_0 \cap A_1, & if \quad t = 1. \end{cases}$$

Obviously $A_t = b_t \cdot A_0$ and $B_t = a_t \cdot B_1$.

Lemma 8. *The following statements are true:*

1. $(A_0 \cdot c_0) \cap B_1 = (B_1 \cdot c_0) \cap A_0 = \emptyset$.
2. $(A_0 \cdot c_0) \cap A_0 = (B_1 \cdot c_0) \cap B_1 = \emptyset$.
3. $A_t \cdot c_0 = B_t$ *and* $B_t \cdot c_0 = A_t$ *for* $t \in E$.

Proof. **1**. We prove only the first equality. The proof of the second is analogous. Assume the contrary, i.e. that there exists an element $g_0 \in G$ such that

$$g_0 \in (A_0 \cdot c_0) \cap B_1 = (A_0 \cdot (A_1 \cap B_0)) \cap B_1.$$

Then we obtain

$$\begin{cases} g_0 \in B_1 \\ g_0 \in A_0 \cdot (A_1 \cap B_0) \end{cases} \iff \begin{cases} g_0 = b \in B_1 \\ g_0 \in (a \cdot A_1) \cap (a \cdot B_0) \\ a \in A_0 \end{cases} \iff$$

$$\left\{\begin{array}{l} a \in A_0 \\ B_1 \ni b = (a \cdot A_1) \cap (a \cdot B_0) \end{array}\right. \Longleftrightarrow \left\{\begin{array}{l} a \in A_0 \\ a \cdot B_0 = B_1 \end{array}\right. \Longleftrightarrow$$

$$\left\{\begin{array}{l} a^{-1} \in A_0 \\ B_0 = a^{-1} \cdot B_1 \end{array}\right. \Longleftrightarrow \left\{\begin{array}{l} a^{-1} \in A_0 \\ a^{-1} \in B_0 \end{array}\right. \Longrightarrow a^{-1} \in A_0 \cap B_0 = \emptyset.$$

We have obtained a contradiction.

2. As in the previous case assume that there exists an element $g_0 \in G$ such that

$$g_0 \in (A_0 \cdot c_0) \cap A_0 = (A_0 \cdot (A_1 \cap B_0)) \cap A_0 \,.$$

Then

$$\left\{\begin{array}{ll} g_0 \in A_0, & g_0 = a \cdot c_0 \\ a \in A_0, & c_0 = A_1 \cap B_0 \end{array}\right. \Longleftrightarrow \left\{\begin{array}{l} c_0 \in B_0 \\ c_0 = (a^{-1} \cdot g_0) \in A_0 \,, \end{array}\right.$$

which implies $c_0 = A_0 \cap B_0 = \emptyset$. But this is impossible.

The obtained contradiction proves the first equality.

The proof of the second is analogous.

3. Observe that $B_t = a_t \cdot B_1$ and $a_t \in A_0$ for any $t \neq 0$. According to statement **1** of the Lemma, for any $t \neq 0$ we have

$$\begin{aligned} (A_0 \cdot c_0) \cap B_t &= (a_t \cdot a_t^{-1}) \cdot ((A_0 \cdot c_0) \cap (a_t \cdot B_1)) \\ &= a_t \cdot ((a_t^{-1} \cdot A_0 \cdot c_0) \cap B_1) \\ &= a_t \cdot ((A_0 \cdot c_0) \cap B_1) = a_t \cdot \emptyset = \emptyset, \end{aligned}$$

which gives

$$A_0 \cdot c_0 = B_0. \tag{2}$$

As we have $A_t = b_t \cdot A_0$ (where $b_1 = c_0$ and $b_t \in B_1$ for $t \neq 1$) for any t, then from (2) we obtain

$$A_t \cdot c_0 = b_t \cdot A_0 \cdot c_0 = b_t \cdot B_0 = B_{\alpha(t)} \,. \tag{3}$$

According to statement **2** of the Lemma, we have for any t

$$(A_t \cdot c_0) \cap A_t = (b_t \cdot A_0 \cdot c_0) \cap (b_t \cdot A_0) = b_t \cdot ((A_0 \cdot c_0) \cap A_0) = b_t \cdot \emptyset = \emptyset,$$

which together with (3) implies $B_{\alpha(t)} \cap A_t = \emptyset$.

It means that $B_{\alpha(t)} = B_t$ for any t. Applying (3) we obtain $A_t \cdot c_0 = B_t$, which completes the proof of the first equality. Analogously we can prove the second equality. □

Corollary 1. *The following equality is true* $c_0 = c_0^{-1}$.

Proof. From the above Lemma

$$c_0^2 = c_0 \cdot c_0 = (A_1 \cap B_0) \cdot c_0 = (A_1 \cdot c_0) \cap (B_0 \cdot c_0) = B_1 \cap A_0 = e,$$

which gives $c_0 = c_0^{-1}$. □

Lemma 9. *There exists a coordinatization of plane* π *such that it satisfies all conditions mentioned above and the following equalities hold:*

$$[t,t] = b_t \cdot [0,0] \cdot b_t^{-1} = b_t \cdot A_0 \cdot b_t^{-1}$$

for any $t \in E$.

Proof. According to Lemma 6 and Corollary 1 we have

$$\begin{aligned} b_0 \cdot A_0 \cdot b_0^{-1} &= e \cdot A_0 \cdot e = A_0 = [0,0], \\ b_1 \cdot A_0 \cdot b_1^{-1} &= c_0 \cdot A_0 \cdot c_0^{-1} = c_0 \cdot A_0 \cdot c_0 = c_0 \cdot B_0 = B_1 = [1,1]. \end{aligned}$$

To determine the coordinatization of the plane π, we choose the ΣG-lines $M_1 = A_0$ and $M_2 = B_1$ arbitrarily - they must only be incident to the point $(0,1)$ and mustn't be incident to the point (∞). Let us determine the new coordinatization of π, taking instead of ΣG-line M_2 some ΣG-line M_3, which is incident to the point $(0,1)$, but is not incident to the point (∞) and is different from ΣG-lines M_1 and M_2. This new coordinatization is determined in the same way as the coordinatization described above. Using the analogous reasonings, we obtain $M_3 = g_0 \cdot M_1 \cdot g_0^{-1}$.

But in the initial coordinatization for some $t_0 \in E$ we have

$$g_0 \in b_{t_0} \cdot A_0, \text{ i.e. } g_0 = b_{t_0} \cdot a_k \,,$$

where $a_k \in A_0$. Thus

$$M_3 = (b_{t_0} \cdot a_k) \cdot A_0 \cdot (b_{t_0} \cdot a_k)^{-1} = b_{t_0} \cdot (a_k \cdot A_0 \cdot a_k^{-1}) \cdot b_{t_0}^{-1} = b_{t_0} \cdot A_0 \cdot b_{t_0}^{-1}.$$

By the help of renaming of points (a,a) $(a \neq 0,1)$, which are incident to the line $[0]$, we obtain $M_3 = [t_0, t_0]$, i.e.

$$[t_0, t_0] = M_3 = b_{t_0} \cdot A_0 \cdot b_{t_0}^{-1}.$$

Using the analogous reasonings for every ΣG-line M_i, which is incident to the point $(0,1)$ and is not incident to the point (∞), we obtain $[t,t] = b_t \cdot A_0 \cdot b_t^{-1}$ for any $t \in E$. This completes our proof. $\square$

Let $\alpha_{x,y}$ be the ΣG-point $(x,y) = [0,x] \cap [1,y] = A_x \cap B_y$ $(x \neq y)$ and let $\hat{G}$ be the representation of the group G determined by the following permutations:

$$\alpha_{x,y}(t) = u \quad \overset{def}{\Longleftrightarrow} \quad \alpha_{x,y} \cdot A_t = A_u. \tag{4}$$

Lemma 10. *The following statements are true:*

1. *The permutation group $\hat{G}$ is isomorphic to the group G.*
2. $\alpha_{x,y}(0) = x$, $\alpha_{x,y}(1) = y$ *for any $x \neq y$ from E.*
3. *For any fixed elements $a, b \in E$, $(a \neq b)$, there exists an uniquely determined permutation $\alpha_{u,v}$ such that $\alpha_{u,v}(0) = a$, $\alpha_{u,v}(1) = b$.*
4. *For any fixed pairs $(a,b),(c,d) \in E \times E$, $(a \neq b,\ c \neq d)$, there exists an uniquely determined permutation $\alpha_{u,v} \in \hat{G}$ such that*
$$\alpha_{u,v}(a) = c, \quad \alpha_{u,v}(b) = d.$$
5. *For any fixed $a, b \in E$, $(a \neq b)$, there exists an uniquely determined fixed-point-free permutation $\alpha_{u,v}$ such that $\alpha_{u,v}(a) = b$.*

Proof. **1**. As we can see from (4), the representation $\hat{G}$ is a representation of the group G by left cosets with respect to the subgroup A_0. According to Theorem 5.3.2 from [3], the kernel of this representation is a subgroup H_0 of G such that $H_0 \subseteq A_0$ and $H_0 \lhd G$.

Taking $g = c_0 = A_1 \cap B_0$, we obtain

$$A_0 \supseteq H_0 = c_0 H_0 c_0^{-1} \subseteq c_0 A_0 c_0^{-1} = B_1,$$

i.e.

$$H_0 \subseteq A_0 \cap B_1 = e.$$

So representation (4) is the exact representation, and $\hat{G} \simeq G$.

2. We have

$$\alpha_{x,y}(0) = u \iff \alpha_{x,y} \cdot A_0 = A_u \implies \alpha_{x,y} \in A_u.$$

Directly from the definition of $\alpha_{x,y}$ we obtain $u = x$, i.e. $\alpha_{x,y}(0) = x$. By Lemma 6 we have

$$\begin{aligned} \alpha_{x,y}(1) = v \iff \alpha_{x,y} \cdot A_1 = A_v \iff \alpha_{x,y} \cdot A_1 \cdot c_0 = A_v \cdot c_0 \\ \iff \alpha_{x,y} \cdot B_1 = B_v \implies \alpha_{x,y} \in B_v. \end{aligned}$$

This gives $y = v$, i.e. $\alpha_{x,y}(1) = y$.

3. Let $a, b \in E$, $(a \neq b)$. Since $\alpha_{a,b}(0) = a$ and $\alpha_{a,b}(1) = b$, then the necessary permutation $\alpha_{u,v} \in \hat{G}$ exists and coincides with $\alpha_{a,b}$. If there exists the other permutation $\alpha_{u,v} \in \hat{G}$ such that $\alpha_{u,v}(0) = a$, $\alpha_{u,v}(1) = b$, then for the permutation $\alpha_{k,m} = \alpha_{a,b}^{-1}\alpha_{u,v}$ we have:

$$\begin{aligned} \alpha_{k,m}(0) = \alpha_{a,b}^{-1}\alpha_{u,v}(0) = \alpha_{a,b}^{-1}(a) = 0, \\ \alpha_{k,m}(1) = \alpha_{a,b}^{-1}\alpha_{u,v}(1) = \alpha_{a,b}^{-1}(b) = 1. \end{aligned}$$

Moreover, applying (4) and Lemma 6, we obtain

$$\begin{cases} \alpha_{k,m} \cdot A_0 = A_0 \\ \alpha_{k,m} \cdot A_1 = A_1 \end{cases} \iff \begin{cases} \alpha_{k,m} \in A_0 \\ \alpha_{k,m} \cdot A_1 \cdot c_0 = A_1 \cdot c_0 \end{cases} \iff$$

$$\begin{cases} \alpha_{k,m} \in A_0 \\ \alpha_{k,m} \cdot B_1 = B_1 \end{cases} \iff \begin{cases} \alpha_{k,m} \in A_0 \\ \alpha_{k,m} \in B_1 \end{cases} \iff \alpha_{k,m} = A_0 \cap B_1 = e.$$

Thus $\alpha_{a,b}^{-1}\alpha_{u,v} = e$, i.e. $\alpha_{u,v} = \alpha_{a,b}$. Hence the permutation $\alpha_{u,v}$ is a uniquely determined.

4. Let $a, b, c, d \in E$, $a \neq b$, $c \neq d$ and $\alpha_{u_0,v_0} \overset{def}{=} \alpha_{c,d}\alpha_{a,b}^{-1}$. Then

$$\begin{aligned} \alpha_{u_0,v_0}(a) = \alpha_{c,d}\alpha_{a,b}^{-1}(a) = \alpha_{c,d}(0) = c, \\ \alpha_{u_0,v_0}(b) = \alpha_{c,d}\alpha_{a,b}^{-1}(b) = \alpha_{c,d}(1) = d, \end{aligned}$$

i.e. we have proved the existence of necessary permutation $\alpha_{u,v} \in \hat{G}$.

If $\alpha_{r,s} \in \hat{G}$ and $\alpha_{r,s}(a) = c$, $\alpha_{r,s}(b) = d$, then for the permutation $\gamma = \alpha_{r,s}\alpha_{a,b}$ we have

$$\begin{aligned} \gamma(0) = \alpha_{r,s}\alpha_{a,b}(0) = \alpha_{r,s}(a) = c, \\ \gamma(1) = \alpha_{r,s}\alpha_{a,b}(1) = \alpha_{r,s}(b) = d. \end{aligned}$$

By the statement **3** of the Lemma we obtain $\gamma \equiv \alpha_{c,d}$, i.e.

$$\alpha_{r,s} = \alpha_{c,d}\alpha_{a,b}^{-1} = \alpha_{u_0,v_0}.$$

This proves that the permutation $\alpha_{u,v}$ is uniquely determined.

5. Let $a, b \in E,\ a \neq b$. Since

$$G = \left(\bigcup_{k\in E}[k,k]\right) \cup [(0,\infty,1)]$$

is the set of all ΣG-lines, which are incident to ΣG-point $(0,1)$, then we can obtain the following equivalent systems (by Lemmas 6 and 7):

$$\begin{cases} \alpha_{x,y}(a) = b \\ \alpha_{x,y}(t) \neq t \quad \forall t \in E \end{cases} \Longleftrightarrow \begin{cases} \alpha_{x,y} \cdot A_a = A_b \\ \alpha_{x,y} \cdot A_t \neq A_t \quad \forall t \in E \end{cases} \Longleftrightarrow$$

$$\begin{cases} \alpha_{x,y} \cdot b_a \cdot A_0 = b_a \cdot A_0 \\ \alpha_{x,y} \cdot b_t \cdot A_0 \neq b_t \cdot A_0 \quad \forall t \in E \end{cases} \Longleftrightarrow \begin{cases} \alpha_{x,y} \cdot b_a \in A_b \\ \alpha_{x,y} \cdot b_t \notin b_t \cdot A_0 \quad \forall t \in E \end{cases}$$

$$\Longleftrightarrow \left[\begin{array}{l} \begin{cases} a = 1, \quad b \neq 1 \\ \alpha_{x,y} \cdot c_0 \in A_b \\ \alpha_{x,y} \notin b_t A_0 b_t^{-1} \quad \forall t \in E \end{cases} \\ \begin{cases} a \neq 1, \quad b \neq a \\ \alpha_{x,y} \cdot b_a \in A_b \\ \alpha_{x,y} \notin b_t A_0 b_t^{-1} \quad \forall t \in E \end{cases} \end{array}\right. \Longleftrightarrow$$

$$\Longleftrightarrow \left[\begin{array}{l} \begin{cases} a = 1, \quad b \neq 1 \\ \alpha_{x,y} \in A_b \cdot c_0 = B_b \\ \alpha_{x,y} \notin b_t A_0 b_t^{-1} \quad \forall t \in E \end{cases} \\ \begin{cases} a \neq 1, \quad b \neq a \\ \alpha_{u,v} = \alpha_{x,y} \cdot b_a \in A_b \\ b_a^{-1} \cdot \alpha_{u,v} \notin (b_a^{-1} b_t) A_0 (b_a^{-1} b_t)^{-1} \quad \forall t \in E \end{cases} \end{array}\right. \Longleftrightarrow$$

$$\Longleftrightarrow \left[\begin{array}{l} \begin{cases} a = 1, \quad b \neq 1 \\ \alpha_{x,y} \in B_b \\ \alpha_{x,y} \notin b_t A_0 b_t^{-1} \quad \forall t \in E \end{cases} \\ \begin{cases} a \neq 1, \quad b \neq a \\ \alpha_{u,v} = \alpha_{x,y} \cdot b_a \in A_b \\ b_a^{-1} \cdot \alpha_{u,v} \notin b_{t'} A_0 b_{t'}^{-1} \quad \forall t' \in E \end{cases} \end{array}\right. \Longleftrightarrow$$

$$\Longleftrightarrow \left[\begin{array}{l} \begin{cases} a = 1, \quad b \neq 1 \\ \alpha_{x,y} \in B_b \\ \alpha_{x,y} \notin [t,t] \quad \forall t \in E \end{cases} \\ \begin{cases} a \neq 1, \quad b \neq a \\ \alpha_{u,v} = \alpha_{x,y} \cdot b_a \in A_b \\ b_a^{-1} \cdot \alpha_{u,v} \notin [t',t'] \quad \forall t' \in E \end{cases} \end{array}\right. \Longleftrightarrow$$

$$\Longleftrightarrow \left[\begin{array}{l} \begin{cases} a = 1, \quad b \neq 1 \\ \alpha_{x,y} \in B_b \\ \alpha_{x,y} \in [(0, \infty, 1)] \end{cases} \\ \begin{cases} a \neq 1, \quad b \neq a \\ \alpha_{u,v} = \alpha_{x,y} \cdot b_a \in A_b \\ b_a^{-1} \cdot \alpha_{u,v} \in [(0, \infty, 1)] \end{cases} \end{array} \right. \Longleftrightarrow$$

$$\Longleftrightarrow \left[\begin{array}{l} \begin{cases} a = 1, \quad b \neq 1 \\ \alpha_{x,y} = [1, b] \cap [(0, \infty, 1)] \end{cases} \\ \begin{cases} a \neq 1, \quad b \neq a \\ \alpha_{x,y} = ([0, b] \cap b_a \cdot [(0, \infty, 1)]) \cdot b_a^{-1} \end{cases} \end{array} \right.$$

As we can see from the last system, the existence and uniqueness of the necessary permutation $\alpha_{x,y}$ in $\hat{G}$ is obvious. □

The last lemma shows (according to Definition 2) that the group G is isomorphic to a sharply double transitive permutation group on E.

By Theorem 20.7.1 from [3] the group G is isomorphic to the group

$$H = \{\alpha_{a,b} | \alpha_{a,b}(x) = a + x \cdot (b - a),\ b \neq a\}$$

of linear transformations of some nearfield $K = < E, +, \cdot, 0, 1 >$ (a definition of a nearfield is given in [3, 9]). It is easy to see that the group operation in G can be expressed by the operations of the nearfield K in the following way:

$$\alpha_{a,b} \cdot \alpha_{c,d} = \alpha_{a+c\cdot(b-a), a+d\cdot(b-a)}. \tag{5}$$

Now we consider the following ternary operation:

$$\begin{array}{l} [x, t, y] \overset{def}{=} x + t \cdot (y - x), \\ [x, \infty, y] = x - y. \end{array}$$

Over D-ternar $< E, [x, t, y], 0, 1 >$ a projective plane π^* can be constructed (see Lemma 3), which is the plane dual to translation plane

[3, 8]. The incidence relation I^* on plane π^* is determined by:

$$\begin{array}{c} (a,b)\ I^*\ [c,d] \quad \Longleftrightarrow \quad d = a + c\cdot(b-a) \\ (a,b)\ I^*\ [d] \quad \Longleftrightarrow \quad d = a-b \\ (a)\ I^*\ [c,d] \quad \Longleftrightarrow \quad a = c \\ (a)\ I^*\ [\infty], \qquad (\infty)\ I^*\ [d], \qquad (\infty)\ I^*\ [\infty] \\ (a,b)\ I^*\ [\infty] \iff (a)\ I^*\ [d] \iff (\infty) I^*[c,d] \iff false. \end{array} \tag{6}$$

Lemma 11. *The initial plane π, which has been constructed over an incidence system $\Sigma(G)$ by supplementing two lines, is isomorphic to the plane π^*.*

Proof. According to Lemma 4, ΣG-point $(0,1)$ (the unit e of group G) is incident only to ΣG-lines of π, which are subgroups from the system Σ (i.e. lines $[c,c]$, $c\in E$ and $[(0,\infty,1)]$). Since $G \backsimeq H$ then the point $(0,1)$ of the plane π^* is incident to the lines $[c,c]$, $c \in E$ and $[-1] = [[0,\infty,1]]$. Let

$M_c = \{\alpha_{a,b}{\cdot}\alpha_{u,v} | (u,v)I^*[c,c],\ c$ be an *arbitrary fixed element from* $E\}$,

$$R = \{\alpha_{a,b}\cdot\alpha_{z,w} | (z,w)I^*[-1]\},$$

where (a,b) is an arbitrary fixed point of the plane π^*, which is not incident to the lines $[0]$ and $[\infty]$. In order to prove the isomorphism of the planes π and π^*, it is sufficient to prove that the set M_c is a line $[c,d]$ on π^* (for some $d\in E$) and the set R is a line $[h]$ on π^* (for some $h \in E$). By the help of (5) and (6) we obtain

$$(k,l)\in M_c \iff \left\{\begin{array}{c} \alpha_{k,l} = \alpha_{a,b}\cdot\alpha_{u,v} \\ (u,v)I^*[c,c] \end{array}\right. \iff \left\{\begin{array}{c} k = a+u\cdot(b-a) \\ l = a+v\cdot(b-a) \\ c = u + c\cdot(v-u) \end{array}\right. \iff$$

$$\begin{aligned} k + c\cdot(l-k) &= a+u\cdot(b-a)+c\cdot(a+v\cdot(b-a)-a-u\cdot(b-a)) \\ &= a+u\cdot(b-a)+c\cdot(v-u)\cdot(b-a) \\ &= a+(u+c\cdot(v-u))\cdot(b-a) = a+c\cdot(b-a) = d, \end{aligned}$$

i.e. $(k,l)I^*[c,d]$.

Analogously,

$$(k,l)\in R \iff \left\{\begin{array}{l} \alpha_{k,l} = \alpha_{a,b}\cdot\alpha_{z,w} \\ (z,w)I^*[-1] \end{array}\right. \iff \left\{\begin{array}{l} k = a+z\cdot(b-a) \\ l = a+w\cdot(b-a) \\ -1 = z-w \end{array}\right. \iff$$

$$\begin{aligned} k - l &= a + z \cdot (b - a) - a - w \cdot (b - a) \\ &= (z - w) \cdot (b - a) = (-1) \cdot (b - a) = a - b = h, \end{aligned}$$

i.e. $(k, l)I^*[h]$, which completes our proof. $\square$

Theorem 1 follows from the above lemmas.

6. Proof of Theorem 2

Let the assumption of Theorem 2 be satisfied.

Lemma 12. *Let $H = C_a(G)$ be the centralizer of $a \in G$, $a \neq e$. Then for any $h \in H - \{e\}$ we have $C_h(G) = H$ and H is an abelian group.*

Proof. It is evident that $e, h \in C_h(G)$ for any $h \in H - \{e\}$. If $h_1 \neq k_2$ and $h_1, h_2 \in H - \{e\}$, then

$$h_1 \in C_a(G) \iff h_1^{-1} a h_1 = a \iff a^{-1} h_1 a = h_1 \iff a \in C_{h_1}(G),$$
$$h_2 \in C_a(G) \iff h_2^{-1} a h_2 = a \iff a^{-1} h_2 a = h_2 \iff a \in C_{h_2}(G),$$

i.e. $\{e, a\} \subset C_{h_1}(G) \cap C_{h_2}(G)$.

But the centralizers $C_{h_1}(G)$ and $C_{h_2}(G)$ are lines in the plane π, so either they coincide or they have no more than one common point. Then we obtain

$$C_{h_1}(G) \equiv C_{h_2}(G) \equiv C_h(G)$$

for any $h \in H - \{e\}$. Since $a \in C_a(G) = H$ then for any $h \in H - \{e\}$ we have $H = C_h(G)$. So for any $h_1, h_2 \in H$

$$h_1 \in H = C_{h_2}(G) \iff h_1^{-1} h_2 h_1 = h_2 \iff h_2 h_1 = h_1 h_2,$$

i.e. H is an abelian group. $\square$

This means that all ΣG-lines $[c, c]$ of the plane π are abelian groups. According to (5) we have for any $a, b \in E - \{0\}$:

$$\alpha_{0,a} \cdot \alpha_{0,b} = \alpha_{0,b \cdot a}, \qquad (0, a)I^*[0, 0].$$

So multiplication of the nearfield $K =< E, +, \cdot, 0, 1 >$ is commutative, i.e. K is a field. Then the group G is isomorphic to the group G_K

of linear transformations of the field K. The plane π is isomorphic to the plane π^*, which is constructed by the natural way over the field K, i.e. it is desarguesian [3, 8].

The proof of Theorem 2 is complete.

References

[1] **J. Denes, A. D. Keedwell**: *Latin squares and their applications*, Akademiai Kiado, Budapest, 1974.

[2] **H. R. Gumm**: *The Little Desarguesian Theorem for algebras in modular varieties*, Proc. Amer. Math. Soc., **80** (1980), 393 – 399.

[3] **M. Hall**: *The theory of groups*, (Russian), Moscow, 1962.

[4] **M. Hall**: *Combinatorics*, (Russian), Moscow, 1970.

[5] **T. Ihringer**: *Projective Erweiterung von Äquivalenzklassengeometrien*, Mitt. Math. Semin. Giessen, **142** (1980), 31 – 87.

[6] **F. Kartesi**: *Introduction to finite geometries*, (Russian), Nauka, Moscow, 1980.

[7] **Kourovskaya Tetradi** (open problems of group theory) (Russian), 10th issue, supplemented, Novosibirsk, 1986.

[8] **A. V. Kuznetsov, E. A. Kuznetsov**: *On the twice-generated double homogeneous quasigroups*, (Russian). Mat. Issled., **71** (1983), 34 – 53.

[9] **E. A. Kuznetsov**: *About some algebraic systems related with projective planes*, Quasigroups and Related Systems, **2** (1995), 6 – 33.

[10] **E. A. Kuznetsov**: *Loop transversals in S_n by $St_{a,b}(S_n)$ and coordinatization of projective planes*, Quasigroups and Related Systems (in appear).

[11] **A. Pasini**: *Sul reticolo dei sottospazi passanti per uh punto in uno spasio definito da un algebra di insidenza*, Matematiche, **33** (1978), 261 – 278.

[12] **H. Schwerdtfeger**: *Projective geometry in the dimensional affine group*, Canad. J. Math., **16** (1964), 683 – 700.

[13] **H. Werner, R. Wille**: *Über den projectiven Äbshlus von Äquivalenzklassengeometrien*, Beitrage zur Geom. Algebra, (1977), 345 – 352.

[14] **R. Wille**: *Kongruentzklassengeometrien*, Lecture Notes in Mathematics, **113** (1970).

Department of Quasigroups Theory
Institute of Mathematics and Informatics
Academy of Sciences of Moldova
Academiei str., 5
MD-2028 Chishinau
Moldova
E-mail: ecuz@math.md

Received November 20, 1998

Quasigroups and Related Systems **5** (1998), 53 – 68

Invertible elements in associates and semigroups. 1

Fedir Sokhatsky

Abstract

Some invertibility criteria of an element in associates, in particular in n-ary semigroups, are given. As a corollary, axiomatics for polyagroups and n-ary groups are obtained.

Invertible elements play a special role in the theory of n-ary groupoids. For example, the structure of operations in an associate without invertible elements is still open. However, in the associate of the type (r, s, n) the structure of its operation is determined by Theorem 4 from [2] as soon as there exists at least one r-multiple invertible element in it. In particular, this theorem reduces the study of the groupoid to the study of associate of the type $(1, s, n)$ with invertible elements. Since, as was shown in [3], a binary semigroup with an invertible element is exactly a monoid, so we will take the characteristic to introduce a notion of multiary monoid.

1. Necessary informations

Let $(Q; f)$ be an $(n+1)$-ary groupoid. The operation f and the groupoid $(Q; f)$ are called (i, j)-*associative,* if the identity

$$f(x_0, \dots, x_{i-1}, f(x_i, \dots, x_{i+n}), x_{i+n+1}, \dots, x_{2n})$$
$$= f(x_0, \dots, x_{j-1}, f(x_j, \dots, x_{j+n}), x_{j+n+1}, \dots, x_{2n}).$$

1991 Mathematics Subject Classification: 20N15
Keywords: polyagroup, invertible element, n-ary group

holds in $(G; f)$.

Definition 1. A groupoid $(Q; f)$ of the arity $n + 1$ is said to be an *associate of the type* (r, s, n), where r divides s, s divides n, and $n > s$, if it is (i, j)-associative for all (i, j) such, that $i \equiv j \equiv 0 \pmod r$, and $i \equiv j \pmod s$. In an associate of the type (s, n), that is of the type $(1, s, n)$, the number s will be called a *degree of associativity*, and the associative operation f will be called *s-associative*. The least of the associativity degrees will be called a *period of associativity*.

The following theorem is proved in [4].

Theorem 1. *Let $(Q; f)$ be an associate of a type (r, s, n). If the words w_1 and w_2 differ from each other by bracketting only; the coordinate of every f's occurrence in the words w_1 and w_2 is divisible by r and there exists an one-to-one correspondence between f's occurrences in the word w_1 and those in the word w_2 such that the corresponding coordinates are congruent modulo s, then the formula $w_1 = w_2$ is an identity in $(Q; f)$.*

Here the *coordinate of the i-th occurrence of the symbol f in a word w* is called a number of all individual variables and constants, appearing in the word w from the beginning of w to the i-th occurrence of the operation symbol f.

To define an invertible element we need the notion of a shift.

Let $(Q; f)$ be an $(n + 1)$-ary groupoid. The notation $\overset{i}{a}$ denotes a sequence $a, \ldots, a$ (i times).

A transformation $\lambda_{i,a}$ of the set Q, which is determined by the equality

$$\lambda_{i,a}(x) = f(\overset{i}{a}, x, \overset{n-i}{a}), \tag{1}$$

is said to be an *i-th shift of the groupoid $(Q; f)$, induced by an element a*. Hence, the i-th shift is a partial case of the translation (see [1]). If an i-th shift is a substitution of the set Q, then the element a is called *i-invertible*. If an element a is i-invertible for all i multiple of r, then it is called *r-multiple invertible*, when $r = 1$ it is called *invertible*. The unit is always invertible, since, it determines a shift being an identity transformation.

The notion of an invertible element for binary and n-ary groupoids coincides with a well known one. Namely, if $(Q;\cdot)$ is a semigroup, and a is its arbitrary invertible element, that is the shifts $\lambda_{0,a}$ and $\lambda_{1,a}$ are substitutions of the set Q, then it is easy to prove (see [3]), that the elements $\lambda_{0,a}^{-1}(a)$, $\lambda_{1,a}^{-1}(a)$ are right and left identity elements in the semigroup. Therefore, $\lambda_{0,a}^{-1}(a) = \lambda_{1,a}^{-1}(a)$ is an identity element, left and right inverse elements of the element a are $\lambda_{1,a}^{-2}(a)$ and $\lambda_{0,a}^{-2}(a)$ respectively. Thus, $a^{-1} := \lambda_{1,a}^{-2}(a) = \lambda_{0,a}^{-2}(a)$ is an inverse element of a.

If an element a of a multiary groupoid is i-invertible, then the element $\lambda_{i,a}^{-1}(a)$ coincides with the *i-th skew* element of a, which is denoted by $\bar{a}^i$, where $\bar{a} = \bar{a}^0$, and it is determined by the equality

$$f(\overset{i}{a}, \bar{a}^i, \overset{n-i}{a}) = a.$$

The following two lemmas are proved in [2]

Lemma 2. *If in an associate of the type (r,s,n) an element a is s-multiple invertible and $i \equiv 0 \pmod{s}$, then there exists a unique i-th skew of the element a, and, in addition, the equality*

$$\bar{a} = \bar{a}^i \tag{2}$$

holds.

Lemma 3. *In every associate of the type (r,s,n) for every s-multiple invertible element of the element a and for all $i \equiv 0 \pmod{s}$ the following identities are true*

$$f(\overset{i}{a}, \bar{a}, \overset{n-i-1}{a}, x) = x, \qquad f(x, \overset{n-i-1}{a}, \bar{a}, \overset{i}{a}) = x. \tag{3}$$

2. Criteria of invertibility of elements

One of the main results of this article is the following.

Theorem 4. *An element $a \in Q$ is r-multiple invertible in an associate $(Q;f)$ of the type (r,s,n) iff there exists an element $\bar{a} \in Q$ such that*

$$f(\bar{a}, a, \ldots a, x) = x, \qquad f(x, a, \ldots a, \bar{a}) = x \tag{4}$$

holds for all $x \in Q$.

Proof. If an element a is r-multiple invertible in $(Q; f)$, then the relation (4) follows from (3) when $i = 0$.

Let the relationship (4) hold. To establish the invertibility of the element a, we have to prove the existence of an inverse transformation for every of the shifts induced by the element a. This follows from the following lemma.

Lemma 5. *Let $(Q; f)$ be an associate of the type (r, s, n). If for $a \in Q$ there exists an element $\bar{a}$ satisfying (4), then every i-th shift, induced by a, has an inverse transformation, which can be found by the formulae*

$$\begin{aligned}
&\lambda_{0,a}^{-1}(x) = f\left(x, \overset{n-s-1}{a}, \bar{a}, \overset{s-1}{a}, \bar{a}\right),\\
&\lambda_{n,a}^{-1}(x) = f\left(\bar{a}, \overset{s-1}{a}, \bar{a}, \overset{n-s-1}{a}, x\right),\\
&\lambda_{i,a}^{-1}(x) = f\left(\overset{n-s-i}{a}, \bar{a}, \overset{s-1}{a}, x, \overset{i-1}{a}, \bar{a}\right), \quad \textit{when } 0 < i \leqslant n-s,\\
&\lambda_{i,a}^{-1}(x) = f\left(\bar{a}, \overset{n-i-1}{a}, x, \overset{s-1}{a}, \bar{a}, \overset{i-s}{a}\right), \quad \textit{when } s \leqslant i < n.
\end{aligned} \tag{5}$$

Proof of Lemma. If i in (3) is a multiple of s, then

$$\begin{aligned}
x &\overset{(4)}{=} f(\bar{a}, \overset{n-1}{a}, x) \overset{(4)}{=} f(\bar{a}, \overset{i-1}{a}, f(\overset{n}{a}, \bar{a}), \overset{n-i-1}{a}, x)\\
&\overset{Th1}{=} f(f(\bar{a}, \overset{n}{a}), \overset{i-1}{a}, \bar{a}, \overset{n-i-1}{a}, x) \overset{(4)}{=} f(\overset{i}{a}, \bar{a}, \overset{n-i-1}{a}, x).
\end{aligned}$$

The other relationships from (3) are proved by the same way:

$$\begin{aligned}
x &\overset{(4)}{=} f(x, \overset{n-1}{a}, \bar{a}) \overset{(4)}{=} f(x, \overset{n-i-1}{a}, f(\bar{a}, \overset{n}{a}), \overset{i-1}{a}, \bar{a})\\
&\overset{Th1}{=} f(x, \overset{n-i-1}{a}, \bar{a}, \overset{i-1}{a}, f(\overset{n}{a}, \bar{a})) \overset{(4)}{=} f(x, \overset{n-i-1}{a}, \bar{a}, \overset{i}{a}).
\end{aligned}$$

Let us prove that the transformation $\lambda_{0,a}^{-1}$, which is determined by the equality (5) is inverse to $\lambda_{0,a}$.

$$\begin{aligned}
\lambda_{0,a}^{-1}\lambda_{0,a}(x) &\overset{(5)}{=} f(\lambda_{n,a}(x), \overset{n-s-1}{a}, \bar{a}, \overset{s-1}{a}, \bar{a}) \overset{(1)}{=} f(f(x, \overset{n}{a}), \overset{n-s-1}{a}, \bar{a}, \overset{s-1}{a}, \bar{a})\\
&\overset{Th1}{=} f(x, \overset{n-s-1}{a}, f(\overset{n}{a}, \bar{a}), \overset{s-1}{a}, \bar{a}) \overset{(3)}{=} f(x, \overset{n-1}{a}, \bar{a}) \overset{(3)}{=} x\,,
\end{aligned}$$

$$\begin{aligned}
\lambda_{0,a}\lambda_{0,a}^{-1}(x) &\overset{(5)}{=} \lambda_{0,a} f(x, \overset{n-s-1}{a}, \bar{a}, \overset{s-1}{a}, \bar{a}) \overset{(1)}{=} f(f(x, \overset{n-s-1}{a}, \bar{a}, \overset{s-1}{a}, \bar{a}), \overset{n}{a})\\
&\overset{Th1}{=} f(x, \overset{n-s-1}{a}, \bar{a}, \overset{s-1}{a}, f(\bar{a}, \overset{n}{a})) \overset{(3)}{=} f(x, \overset{n-s-1}{a}, \bar{a}, \overset{s}{a}) \overset{(3)}{=} x.
\end{aligned}$$

Hence $\lambda_{0,a}\lambda_{0,a}^{-1} = \lambda_{0,a}^{-1}\lambda_{0,a} = \varepsilon$, where ε is the identity mapping. Thus, the transformation $\lambda_{0,a}^{-1}$, determined by the equality (5), is inverse to the shift $\lambda_{0,a}$. Analogously one can prove the other equalities from (5).

$$\begin{aligned}
\lambda_{n,a}^{-1}\lambda_{n,a}(x) &\overset{(5)}{=} f(\bar{a}, \overset{s-1}{a}, \bar{a}, \overset{n-s-1}{a}, \lambda_{n,a}(x)) \overset{(1)}{=} f(\bar{a}, \overset{s-1}{a}, \bar{a}, \overset{n-s-1}{a}, f(\overset{n}{a}, x)) \\
&\overset{Th1}{=} f(\bar{a}, \overset{s-1}{a}, f(\bar{a}, \overset{n}{a}), \overset{n-s-1}{a}, x) \overset{(3)}{=} f(\bar{a}, \overset{n-1}{a}, x) \overset{(3)}{=} x\,,
\end{aligned}$$

$$\begin{aligned}
\lambda_{n,a}\lambda_{n,a}^{-1}(x) &\overset{(5)}{=} \lambda_{n,a} f(\bar{a}, \overset{s-1}{a}, \bar{a}, \overset{n-s-1}{a}, x) \overset{(1)}{=} f(\overset{n}{a}, f(\bar{a}, \overset{s-1}{a}, \bar{a}, \overset{n-s-1}{a}, x)) \\
&\overset{Th1}{=} f(f(\overset{n}{a}, \bar{a}), \overset{s-1}{a}, \bar{a}, \overset{n-s-1}{a}, x) \overset{(3)}{=} f(\overset{s}{a}, \bar{a}, \overset{n-s-1}{a}, x) \overset{(3)}{=} x.
\end{aligned}$$

Let number $i \leqslant n-3$ be a multiple of r. Then

$$\begin{aligned}
\lambda_{i,a}\lambda_{i,a}^{-1}(x) &\overset{(5)}{=} f(\overset{i}{a}, f(\overset{n-s-i}{a}, \bar{a}, \overset{s-1}{a}, x, \overset{i-1}{a}, \bar{a}), \overset{n-i}{a}) \\
&\overset{(3)}{=} f(\overset{i}{a}, f(\overset{n-s-i}{a}, \bar{a}, \overset{s-1}{a}, x, \overset{i-1}{a}, \bar{a}), \overset{n-i-1}{a}, f(\overset{n}{a}, \bar{a})) \\
&\overset{Th1}{=} f(f(\overset{n-s}{a}, \bar{a}, \overset{s-1}{a}, x), \overset{i-1}{a}, f(\bar{a}, \overset{n}{a}), \overset{n-i-1}{a}, \bar{a}) = \\
&\overset{(3)}{=} f(f(\overset{n-s}{a}, \bar{a}, \overset{s-1}{a}, x), \overset{n-1}{a}, \bar{a}) \overset{(3)}{=} f(x, \overset{n-1}{a}, \bar{a}) \overset{(3)}{=} x.
\end{aligned}$$

If $i = n-s$, then the equality (5) defines the transformation

$$\lambda_{n-s,a}^{-1}(x) = f(\bar{a}, \overset{s-1}{a}, x, \overset{n-s-1}{a}, \bar{a})\,,$$

which implies

$$\begin{aligned}
\lambda_{n-s,a}^{-1}\lambda_{n-s,a}(x) &\overset{(1)}{=} f(\bar{a}, \overset{s-1}{a}, f(\overset{n-s}{a}, x, \overset{s}{a}), \overset{n-s-1}{a}, \bar{a}) \\
&\overset{Th1}{=} f(f(\bar{a}, \overset{n-1}{a}, x), \overset{n-1}{a}, \bar{a}) \overset{(3)}{=} f(x, \overset{n-1}{a}, \bar{a}) \overset{(3)}{=} x.
\end{aligned}$$

If $i < n-s$, then

$$\begin{aligned}
\lambda_{i,a}^{-1}\lambda_{i,a}(x) &\overset{(5)}{=} f(\overset{n-s-i}{a}, \bar{a}, \overset{s-1}{a}, f(\overset{i}{a}, x, \overset{n-i}{a}), \overset{i-1}{a}, \bar{a}) \\
&\overset{(3)}{=} f(f(\bar{a}, \overset{n}{a}), \overset{n-s-i-1}{a}, \bar{a}, \overset{s-1}{a}, f(\overset{i}{a}, x, \overset{n-i}{a}), \overset{i-1}{a}, \bar{a}) \\
&\overset{Th1}{=} f(f(\bar{a}, \overset{n-i-1}{a}, f(\overset{n-s}{a}, \bar{a}, \overset{s}{a}), \overset{i-1}{a}, x), \overset{n-1}{a}, \bar{a}) \overset{(3)}{=} x.
\end{aligned}$$

If $i \geqslant s$, then

$$\begin{aligned}\lambda_{i,a}\lambda_{i,a}^{-1}(x) &\overset{(5)}{=} f(\overset{i}{a}, f(\bar{a}, \overset{n-i-1}{a}, x, \overset{s-1}{a}, \bar{a}, \overset{i-s}{a}), \overset{n-i}{a})\\ &\overset{(3)}{=} f(f(\bar{a}, \overset{n}{a}), \overset{i-1}{a}, f(\bar{a}, \overset{n-i-1}{a}, x, \overset{s-1}{a}, \bar{a}, \overset{i-s}{a}), \overset{n-i}{a})\\ &\overset{Th1}{=} f(f(\bar{a}, \overset{i-1}{a}, f(\overset{n}{a}, \bar{a}), \overset{n-i-1}{a}, x), \overset{s-1}{a}, \bar{a}, \overset{n-s}{a}) \overset{(3)}{=} x.\end{aligned}$$

To prove $\lambda_{i,a}^{-1}\lambda_{i,a}(x) = \varepsilon$, we consider two cases: $i = s$ and $i > s$. If $i = s$, then (5) can be rewritten as $\lambda_{s,a}^{-1}(x) = f(\bar{a}, \overset{n-s-1}{a}, x, \overset{s-1}{a}, \bar{a})$. Therefore we get

$$\begin{aligned}\lambda_{s,a}^{-1}\lambda_{s,a}(x) &\overset{(1)}{=} f(\bar{a}, \overset{n-s-1}{a}, f(\overset{s}{a}, x, \overset{n-s}{a}), \overset{s-1}{a}, \bar{a})\\ &\overset{Th1}{=} f(f(\bar{a}, \overset{n-1}{a}, x), \overset{n-1}{a}, \bar{a}) \overset{(3)}{=} f(x, \overset{n-1}{a}, \bar{a}) \overset{(3)}{=} x.\end{aligned}$$

If $i > s$, then

$$\begin{aligned}\lambda_{i,a}^{-1}\lambda_{i,a}(x) &\overset{(5)}{=} f(\bar{a}, \overset{n-i-1}{a}, f(\overset{i}{a}, x, \overset{n-i}{a}), \overset{s-1}{a}, \bar{a}, \overset{i-s}{a})\\ &\overset{(3)}{=} f(\bar{a}, \overset{n-i-1}{a}, f(\overset{i}{a}, x, \overset{n-i}{a}), \overset{s-1}{a}, \bar{a}, \overset{i-s-1}{a}, f(\overset{n}{a}, \bar{a}))\\ &\overset{Th1}{=} f(f(\bar{a}, \overset{n-1}{a}, x), \overset{n-i-1}{a}, f(\overset{s}{a}, \bar{a}, \overset{n-s}{a}), \overset{i-1}{a}, \bar{a}) \overset{(3)}{=} x.\end{aligned}$$

The lemma and the theorem has been proved. □

Since for $r = s = 1$ we obtain an $(n+1)$-ary semigroup, then the following corollary is true.

Corollary 1. *An element $a \in Q$ is invertible in an $(n+1)$-ary semigroup $(Q; f)$ iff there exists an element $\bar{a} \in Q$ such that* (4) *holds for all $x \in Q$.*

3. Monoids and invertible elements

In the associate of the type (r, s, n) the structure of its operation is determined by Theorem 4 from [2] as soon as there exists at least one r-multiple invertible element in it. In particular, this theorem implies (see Corollary 11 in [2]) that the study of the groupoid reduces to the study of an associate of the type $(1, s, n)$ with invertible elements, that is why we will consider the last ones only. Since, as it was shown above, a binary semigroup with an invertible element is exactly a monoid, so we will use this characteristic to introduce its generalization and we will call it *invert* (a multiary monoid was called a semigroup with an identity element).

Since every invertible element of an invert determines some decomposition monoid, natural questions on the relations between the algebraic notions for a monoid and decomposition monoids as well as about relations between different decompositions of the same monoid arise. Here we will consider this relation between the sets of invertible elements.

Definition 2. An associate of the type $(1, s, n)$ containing at least one invertible element will be called an *invert of the type* (s, n).

When $s = 1$, then an invert is an $(n+1)$-ary semigroup containing at least one invertible element. So, every $(n + 1)$-ary monoid is an invert.

If an invert has at least one neutral element e, then, as follows from the results given below, the automorphism of its e-decomposition is identical, therefore its associativity period is equal to one, that is, such invert is a monoid. Every $(n + 1)$-ary group is an invert, since every its element is invertible.

The next statement, which follows from Theorem 4 in [2], gives a decomposition of the operation of an invert.

Theorem 6. *Let* $(Q; f)$ *be an* $(n + 1)$*-ary invert of the associativity period* s*. Then for every its invertible element* 0 *there exists a unique triple of operations* $(+, \varphi, a)$ *such, that* $(Q; +)$ *is a semigroup with a neutral element* 0*, an automorphism* φ *and an invertible element* a*, which satisfies the following relations:*

$$\varphi^n(x) + a = a + x, \quad \varphi^s(a) = a, \tag{6}$$

$$f(x_0, x_1, \dots, x_n) = x_0 + \varphi(x_1) + \varphi^2(x_2) + \dots + \varphi^n(x_n) + a. \tag{7}$$

And conversely, if an endomorphism φ *and an element* a *of an semigroup* $(Q; +)$ *are connected by the relations* (6)*, then the groupoid*

$(G;f)$ determined by the equality (7) *is an $(n+1)$-ary associate of the associativity degree s.*

We will use the following terminology: $(Q;+)$ is called a *monoid of the* 0*-decomposition*; φ is said to be an *automorphism of the* 0*-decomposition*; a is called a *free member of the* 0*-decomposition*; $+$, φ, a are called *components of the* 0*-decomposition*; and $(Q;+,\varphi,a)$ is said to be an *algebra of the* 0*-decomposition* of the invert $(Q;f)$.

Lemma 7. *Let k be a nonnegative integer, which is not greater than n and is a multiple of s, 0 is an arbitrary invertible element of the invert $(Q;f)$, then the components of its* 0*-decomposition are uniquely determined by the following equalities*

$$\begin{aligned} &x+y=f(x,\overset{k-1}{0},\bar{0},\overset{n-k-1}{0},y);\\ &a=f(0,0,\dots,0); \quad -a=\bar{0};\\ &\varphi^i(x)=\lambda_{0,0}^{-1}\lambda_{i,0}(x)=f(\overset{i}{0},x,\overset{n-i-1}{0},\bar{0});\\ &\varphi^{-i}(x)=\lambda_{n,0}^{-1}\lambda_{n-i,0}(x)=f(\bar{0},\overset{n-i-1}{0},x,\overset{i}{0}) \end{aligned} \tag{8}$$

for all $i=1,\dots,n-1$.

Proof. In [2] the first three of the equalities were proved. Since n divides s, then (6) implies $\varphi^n(a)=a$, therefore

$$\varphi^n(\bar{0})=\varphi^n(-a)=-\varphi^n(a)=-a=\bar{0}.$$

The transformation φ is an automorphism of the semigroup $(Q;f)$, therefore $\varphi(0)=0$ and

$$\begin{aligned}\varphi^i(x)=\varphi^i(x)-a+a=0+\varphi(0)+\dots+\varphi^{i-1}(0)+\varphi^i(x)+\\ +\varphi^{i+1}(0)+\dots+\varphi^{n-1}(0)+\varphi^n(\bar{0})+a\overset{(6)}{=}f(\overset{i}{0},x,\overset{n-i-1}{0},\bar{0}).\end{aligned}$$

Let us now make use of the relationships (5):

$$\begin{aligned}\lambda_{0,0}^{-1}\lambda_{i,0}(x)&\overset{(5)}{=}f(f(\overset{i}{0},x,\overset{n-i}{0}),\overset{n-s-1}{0},\bar{0},\overset{s-1}{0},\bar{0})\\ &\overset{Th1}{=}f(\overset{i}{0},x,\overset{n-i-1}{0},f(\overset{n-s}{0},\bar{0},\overset{s-1}{0},\bar{0}))\overset{(3)}{=}f(\overset{i}{0},x,\overset{n-i-1}{0},\bar{0})\overset{(7)}{=}\varphi^i(x).\end{aligned}$$

$$\begin{aligned}
\lambda_{n,0}^{-1}\lambda_{n-i,0}(x) &\overset{(5)}{=} f(\bar{0}, \overset{s-1}{0}, \bar{0}, \overset{n-s-1}{0}, f(\overset{n-i}{0}, x, \overset{i}{0})) = \\
&\overset{Th1}{=} f(f(\bar{0}, \overset{s-1}{0}, \bar{0}, \overset{n-s}{0}), \overset{n-i-1}{0}, x, \overset{i}{0}) \overset{(3)}{=} f(\bar{0}, \overset{n-i-1}{0}, x, \overset{i}{0}) \\
&\overset{(7)}{=} \bar{0} + \varphi(0) + \cdots + \varphi^{n-i}(x) + \varphi^{n-i+1}(0) + \cdots + \varphi^{n}(0) + a \\
&\overset{(6)}{=} -a + \varphi^{n}(\varphi^{-i}(x)) + a \overset{(6)}{=} \varphi^{-i}(x).
\end{aligned}$$

The lemma is proved. □

Corollary 2. *Under the notations of Theorem 6 the associativity period of the invert is equal to the least of the numbers s, such that $\varphi^s(a) = a$, i.e. it is equal to the length of the orbit of the element a, when we consider the action of the cyclic group $\langle\varphi\rangle$ generated by the automorphism φ.*

If an element x is invertible in an a-decomposition monoid, then its inverse element will be denoted by $-x_{\langle a\rangle}$ or by $x_{\langle a\rangle}^{-1}$ depending on additive or multiplicative notation of the a-decomposition monoid. It should be noted that the element $-x_{\langle a\rangle}$ is uniquely determined by the elements a and x.

Theorem 8. *An element of an invert will be invertible iff it is invertible in one (hence, in every) of the decomposition monoids.*

Proof. Let $(Q; f)$ be an invert of the type (s, n) with an invertible element 0 and $(Q; +)$ be a 0-decomposition monoid. Let x be invertible in $(Q; f)$ and let

$$-x_{\langle 0\rangle} := f(0, \overset{n-s-1}{x}, \bar{x}, \overset{s-1}{x}, 0). \tag{9}$$

To prove that the element $-x_{\langle 0\rangle}$ is inverse to x, we will use the equality (8) when $k = s$.

$$\begin{aligned}
x + (-x_{\langle 0\rangle}) &\overset{(8)}{=} f(x, \overset{s-1}{0}, \bar{0}, \overset{n-s-1}{0}, -x_{\langle 0\rangle}) \\
&\overset{(9)}{=} f(x, \overset{s-1}{0}, \bar{0}, \overset{n-s-1}{0}, f(0, \overset{n-s-1}{x}, \bar{x}, \overset{s-1}{x}, 0)) \\
&\overset{Th1}{=} f(f(x, \overset{s-1}{0}, \bar{0}, \overset{n-s}{0}), \overset{n-s-1}{x}, \bar{x}, \overset{s-1}{x}, 0) \overset{(3)}{=} f(\overset{n-s}{x}, \bar{x}, \overset{s-1}{x}, 0) \overset{(3)}{=} 0.
\end{aligned}$$

$$\begin{aligned} -x_{\langle 0\rangle} + x &\overset{(8)}{=} f(-x_{\langle 0\rangle}, \overset{s-1}{0}, \bar{0}, \overset{n-s-1}{0}, x) \\ &\overset{(9)}{=} f(f(0, \overset{n-s-1}{x}, \bar{x}, \overset{s-1}{x}, 0), \overset{s-1}{0}, \bar{0}, \overset{n-s-1}{0}, x) \\ &\overset{Th1}{=} f(0, \overset{n-s-1}{x}, \bar{x}, \overset{s-1}{x}, f(\overset{s}{0}, \bar{0}, \overset{n-s-1}{0}, x)) \overset{(3)}{=} f(0, \overset{n-s-1}{x}, \bar{x}, \overset{s}{x}) \overset{(3)}{=} 0. \end{aligned}$$

Hence, the element $-x_{\langle 0\rangle}$ is inverse to x in $(Q;+)$.

Conversely, let the element x be invertible in the 0-decomposition monoid $(Q;+)$. Then the element

$$f(0, x, \ldots, x, 0) \overset{(7)}{=} \varphi x + \varphi^2 x + \cdots + \varphi^{n-1} x + a$$

is invertible in $(Q;+)$ too. Let us define the element $\bar{x}$ by

$$\bar{x} = -f(0, x, \ldots x, 0)_{\langle 0\rangle}. \tag{10}$$

In particular, this means that

$$\bar{x} + f(0, x, \ldots x, 0)_{\langle 0\rangle} = 0.$$

Then for any element y of Q we get the following relations:

$$\begin{aligned} y &= 0 + y = \bar{x} + f(0, \overset{n-1}{x}, 0) + y \\ &\overset{(8)}{=} f(f(\bar{x}, \overset{s-1}{0}, \bar{0}, \overset{n-s-1}{0}, f(0, \overset{n-1}{x}, 0)), \overset{s-1}{0}, \bar{0}, \overset{n-s-1}{0}, y) \\ &\overset{Th1}{=} f(f(\bar{x}, \overset{s-1}{0}, \bar{0}, \overset{n-s}{0}), \overset{n-1}{x}, f(\overset{s}{0}, \bar{0}, \overset{n-s-1}{0}, y)) \overset{(3)}{=} f(\bar{x}, \overset{n-1}{x}, y)\,, \end{aligned}$$

$$\begin{aligned} y &= y + 0 \overset{(10)}{=} y + f(0, \overset{n-1}{x}, 0) + \bar{x} \\ &\overset{(8)}{=} f\Big(f(y, \overset{s-1}{0}, \bar{0}, \overset{n-s-1}{0}, f(0, \overset{n-2}{x}, 0)), \overset{s-1}{0}, \bar{0}, \overset{n-s-1}{0}, \bar{x}\Big) \\ &\overset{Th1}{=} f\Big(f(y, \overset{s-1}{0}, \bar{0}, \overset{n-s-1}{0}), \overset{n-2}{x}, f(\overset{s}{0}, \bar{0}, \overset{n-s-1}{0}, \bar{x})\Big) \overset{(3)}{=} f(y, \overset{n-2}{x}, \bar{x}). \end{aligned}$$

From Theorem 4 we get the invertibility of the element x in the invert $(Q;f)$. □

Corollary 3. *The sets of all invertible elements of multiary monoid and decomposition monoids are pairwise equal.*

Corollary 4. *Let* 0 *be an invertible element of a monoid* $(Q;f)$ *of the type* (s,n) *and let* k *be multiple of* s*. Then the element* x *will be invertible in* $(Q;f)$ *iff there exists an element* $-x_{\langle 0\rangle}$ *such that*

$$f(x,\overset{s-1}{0},\bar{0},\overset{n-s-1}{0},-x_{\langle 0\rangle})=f(-x_{\langle 0\rangle},\overset{s-1}{0},\bar{0},\overset{n-s-1}{0},x)=0 \tag{11}$$

hold.

Proof. The equality (11) according to the equalities (8) means the truth of the relations $x+(-x_{\langle 0\rangle})=-x_{\langle 0\rangle}+x=0$, where $(Q;+)$ is the 0-decomposition monoid, that is the element x is invertible in $(Q;+)$. Hence, by Theorem 8 it will be invertible in the associate $(Q;f)$. □

Lemma 9. *Let* $(Q;f)$ *be an invert of the type* (s,n)*,* $(+,\varphi,a)$ *be its* 0*-decomposition. A triple* $(\cdot,\psi,b)$ *of operations defined on* Q *will be a decomposition of* $(Q;f)$ *iff there exists an invertible in* $(Q;+)$ *element* e *satisfying the conditions*

$$\begin{aligned} &x\cdot y=x-e+y,\quad \psi(x)=e+\varphi(x)-\varphi(e),\\ &b=e+\varphi(e)+\varphi^2(e)+\cdots+\varphi^n(e)+a. \end{aligned} \tag{12}$$

The algebra $(Q;\cdot,\psi,b)$ *in this case will be* e*-decomposition of the invert* $(Q;f)$*.*

Proof. Let $(\cdot,\psi,b)$ be e-decomposition of the invert $(Q;f)$, then

$$\begin{aligned} x\cdot y &\overset{(8)}{=} f(x,\overset{s-1}{e},\bar{e},\overset{n-s-1}{e},y)\overset{(7)}{=}x+\varphi e+\cdots+\varphi^{s-1}(e)+\\ &\quad+\varphi^s(\bar{e})+\varphi^{s+1}(e)+\cdots+\varphi^{n-1}(e)+\varphi^n(y)+a\\ &\overset{(6)}{=}x+(\varphi(e)+\cdots+\varphi^{s-1}(e)+\varphi^3(\bar{e})+\\ &\quad+\varphi^{s+1}(e)+\cdots+\varphi^{n-1}(e)+a)+y\,. \end{aligned}$$

Hence $x\cdot y=x+c+y$ for some $c\in Q$ and all $x,y\in Q$. In particular, when $x=e,y=0$ and $x=0,y=e$ we get the invertibility of the element c in $(Q;+)$, and the relation $c=-e$. Next,

$$\begin{aligned} \psi(x)\overset{(8)}{=}f(e,x,\overset{n-2}{e},\bar{e})\overset{(7)}{=}e+\varphi(x)+\varphi^2(e)+\cdots+\\ +\varphi^{n-1}(e)+\varphi^n(\bar{e})+a=e+\varphi(x)+d \end{aligned}$$

for some $d \in Q$. But $e = \psi(e) = e + \varphi(e) + d$, therefore $d = -\varphi(e)$.

On the other hand, let an element e be invertible in $(Q;+)$ and determine a triple of operations $(\cdot, \psi, b)$ on Q by the equalities (12). The invertibility of the element e in the invert $(Q;f)$ is ensured by Theorem 8. If the component of the e-decomposition of the invert $(Q;f)$ are denoted by $(\circ, \chi, c)$, then just proved assertion gives

$$x \circ y = x - e + y, \quad \chi(x) = e + \varphi(x) - \varphi(e),$$
$$c = e + \varphi(e) + \varphi^2(e) + \cdots + \varphi^n(e) + a\,.$$

Therefore $(\cdot, \psi, b) = (\circ, \chi, c)$. This means, that $(\cdot, \psi, b)$ will be a decomposition of $(Q;f)$. $\square$

We say that the monoids $(Q;\cdot)$ and $(Q;+)$ *differ from each other by a unit*, if the equality $x \cdot y = x - e + y$ holds for some invertible in $(Q;+)$ element e, because they coincide once their units coincide. This relationship between monoids is stronger than isomorphism since the translations L_e^{-1} and R_e^{-1} are isomorphic mappings from one to the other. Therefore the following statement is obvious.

Corollary 5. *Any two decomposition monoids of the same invert differ from each other by a unit.*

Theorem 10. *The set of all invertible elements of an invert is its subquasigroup and coincides with the group of all invertible elements of any of its decomposition monoids.*

Proof. Let $(Q;f)$ be an invert of the type (s,n) and let $(+,\varphi,a)$ be its 0-decomposition. Theorem 8 implies that the sets of all invertible elements of groupoids $(Q;f)$ and $(Q;+)$ coincide. Denote this set by G. Inasmuch as G is a subgroup of the monoid $(Q;+)$ and $\varphi G = G$, $a \in G$, so for any elements $c_0, c_1, \ldots, c_n \in G$ the element

$$f(c_0, c_1, \ldots, c_n) \overset{(7)}{=} c_0 + \varphi(c_1) + \varphi^2(c_2) + \cdots + \varphi^n(c_n) + a$$

is in G also. Furthermore for any number $i = 0, 1, \ldots, n$ the solution of $f(c_0, \ldots, c_{i-1}, x, c_{i+1}, \ldots, c_n) = c$, where $c \in G$, is unique and coincides with the element

$$x \overset{(6)}{=} \varphi^{-i}\Big(- \varphi^{i-1}(c_{i-1}) - \cdots \quad -\varphi(c_1) - c_0 + c - a - \\ -\varphi^{n}(c_n) - \cdots - \varphi^{i+1}(c_{i+1})\Big). \tag{13}$$

which is in G too. Hence, $(G; f)$ is a subquasigroup of $(Q; f)$. □

Theorem 11. *The period of associativity of the invert determined by (θ, a) coincides with the number of different skew elements of an invertible element and with the length of the orbit $< \theta > (a)$, where $< \theta >$ is the automorphism group generated by θ.*

Proof. Let number s be the period of associativity of the $(n+1)$-ary invert $(Q; f)$ and let x be any of its invertible elements. Denote by $(*, \psi, b)$ the x-decomposition of the invert $(Q; f)$. Since

$$f(\overset{i}{x}, \psi^{n-i}(\bar{x}), \overset{n-i}{x}) \overset{(8)}{=} f(\overset{i}{x}, f(\overset{n-i}{x}, \bar{x}, \overset{i-1}{x}, \bar{x}), \overset{n-i-1}{x}, f(\overset{n}{x}, \bar{x})) \\ \overset{Th1}{=} f(f(\overset{n}{x}, \bar{x}), \overset{i-1}{x}, f(\bar{x}, \overset{n}{x}), \overset{n-i-1}{x}, \bar{x}) \overset{(3)}{=} f(\overset{n}{x}, \bar{x}) = x,$$

then the i-th skew $\bar{x}^i$ of the element x is determined by the equality

$$\bar{x}^i = \psi^{n-i}(\bar{x}) \overset{(8)}{=} f(\overset{n-i}{x}, \bar{x}, \overset{i-1}{x}, \bar{x}), \quad i = 0, 1, \ldots, n. \tag{14}$$

Inasmuch as, in accordance with the equality (8),

$$\psi^s(\bar{x}) = \psi^s(b^{-1}) = (\psi^s(b))^{-1} = b^{-1} = \bar{x},$$

there are at most s different skew elements of the element x: Namely $\bar{x}$, $\bar{x}^1$, $\ldots$, $\bar{x}^{s-1}$.

Suppose, for some numbers i, j with $i < j < s$, the i-th and j-th skew elements of x coincide. The results obtained imply the equality $\psi^{n-i}(\bar{x}) = \psi^{n-j}(\bar{x})$, so that $\psi^{j-i}(\bar{x}) = \bar{x}$. The last equality together with equality $\psi^s(\bar{x}) = \bar{x}$ give the relation $\psi^d(\bar{x}) = \bar{x}$, where $d =$ g.c.d.$(s, j-i)$. In view of (8) this implies $\psi^d(b) = b$. It follows from Theorem 6 that the pair (d, n) will be a type of the invert $(Q; f)$. At the same time $d < s$. A contradiction to the definition of the associativity period.

Thus, the element x has exactly s skew elements. They are determined by the relation (14) and by any full collection of pairwise noncongruent indices modulo s.

Corollary 6. *If one of skew elements of an invertible element x of a monoid coincides with x, then all skew elements of x are equal and this invert is a semigroup.*

Proof. Let $\bar{0}^i = 0$. The relation (14) implies $\varphi^{n-i}(\bar{0}) = 0$, where φ denotes an automorphism of the 0-decomposition. Apply to the last equality φ^i we obtain $\varphi^n(\bar{0}) = \varphi^i(0)$.

Since $\varphi^n(\bar{0}) = \varphi^n(-a) = -\varphi^n(a) = -a = \bar{0}$, then accounting to (8) we obtain $f(\overset{i}{0}, 0, \overset{n-i-1}{0}, \bar{0}) = \bar{0}$, that is $\bar{0} = 0$. Thus $a = f(0, \dots, 0) = 0$ and $\varphi(a) = \varphi(0) = 0 = a$. Hence, by Theorem 11 the associativity period of the invert is equal to 1, i.e. the invert is a semigroup. □

Corollary 7. *An invert of associativity period s has at least $s + 1$ different invertible elements.*

Corollary 8. *An invert having at most two invertible elements is associative i.e. is a semigroup.*

Proof. If an invert has exactly one invertible element, then it will be associative by Corollary 6, since its skews coincide with it. If the invert has exactly two invertible elements a and b, then $\bar{a}^0 = a$ or $\bar{a}^0 = b$. If $\bar{a}^0 = a$, then according to Corollary 6 the invert is a semigroup. If $\bar{a}^0 = b$, then Theorem 11 implies $\bar{a}^1 = a$. And Theorem 11 implies that the invert is a quasigroup. □

Axiomatics of polyagroups

Both for binary and for n-ary cases an associative quasigroup is called a *group*. Therefore, retaining this regularity we will introduce the notion of a polyagroup.

Definition 3. When $s < n$ the s-associative $(n+1)$-ary quasigroup we will call a *nonsingular polyagroup of the type* (s, n).

It is easy to see, that $s = 1$ means the polyagroup is an $(n+1)$-ary group. Theorem 6 implies an analogue of Gluskin-Hosszú theorem.

Proposition 12. *Any polyagroup of the type* (s, n) *is* (i, j)*-associative for all* i, j *with* $i \equiv j \pmod{s}$*. When* s *is its associativity period, then no other* (i, j)*-associativity identity holds.*

Theorem 13. *Let* $(Q; f)$ *be an associate of the type* (s, n) *and* $s < n$, $n > 1$*. Then the following statements are equivalent*

1) $(Q; f)$ *is a polyagroup,*
2) *every element of the associate is invertible,*
3) *for every* $x \in Q$ *there exists* $\bar{x} \in Q$ *such that*

$$f(\bar{x}, x, \ldots, x, y) = f(y, x, \ldots, x, \bar{x}) = y \tag{15}$$

holds for all $y \in Q$,

4) $(Q; f)$ *has an invertible element* 0 *and for every* $x \in Q$ *there exists* $y \in Q$ *such that*

$$f(x, \overset{s-1}{0}, \bar{0}, \overset{n-s-1}{0}, y) = 0, \quad f(y, \overset{s-1}{0}, \bar{0}, \overset{n-s-1}{0}, x) = 0 \tag{16}$$

holds.

Proof. 1)⇔2) follows from Theorem 10; 2)⇔3) from Corollary 1; 2)⇔4) from Corollary 4. □

When $s = 1$ we get a criterion for n-ary groups.

Corollary 9. *Let* $(Q; f)$ *be* $(n+1)$*-ary a semigroup. Then the following statements are equivalent*

1) $(Q; f)$ *is an* $(n+1)$*-ary group,*
2) *every element of the semigroup is invertible,*
3) *for every* $x \in Q$ *there exists* $\bar{x} \in Q$ *such that* (15) *holds for every* $y \in Q$,
4) $(Q; f)$ *has an invertible element* 0 *and for every* $x \in Q$ *there exists* $y \in Q$ *such that* (16) *hold.*

References

[1] **V. D. Belousov**: *n-Ary quasigroups*, (Russian) Chişinău, Ştiinţa 1972.

[2] **F. N. Sokhatsky**: *About associativity of multiary operations*, (Russian) Diskretnaya matematika **4** (1992), 66 − 84.

[3] **F. Sokhatsky**: *On superassociative group isotopes*, Quasigroups and Related Systems **2** (1995), 101 − 119.

[4] **F. M. Sokhatsky**: *On associativity of multiplace operations*, Quasigroups and Related Systems **4** (1997), 51 − 66.

Received May 24, 1998 and in revised form October 11, 1998

Vinnytsia State Pedagogical University
Vinnytsia 287100
Ukraine

Quasigroups and Related Systems **5** (1998), 69 – 80

Symmetric n-loops with the inverse property

Leonid A. Ursu

Abstract

It is proved that the matrix $\|I_{ij}\|$, where the substitutions I_{ij} are defined by the equalities $\big(\overset{i-1}{e}, x, \overset{j-i-1}{e}, I_{ij}x, \overset{n-j}{e}\big) = e$ is one of the inversion matrices of the symmetric n-IP-loop with an unique unit e. From this result it follows that the matrix $\|I_{ij}\|$ is a unique inversion matrix of such loops of an odd arity.

A quasigroup $Q(A)$ of arity n is said to be an IP-*quasigroup* [1] if there exist substitutions ν_{ij}, $i,j = \overline{1,n}$, on Q with $\nu_{ii} = \varepsilon$ (ε is the identical substitition) such that the equalities (the identities with parameters)

$$A(\{\nu_{ij}x_j\}_{j=1}^{i-1}, A(x_1^n), \{\nu_{ij}x_j\}_{j=i+1}^{n}) = x_i \tag{1}$$

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

The substitutions ν_{ij} are called *inversion substitutions* and the matrix $\|\nu_{ij}\|$ is called an *inversion matrix*, $i \in \overline{1,n}$, $j \in \overline{1,n+1}$, where $\nu_{i,n+1} = \varepsilon$ for all i. The rows of this matrix are called *inversion systems* (*rows*) of an n-IP-quasigroup.

A quasigroup $Q(A)$ of an arity n is said to be an IP-quasigroup if the following equalities

$$A^{\pi_i} = A^{T_i} \tag{2}$$

hold for all $i \in \overline{1,n}$, where π_i is the transposition $(i, n+1)$, A^{π_i} is the i-th inverse operation for A and

$$T_i = (\{\nu_{ij}\}_{j=1}^{i-1}, \varepsilon, \{\nu_{ij}\}_{j=i+1}^{n}, \varepsilon).$$

1991 Mathematics Subject Classification: 20N15
Keywords: n-ary quasigroup, IP-loop, autotopy

If an n-IP-quasigroup $Q(A)$ has a unit e, then it is called an n-*IP*-*loop*.

In [1] the substitutions I_{ij} are defined by the equalities

$$A\left(\overset{i-1}{e}, x, \overset{j-i-1}{e}, I_{ij}x, \overset{n-j}{e}\right) = e \qquad (3)$$

in an n-loop $Q(A)$ with a unit e for any $x \in Q$, $i, j \in \overline{1, n}$, with $I_{ii} = I_{i,n+1} = \varepsilon$. From (3) it follows that $I_{ij}^{-1} = I_{ji}$ and $I_{ij}e = e$.

The following equality (cf. [1])

$$I_{ij}x = L_i(\bar{e}_j)\nu_{ji}x \qquad (4)$$

shows a relation between I_{ij} and ν_{ij}, where

$$\bar{e}_j = \{\nu_{jk}e\}_{k=1}^{n},\ \ \nu_{jj}e = e,$$
$$L_i(\bar{e}_j)x = A(\nu_{j1}e, \nu_{j2}e, \dots, \nu_{j,i-1}e, x, \nu_{j,i+1}e, \dots, \nu_{jn}e).$$

It is evident that $L_i(\bar{e}_j)$ is a substitution on Q. From (4) we get the following equality for the corresponding matrices

$$\|I_{ij}\| = \|L_i(\bar{e}_j)\| \cdot \|\nu_{ji}\|. \qquad (5)$$

An $(n+1)$-tuple $T = (\alpha_1^{n+1})$ of substitutions on Q is called an *autotopy* for an n-quasigroup $Q(A)$ if $A^T = A$.

A quasigroup $Q(A)$ of arity n is said to be *symmetric* (cf. [2]) if

$$A(x_{\alpha 1}^{\alpha n}) = A(x_1^n)$$

for all $x_1^n \in Q^n$ and any $\alpha \in S_n$ where S_n is the symmetric qroup of degree n.

It is known that an n-IP-quasigroup $(n > 2)$ can have more than one inversion matrix [1]. In [2] some examples of nonsymmetric n-IP-loops with the inversion matrix $\|I_{ij}\|$ are constructed.

Related to this V.D. Belousov has asced the following questions.

Is the matrix $\|I_{ij}\|$ always one of the inversion matrices of an n-IP-loop ?

Does an n-IP-loop exist such that the matrix $\|I_{ij}\|$ is a unique inversion matrix ?

In this article some properties of the symmetric n-IP-loops are established and answers are given to the V.D. Belousov's questions for such loops.

Let $Q(A)$ be a symmetric n-IP-quasigroup with an inversion matrix $\|\nu_{ij}\|$. Then the following properties are true.

1. *A symmetric n-IP-quasigroup is defined by a unique identity.* Indeed, let the i-th inverse identity

$$A(\{\nu_{ik}x_k\}_{k=1}^{i-1}, A(x_1^n), \{\nu_{ik}x_k\}_{k=i+1}^{n}) = x_i$$

holds in an n-IP-quasigroup $Q(A)$. Then

$$A(\{\nu_{ik}x_k\}_{k=1}^{i-1}, A(x_1^n), \{\nu_{ik}x_k\}_{k=i+1}^{n}) =$$
$$A(\{\nu_{ik}x_k\}_{k=1}^{j-1}, A(x_1^{j-1}, x_i, x_{j+1}^n), \{\nu_{ik}x_k\}_{k=j+1}^{n}) = x_i.$$

Thus, the j-th inverse identity holds in $Q(A)$ for all $j = 1, 2, \dots, i-1, i+1, \dots n$. It means that if $(\{\nu_{ik}\}_{k=1}^{i-1}, \varepsilon, \{\nu_{ik}\}_{k=i+1}^{n}, \varepsilon)$ is the i-th row of the inversion matrix $\|\nu_{ij}\|$, then $(\{\nu_{ik}\}_{k=1}^{j-1}, \varepsilon, \{\nu_{ik}\}_{k=j+1}^{n}, \varepsilon)$ is the j-th row of this matrix, $i, j \in \overline{1,n}$, $i \neq j$.

Hence if one inversion row is known, then the inversion matrix is known.

2. *If $(\nu_{i1}, \nu_{i2}, \dots, \nu_{i,i-1}, \varepsilon, \nu_{i,i+1}, \dots, \nu_{in}, \varepsilon)$ is the i-th inversion row, $i \in \overline{1,n}$, of a symmetric n-IP-quasigroup, then any permutation of the substitutions ν_{ik}, $k = 1, 2, \dots, i-1, i+1, \dots, n$, of this row is the i-th inverse row of the quasigroup.*

In fact, from

$$A(\{\nu_{ik}x_k\}_{k=1}^{i-1}, A(x_1^n), \{\nu_{ik}x_k\}_{k=i+1}^{n}) = x_i$$

it follows that

$$A(\{\nu_{ik}x_k\}_{k=1}^{i-1}, \nu_{it}x_j, \{\nu_{ik}x_k\}_{k=j+1}^{i-1}, A(x_1^n), \{\nu_{ik}x_k\}_{k=i+1}^{t-1}, \nu_{ij}x_t, \{\nu_{ik}x_k\}_{t+1}^{n})$$
$$= A(\{\nu_{ik}x_k\}_{k=1}^{j-1}, \nu_{ij}x_t, \{\nu_{ik}x_k\}_{k=j+1}^{i-1}, A(x_1^{j-1}, x_t, x_{j+1}^{i-1}, x_i, x_{i+1}^{t-1}, x_j, x_{t+1}^n),$$
$$\{\nu_{ik}x_k\}_{k=i+1}^{t-1}, \nu_{it}x_j, \{\nu_{ik}x_k\}_{k=t+1}^{n}) = x_i$$

for any $i, j, t \in \overline{1,n}$, $j < i < t$.

Next, for the sake of simplicity we shall take the first inversion identity, i.e. the first inversion row, as definition of an n-IP-quasigroup. The corresponding inversion matrix we shall denote by $\|\nu_1\|$.

3. *If $T = (\alpha_1^n, \beta)$ is an autotopy of a symmetric n-IP-quasigroup $Q(A)$, then $\tilde{T} = (\alpha_{\sigma 1}^{\sigma n}, \beta)$ is an autotopy of $Q(A)$ also for any $\sigma \in S_n$.*

In other words, any permutation of the first n components of an autotopy of a symmetric n-IP-quasigroup is an autotopy of this quasigroup as well.

Indeed, the equality

$$A(\{\alpha_k x_k\}_{k=1}^{i-1}, \alpha_i x_i, \{\alpha_k x_k\}_{k=i+1}^{j-1}, \alpha_j x_j, \{\alpha_k x_k\}_{k=j+1}^{n}) = \beta A(x_1^n)$$

implies that

$$A(\{\alpha_k x_k\}_{k=1}^{i-1}, \alpha_j x_j, \{\alpha_k x_k\}_{k=i+1}^{j-1}, \alpha_i x_i, \{\alpha_k x_k\}_{k=j+1}^{n}) \\ = \beta A(x_1^{i-1}, x_j, x_{i+1}^{j-1}, x_i, x_{j+1}^n),$$

i.e. $T_{i,j} = (\alpha_1^{i-1}, \alpha_j, \alpha_{i+1}^{j-1}, \alpha_i, \alpha_{j+1}^n, \beta)$ is an autotopy of $Q(A)$ for any $i, j \in \overline{1,n}$, $i \neq j$.

4. *If $T = (\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n, \beta)$ is an autotopy of a symmetric n-IP-quasigroup $Q(A)$ with an inversion system $(\varepsilon, \nu_{12}, \ldots, \nu_{1n}, \varepsilon)$ (i.e. with an inverse matrix $\|\nu_1\|$), then*

$$(\beta,\ \nu_{12}\alpha_2\nu_{12},\ \nu_{13}\alpha_3\nu_{13}, \ldots, \nu_{1,i-1}\alpha_{i-1}\nu_{1,i-1}, \\ \nu_{1i}\alpha_1\nu_{1i}, \nu_{1,i+1}\alpha_{i+1}\nu_{1,i+1}, \ldots, \nu_{1n}\alpha_n\nu_{1n}, \alpha_i)$$

is an autotopy of this quasigroup for any $i \in \overline{1,n}$.

In fact, if $(\alpha_1, \alpha_2, \ldots, \alpha_i, \ldots, \alpha_n, \beta) \in \mathfrak{A}_A$, where $\mathfrak{A}_A$ is the autotopy group of $Q(A)$, then by property 3

$$(\alpha_i, \alpha_2, \alpha_3, \ldots, \alpha_{i-1}, \alpha_1, \alpha_{i+1}, \ldots, \alpha_n, \beta) \in \mathfrak{A}_A.$$

and by the property of autotopies of n-IP-quasigroups, proved in [1],

$$(\beta,\ \nu_{12}\alpha_2\nu_{12},\ \nu_{13}\alpha_3\nu_{13}, \ldots, \nu_{1,i-1}\alpha_{i-1}\nu_{1,i-1},\ \nu_{1i}\alpha_1\nu_{1i},$$

$$\nu_{1,i+1}\alpha_{i+1}\nu_{1,i+1}, \ldots, \nu_{1n}\alpha_n\nu_{1n}, \alpha_i) \in \mathfrak{A}_A.$$

As a corollary from this result, we get that if

$$T_1 = (\varepsilon, \nu_{12}, \nu_{13}, \ldots, \nu_{1n}, \varepsilon)$$

is an inversion system of a symmetric n-IP-quasigroup, then

$$T_1^2 = (\varepsilon, \nu_{12}^2, \nu_{13}^2, \ldots, \nu_{1n}^2, \varepsilon)$$

is its autotopy, since $T = \binom{n+1}{\varepsilon} \in \mathfrak{A}_A$.

5. *Let $Q(A)$ be a symmetric n-IP-loop with a unit e and with an inversion matrix $\|\nu_1\|$. Then $\nu_{1j}^2 = \varepsilon$ for any $j \in \overline{2,n}$.*

Indeed, from the equality

$$A(A(x_1^k), \{\nu_{1i}x_i\}_{i=2}^n) = x_1$$

by $x_1 = x_2 = \cdots = x_{j-1} = x_{j+1} = \cdots = x_n = e$ we get

$$A(x_j, \{\nu_{1i}e\}_{i=2}^{j-1}, \nu_{1j}x_j, \{\nu_{1i}e\}_{i=j+1}^n) = e.$$

Changing in this equality x_j for $\nu_{1j}e$ we get

$$A(\nu_{1j}e, \{\nu_{1i}e\}_{i=2}^{j-1},\ \nu_{1j}^2e, \{\nu_{1i}e\}_{i=j+1}^n) = e$$

or $A(\nu_{1j}^2e, \{\nu_{1i}e\}_{i=2}^n) = e$. Thus, $A^{\pi_1}(e, \{\nu_{1i}e\}_{i=2}^n) = \nu_{1j}^2e$ from which according to (2) and symmetry we have

$$A(e, \{\nu_{1i}^2e\}_{i=2}^n) = \nu_{1j}^2e.$$

But $T_1^2 \in \mathfrak{A}_A$ so $A(e, \{\nu_{1i}^2e\}_{i=2}^n) = A\binom{n}{e} = e$ and $\nu_{1j}^2e = e$ for all $j \in \overline{2,n}$.

Now from

$$A(x_1, \{\nu_{1i}^2x_i\}_{i=2}^n) = A(x_1^n)$$

by $x_1 = x_2 = \cdots = x_{j-1} = x_{j+1} = \cdots = x_n = e$, $x_j = x$, $j > 1$, one has $\nu_{1j}^2x = x$ for any $j \in \overline{2,n}$.

6. *If $(\varepsilon, \nu_{12}, \nu_{13}, \ldots, \nu_{1n}, \varepsilon)$ is an inversion system of a symmetric n-IP-loop with a unique unit, then*

$$\left(\overset{i-1}{\varepsilon}, \nu_{1i}\nu_{1j}, \overset{j-i-1}{\varepsilon}, \nu_{1j}\nu_{1i}, \overset{n-j+1}{\varepsilon}\right)$$

is an autotopy of this loop for any $i, j \in \overline{2, n}$.

This statement follows from properties 2 and 5 since the product (in the sense of component-wise multiplication) of two i-th inversion systems of an n-IP-quasigroup is an autotopy of this quasigroup [1].

In fact, let $(\varepsilon, \nu_{12}, \dots, \nu_{1i}, \dots, \nu_{1n}, \varepsilon)$ be an inversion system of a symmetric n-IP-loop. Then by property 2

$$(\varepsilon, \nu_{12}, \dots, \nu_{1,i-1}, \nu_{1j}, \nu_{1,i+1}, \dots, \nu_{1,j-1}, \nu_{1i}, \nu_{1,j+1}, \dots, \nu_{1n}, \varepsilon)$$

is an inversion system of this loop too, and their product (since $\nu_{1i}^2 = \varepsilon$)

$$\left(\overset{i-1}{\varepsilon}, \nu_{1i}\nu_{1j}, \overset{j-i-1}{e}, \nu_{1j}\nu_{1i}, \overset{n-j-1}{\varepsilon}\right)$$

is an autotopy of the loop for all $i, j \in \overline{2, n}$.

7. *In a symmetric* n-IP*-loop* $Q()$ *with an inversion matrix* $\|\nu_1\|$ *the following equalities are true*

$$\nu_{1i}(x_1^n) = (\nu_{1i}x_i, \nu_{12}x_2, \nu_{13}x_3, \dots, \nu_{1,i-1}x_{i-1}, \nu_{1i}x_i, \nu_{1,i+1}x_{i+1}, \dots, \nu_{1n}x_n)$$

for any $i \in \overline{2, n}$.

Indeed, from

$$((x_1^n), \nu_{12}x_2, \dots, \nu_{1,i-1}x_{i-1}, \nu_{1i}x_i, \nu_{1,i+1}x_{i+1}, \dots, \nu_{1n}x_n) = x_1$$

it follows that

$$(\nu_{1i}x_i, \nu_{12}x_2, \dots, \nu_{1,i-1}x_{i-1}, (x_1^n), \nu_{1,i+1}x_{i+1}, \dots, \nu_{1n}x_n) = x_1.$$

Using (2) and taking into account that $\nu_{1i}^2 = \varepsilon$ for all $i \in \overline{2, n}$ we get

$$(x_1^{i-1}, \nu_{1i}(x_1^n), x_{i+1}^n) = \nu_{1i}x_i$$

or

$$(\nu_{1i}(x_1^n), x_2^{i-1}, x_1, x_{i+1}^n) = \nu_{1i}x_i.$$

Using (2) again one has

$$\nu_{1i}(x_1^n) = (\nu_{1i}x_i, \nu_{12}x_2, \nu_{13}x_3, \dots, \nu_{1,i-1}x_{i-1}, \nu_{1i}x_1, \nu_{1,i+1}x_{i+1}, \dots, \nu_{1n}x_n)$$

for any $i \in \overline{2, n}$.

8. *In a symmetric n-IP-loop*
a) all substitutions I_{ij} are equal, i.e. $I_{ij}x = Ix$ for any $i, j \in \overline{1, n}$, $i \neq j$ and any $x \in Q$,
b) $I^2 = \varepsilon$.

We prove these statements.

a) Let e be a unit of a symmetric n-IP-loop. Then from the equalities

$$\left(\overset{i-1}{e}, x, \overset{j-i-1}{e}, I_{ij}x, \overset{n-j}{e}\right) = \left(\overset{k-1}{e}, x, \overset{t-k-1}{e}, I_{kt}x, \overset{n-t}{e}\right) = e$$

it follows that

$$\left(\overset{i-1}{e}, x, \overset{j-i-1}{e}, I_{ij}x, \overset{n-j}{e}\right) = \left(\overset{i-1}{e}, x, \overset{j-i-1}{e}, I_{kt}x, \overset{n-j}{e}\right),$$

i.e. $I_{ij}x = I_{kt}x = I_x$ for all $i, j, k, t \in \overline{1, n}$, $i \neq j$, $k \neq t$ and any $x \in Q$.

b) Changing in $\left(\overset{i-1}{e}, x, \overset{j-i-1}{e}, Ix, \overset{n-1}{e}\right) = e$ the element x for Ix we get

$$\left(\overset{i-1}{\rightarrow} e, Ix, \overset{j-i-1}{\rightarrow} e, I^2x, \overset{n-j}{\rightarrow} e\right) = e = \left(\overset{i-1}{e}, Ix, \overset{j-i-1}{e}, x, \overset{n-j}{e}\right)$$

from which it follows that

$$I^2x = x \quad \text{for any} \quad x \in Q.$$

It is known (cf. [1]) that
i) the product of two autotopies of an n-quasigroup is an autotopy,
ii) the product of two i-th inversion systems, $i \in \overline{1, n}$, of an n-IP-quasigroup is an autotopy,
iii) the product of an autotopy and an inversion system of an n-IP-quasigroup is an inversion system of this quasigroup.

The analogous results are true for the product of corresponding matrices.

Let $Q(A)$ be a symmetric n-IP-loop with a unique unit e and with an inversion matrix $\|\nu_1\|$. Then a connection between the substitute I and the inversion substitutions ν_{1i} is given by the following equality (see [1])

$$Ix = (e, \nu_{12}e, \ldots, \nu_{1,i-1}e, \nu_{1i}x, \nu_{1,i+1}e, \ldots, \nu_{1n}e) = L_i(\bar{e})\nu_{1i}x \qquad (6)$$

where

$$L_i(\bar{e})x = (e, \nu_{12}e, \ldots, \nu_{1,i-1}e, x, \nu_{1,i+1}e, \ldots, \nu_{1n}e)$$

are substitutions of Q, $i \in \overline{1,n}$, $(\bar{e}) = (e, \nu_{12}e, \ldots, \nu_{1n}e)$.

Denote by $\mathfrak{O}_A$ the set of all inversion matrices and by $\mathfrak{A}_A$ the set of all matrices of autotopies of a symmetric n-IP-loop $Q(A)$. Let $\|\mathcal{L}\| = \|L_i(\bar{e})\|$. Then the equality (6) takes the form

$$\|I\| = \|\mathcal{L}\| \cdot \|\nu_1\|, \qquad (7)$$

i.e.

$$\begin{pmatrix} \varepsilon & I & I & \cdots & I & I & \varepsilon \\ I & \varepsilon & I & \cdots & I & I & \varepsilon \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ I & I & I & \cdots & I & I & \varepsilon \end{pmatrix} =$$

$$\begin{pmatrix} \varepsilon & L_2(\bar{e}) & L_3(\bar{e}) & \cdots & L_{n-1}(\bar{e}) & L_n(\bar{e}) & \varepsilon \\ L_2(\bar{e}) & \varepsilon & L_3(\bar{e}) & \cdots & L_{n-1}(\bar{e}) & L_n(\bar{e}) & \varepsilon \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ L_2(\bar{e}) & L_3(\bar{e}) & L_4(\bar{e}) & \cdots & L_{n-1}(\bar{e}) & \varepsilon & \varepsilon \end{pmatrix} \times$$

$$\times \begin{pmatrix} \varepsilon & \nu_{12} & \nu_{13} & \cdots & \nu_{1,n-1} & \nu_{1n} & \varepsilon \\ \nu_{12} & \varepsilon & \nu_{13} & \cdots & \nu_{1,n-1} & \nu_{1n} & \varepsilon \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \nu_{12} & \nu_{13} & \nu_{14} & \cdots & \nu_{1,n-1} & \varepsilon & \varepsilon \end{pmatrix}.$$

From (7) it follows that

$$\|I\| \in \mathfrak{O}_A \Longleftrightarrow \|\mathcal{L}\| \in \mathfrak{A}_A. \qquad (8)$$

Theorem 1. *The matrix $\|I\|$ is one of the inversion matrices of a symmetric n-IP-loop with a unique unit.*

Proof. Let $Q(A) = Q(\ )$ be a symmetric n-IP-loop with an inversion matrix $\|\nu_1\|$ and with a unique unit e. Then $(\varepsilon, \nu_{12}, \nu_{13}, \ldots, \nu_{1n}, \varepsilon) \in \mathfrak{O}_A$, and by property 3 any permutation of the first n substitutions of this inversion system gives an inversion system of this loop. According to property 6

$$\left(\overset{i-1}{\varepsilon}, \nu_{1i}\nu_{1j}, \overset{j-i-1}{\varepsilon}, \nu_{1j}\nu_{1i}, \overset{n-j+1}{\varepsilon}\right) \in \mathfrak{A}_A$$

for any $i, j \in \overline{2, n}$. By property 3 any permutation of the first n components is an autotopy of the loop. Thus, by $1 < i < j < n$, we have

$$\begin{gathered}(\nu_{1i}, \nu_{1j}, \nu_{12}, \nu_{13}, \ldots, \nu_{1,i-1}, \nu_{1,i+1}, \ldots, \nu_{1,j-1}, \nu_{1,j+1}, \ldots, \nu_{1n}, \varepsilon, \varepsilon)\times\\ \times(\nu_{1j}\nu_{1i}, \nu_{1i}\nu_{1j}, \overset{n-1}{\to} \varepsilon) = (\nu_{1i}\nu_{1j}\nu_{1i}, \nu_{1j}\nu_{1i}\nu_{1j}, \nu_{12}, \nu_{13}, \ldots\\ \ldots, \nu_{1,i-1}, \nu_{1,i+1}, \ldots, \nu_{1,j-1}, \nu_{1,j+1}, \ldots, \nu_{1n}, \varepsilon, \varepsilon) \in \mathfrak{O}_A.\end{gathered}$$

Then by property 5

$$\begin{gathered}(\varepsilon, \nu_{1j}, \nu_{12}, \nu_{13}, \ldots, \nu_{1,i-1}, \nu_{1,i+1}, \ldots, \nu_{1,j-1}, \nu_{1i}, \nu_{1,j+1}, \ldots, \nu_{1n}, \varepsilon)\times\\ \times(\nu_{1i}\nu_{1j}\nu_{1i}, \nu_{1j}\nu_{1i}\nu_{1j}, \nu_{12}, \nu_{13}, \ldots, \nu_{1,i-1}, \nu_{1,i+1}, \ldots, \nu_{1,j-1}, \nu_{1,j+1}, \ldots\\ \ldots, \nu_{1n}, \varepsilon, \varepsilon) = (\nu_{1i}\nu_{1j}\nu_{1i}, \nu_{1i}\nu_{1j}, \overset{j-3}{\to} \varepsilon, \nu_{1i}, \overset{n-j+1}{\to} \varepsilon) \in \mathfrak{A}_A \qquad .\end{gathered}$$

Next,

$$\begin{gathered}(\nu_{1i}\nu_{1j}\nu_{1i}, \nu_{1i}\nu_{1j}, \overset{j-3}{\to} \varepsilon, \nu_{1i}, \overset{n-j+1}{\to} \varepsilon) \cdot (\varepsilon, \nu_{1j}\nu_{1i}, \overset{j-3}{\to} \varepsilon, \nu_{1i}\nu_{1j}, \overset{n-j+1}{\to} \varepsilon)\\ = (\nu_{1i}\nu_{1j}\nu_{1i}, \overset{j-2}{\to} \varepsilon, \nu_{1j}, \overset{n-j+1}{\to} \varepsilon) \in \mathfrak{A}_A.\end{gathered}$$

Now use properties 4 and 5:

$$\left(\overset{j-1}{\varepsilon}, \nu_{1j}, \overset{n-j}{\varepsilon}, \nu_{1i}\nu_{1j}\nu_{1i}\right) \in \mathfrak{A}_A,$$

i.e.

$$\nu_{1i}\nu_{1j}\nu_{1i}A(x_1^n) = A(x_1^{j-1}, \nu_{1j}x, x_{j+1}^n).$$

From these equalities by $x_1 = x_2 = \cdots = x_{j-1} = x_{j+1} = \cdots = x_n = e$ we get that

$$\nu_{1i}\nu_{1j}\nu_{1i}x = \nu_{1j}x.$$

Replacing x by $\nu_{1i}x$ and using property 5 one has

$$\nu_{1i}\nu_{1j}x = \nu_{1j}\nu_{1i}x \tag{9}$$

for all $x \in Q$ and any $i, j \in \overline{1, n}$.

Now let $Q(A)$ have an odd arity. Then by property 6 and equality (9) the equality

$$(x, \nu_{1i}\nu_{1j}e, \nu_{ij}\nu_{1i}e, \nu_{1i}\nu_{1j}e, \nu_{1j}\nu_{1i}e, \ldots, \nu_{1i}\nu_{1j}e, \nu_{1j}\nu_{1i}e) = x$$

implies

$$\left(\overset{k-1}{\nu_{1i}\nu_{1j}e}, x, \overset{n-k}{\nu_{1i}\nu_{1j}e}\right) = x$$

for any $k \in \overline{1, n}$ and $x \in Q$. Thus, $\nu_{1i}\nu_{1j}e = e$, since $n - 1$ is an even number and e is a unique unit. But then $\nu_{1i}e = \nu_{1j}e$ for any $i, j \in \overline{2, n}$ since the inverse substitutions have order two. Therefore,

$$\nu_{12}e = \nu_{13}e = \cdots = \nu_{1n}e.$$

Next, since

$$\left(\overset{i-1}{\varepsilon}, \nu_{1i}\nu_{1j}, \overset{j-i-1}{\varepsilon}, \nu_{1j}\nu_{1i}, \overset{n-j+1}{\varepsilon}\right) \in \mathfrak{A}_A$$

then $\left(\overset{i-1}{e}, x, \overset{n-i}{e}\right) = x$ implies

$$\left(\overset{i-1}{e}, \nu_{1i}\nu_{1j}x, \overset{j-i-1}{e}, \nu_{1j}\nu_{1i}e, \overset{n-j}{e}\right) = x,$$

from which receive $\nu_{1i}\nu_{1j}x = x$ and $\nu_{1i}x = \nu_{1j}x$ for any $i, j \in \overline{2, n}$ and any $x \in Q$. From $(x, \nu_{12}e, \nu_{13}e, \ldots, \nu_{1n}e) = x$ (see (1) by $i = 1$) it follows that $\left(\overset{i-1}{\nu_{12}e}, x, \overset{n-i}{\nu_{12}e}\right) = x$ for any $i \in \overline{1, n}$ and $x \in Q$. Thus, $\nu_{12}e = \nu_{13}e = \cdots = \nu_{1n}e = e$ and the equality

$$Ix = (e, \nu_{12}e, \nu_{13}e, \ldots, \nu_{1,i-1}e, \nu_{1i}x, \nu_{1,i+1}e, \ldots, \nu_{1n}e)$$

implies $Ix = \nu_{1i}x$ for any $i \in \overline{2, n}$, $x \in Q$.

Now from (6) we have that $L_i(\bar{e}) = \varepsilon$. Thus, $\|\mathcal{L}\| = \|E\|$, where $\|E\|$ is the identical matrix, i.e. the matrix consisting of ε, and so $\|\mathcal{L}\| \in \mathfrak{A}_A$. But according to (8) and (7)

$$\|I\| = \|\nu_1\|. \tag{10}$$

Now let $Q(A)$ have an even arity. In this case

$$(\varepsilon, \nu_{12}\nu_{13}\ldots\nu_{1n}, \nu_{13}\nu_{14}\ldots\nu_{1n}\nu_{12}, \nu_{14}\nu_{15}\ldots\nu_{1n}\nu_{12}\nu_{13}, \ldots$$
$$\ldots, \nu_{1n}\nu_{12}\nu_{13}\ldots\nu_{1,n-1}, \varepsilon) \in \mathfrak{A}_A$$

and according to (9)

$$\left(\varepsilon, \nu_{12}\nu_{13}\overset{n-1}{\cdots}\nu_{1n}, \varepsilon\right) \in \mathfrak{A}_A.$$

Hence, by property 3 from $\left(\overset{i-1}{e}, x, \overset{n-i}{e}\right) = x$ it follows that

$$\left(\nu_{12}\nu_{13}\overset{i-1}{\cdots}\nu_{1n}e, x, \nu_{12}\nu_{13}\overset{n-i}{\cdots}\nu_{1n}e\right) = x$$

for all $i \in Q$, i.e. $\nu_{12}\nu_{13}\ldots\nu_{1n}e = e$. On the other hand, since n is an even arity, then

$$T = (\varepsilon, \nu_{13}\nu_{14}\ldots\nu_{1n}, \nu_{12}\nu_{14}\nu_{15}\ldots\nu_{1n}, \ldots, \nu_{12}\nu_{13}\ldots\nu_{1,i-1}\nu_{1,i+1}\ldots\nu_{1n}, \\ \ldots, \nu_{12}\nu_{13}\ldots\nu_{1,n-1}, \varepsilon) \in \mathfrak{A}_A.$$

Using this autotopy, equality (9) and property 5 we get

$$L_i(\bar{e})x = (e, \nu_{12}e, \nu_{13}e, \ldots, \nu_{1,i-1}e, x, \nu_{1,i+1}e, \ldots, \nu_{1n}e) = \\ (e, \nu_{12}\nu_{13}\ldots\nu_{1n}e, \nu_{12}\nu_{13}\ldots\nu_{1n}e, \ldots, \nu_{12}\nu_{13}\ldots\nu_{1,i-1}\nu_{1,i+1}\ldots\nu_{1n}x, \\ \nu_{12}\nu_{13}\ldots\nu_{1n}e, \ldots, \nu_{12}\nu_{13}\ldots\nu_{1n}e) = \nu_{12}\nu_{13}\ldots\nu_{1,i-1}\nu_{1,i+1}\ldots\nu_{1n}x$$

for any $i \in \overline{2,n}$. Thus,

$$(\varepsilon, L_2(\bar{e}), L_3(\bar{e}), \ldots, L_i(\bar{e}), \ldots, L_n(\bar{e}), \varepsilon) \in \mathfrak{A}_A.$$

It means that $\|\mathcal{L}\| \in \mathfrak{A}_A$. Then by (8) $\|I\| \in \mathfrak{A}_A$ and

$$Ix = (e, \nu_{12}e, \nu_{13}e, \ldots, \nu_{1,i-1}e, \nu_{1i}x, \nu_{1,i+1}e, \ldots, \nu_{1n}e) = \\ (e, \nu_{12}\nu_{13}\ldots\nu_{1n}e, \nu_{12}\nu_{13}\ldots\nu_{1n}e, \ldots, \nu_{12}\nu_{13}\ldots\nu_{1,i-1}\nu_{1i}\nu_{1,i+1}\ldots\nu_{1n}x, \\ \nu_{12}\nu_{13}\ldots\nu_{1n}e, \ldots, \nu_{12}\nu_{13}\ldots\nu_{1n}e) = \nu_{12}\nu_{13}\ldots\nu_{1n}x.$$

The theorem is proved. □

Corollary 1. *Any symmetric n-IP-loop of an odd arity with a unique unit has only one inversion matrix, namely, the matrix $\|I\|$.*

This statement follows from the proof of the first part of Theorem, since any inversion matrix of a symmetric n-IP-loop of an odd arity with a unique unit coincides with the matrix $\|I\|$.

References

[1] **V. D. Belousov**: *n-Ary quasigroups*, (Russian), Ştiinţa, Chişinău 1972.

[2] **L. A. Ursu**: *n-Ary loop with the inverse property*, (Russian), Mat. Issled., **113** (1990), 108 − 118.

Department of Higher Mathematics
Technical State University
Dacia str., 41
MD-2060 Chishinau
Moldova

Received August 16, 1998