Quasigroups and Related Systems, **4** (1997), 23–38

The transitive and multitransitive automorphism groups of the multiplace quasigroups

Oleg U. Kirnasovsky

Abstract

In this paper, for every k, the multiplace group isotopes, which have $k-$transitive automorphism groups, are described.

1. Introduction

A groupoid $(G;g)$ is called an *isotope of a group* $(Q;+)$, iff for some bijections $\gamma_1, \ldots, \gamma_n$ and γ of G on Q the equality

$$\gamma g(x_1, \ldots, x_n) = \gamma_1 x_1 + \ldots + \gamma_n x_n$$

holds. The groupoid $(G;g)$ is called also a *group isotope*. A groupoid $(G;g)$ is called a *linear isotope* of a group $(G;+)$ iff there are automorphisms $\alpha_1, \ldots, \alpha_n$ of a group $(G;+)$ such that

$$g(x_1, \ldots, x_n) = \alpha_1 x_1 + \ldots + \alpha_n x_n + a$$

for some fixed $a \in G$. It is easy to see that every group isotope is a quasigroup. Also a quasigroup isomorphic to a linear isotope is a linear isotope.

Let $S(Q)$ be a permutation group of Q. We say that a group $S(Q)$ is *k-times transitive (or k-transitive) on the set $H \subset Q$*, where k is a

1991 Mathematics Subject Classification: 20N05, 20N15
Keywords: quasigroup, isotopy, n-ary quasigroup

fixed cardinal number, iff $|H| \geq k$, $\sigma(H) = H$ for every $\sigma \in S(Q)$ and for each bijection $\varphi : A \to B$ of k-element subsets A, B of H there exists $\alpha \in S(Q)$ such that $\alpha x = \varphi x$ for all $x \in A$.

1-transitive group will be also called *transitive*. The words "on the set H" will be omitted if $H = Q$.

The D-quasigroups, i.e. the finite binary quasigroups having double-transitive automorphism groups, are investigated in [3]. The finite binary groupoids having double-transitive automorphism groups are described in [2]. Here we continue the investigation for the case of the multiplace quasigroups.

The author would like to expresses his sincere thanks to Dr. Volodymyr Derech for suggesting the problem. Author also expresses his great thanks to Dr. Fedir Sokhatsky for his very useful comments.

2. Some individual cases

Theorem 1. *The automorphism group of an unary quasigroup $(Q; f)$ is transitive iff either all cycles of f are infinite, or all these cycles are finite and have the same length.*

Proof. Let the automorphism group be transitive and

$$(x_1, \ldots, x_n), \quad (\ldots, y_1, \ldots, y_n, \ldots)$$

be some cycles of f, and let the length of the second cycle be greater than n (or be infinite). Transitivity of the automorphism group implies the existence of an automorphism α of the unary quasigroup $(Q; f)$, for which $\alpha x_1 = y_1$. Then α commutes with f, and in the consequence, with f^n. Thus $y_{n+1} = f^n y_1 = f^n \alpha x_1 = \alpha f^n x_1 = \alpha x_1 = y_1$, which is a contradiction.

On the other hand, let all cycles of f have the same (may be infinite) length and let $x, y \in Q$ be arbitrary elements. If they are in the same cycle, then there exists a positive integer n such that $f^n x = y$ and f^n is an automorphism of $(Q; +)$. If $x = x_1$, $y = y_1$, and

$$(\ldots, x_1, \ldots, x_n, \ldots), \quad (\ldots, y_1, \ldots, y_n, \ldots)$$

are different cycles of f, then the permutation α being the product of all cycles of the type (x_i, y_i) is an automorphism of $(Q; f)$, with the

condition $\alpha x = y$. This proves the transitivity. □

We say that a groupoid $(Q; h)$ is *derived from a group* $(Q; +)$, iff

$$h(x_1, \ldots, x_n) = x_1 + \ldots + x_n \,. \tag{1}$$

Lemma 2. *Every quasigroup with at most* 3 *elements is a linear isotope of a cyclic group.*

Proof. Let $(Q; f)$ be a quasigroup. For $|Q| = 1$ the lemma is evident. Let $|Q| > 1$. We consider the ring $(Q; +, \cdot)$. The element 0 is an idempotent of the operation g:

$$g(x_1, \ldots, x_n) = f(x_1, \ldots, x_n) - f(0, \ldots, 0).$$

Define the operation h by

$$h(x_1, x_2, \ldots, x_n) =$$
$$= g(g(1, 0, \ldots, 0) \cdot x_1, g(0, 1, 0, 0, \ldots, 0) \cdot x_2, \ldots, g(0, \ldots, 0, 1) \cdot x_n).$$

We prove that the groupoid $(Q; h)$ is derived from the cyclic group $(Q; +)$. For $|Q| = 2$ the equality is easy provable by the induction on the number of the appearances of the element 1 in the collection $\langle x_1, \ldots, x_n \rangle$. Let $|Q| = 3$. Denote by r_i the number of the appearances for an element i in the collection $\langle x_1, \ldots, x_n \rangle$. For $k = 0$ we have:

$$h(0, \ldots, 0) = g(0, \ldots, 0) = 0.$$

Assume by the induction that this is true for $k = j$. We prove it for $k = j + 1$. At first, we consider the case when r_1 and r_2 are positive. Then we replace either one of the appearances of the element 1 by the element 0, or one of the appearances of the element 2 by the element 0. In this case the result of the operation will be changed because h is a quasigroup operation. Then by the inductive hypothesis the result of the application of h to the given collection is not equal modulo 3 to none of the numbers

$$(r_0 + 1) \cdot 0 + (r_1 - 1) \cdot 1 + r_2 \cdot 2, \quad (r_0 + 1) \cdot 0 + r_1 \cdot 1 + (r_2 - 1) \cdot 2,$$

and consequently, is equal to $0 \cdot r_0 + 1 \cdot r_1 + 2 \cdot r_2 = r_1 + 2r_2$.

Now, let $r_1 = 0$, then $r_2 \neq 0$, since $k > 0$. For $r_2 = 1$ the statement follows from the construction of the operation h. If $r_2 > 1$, then we replace either one of the appearances of the element 2 by the element 0, or one of the appearances of the element 2 by the element 1. Then by the hypothesis and by the statement proved above, the result of the application of h to the given collection is not equal modulo 3 to none of the numbers

$$(r_0 + 1) \cdot 0 + r_1 \cdot 1 + (r_2 - 1) \cdot 2, \quad r_0 \cdot 0 + (r_1 + 1) \cdot 1 + (r_2 - 1) \cdot 2.$$

Now, let $r_2 = 0$. Then we replace either one of the appearances of the element 1 by the element 0, or one of the appearances of the element 1 by the element 2. Thence, analogously by the inductive hypothesis and by the statement proved above, we receive that the result of the application of h to the given collection is not equal modulo 3 to none of the numbers

$$(r_0 + 1) \cdot 0 + (r_1 - 1) \cdot 1 + r_2 \cdot 2, \quad r_0 \cdot 0 + (r_1 - 1) \cdot 1 + (r_2 + 1) \cdot 2,$$

which completes the proof. □

As a consequence of the above Lemma we obtain

Corollary 3. *The automorphism group of the quasigroup $(Q; f)$ with $|Q| = 2$ is double-transitive.*

A group $S(Q)$ is called *k-cotransitive*, where k is some fixed cardinal number, iff $|Q| \geq k$, and for every bijection $\varphi : Q \setminus A \to Q \setminus B$, where A and B are arbitrary k-subsets of Q, there exists $\alpha \in S(Q)$ such that $\alpha x = \varphi x$ for all $x \in Q \setminus A$.

It is clear that with $|Q| = n < \aleph_0$ such k-cotransitivity is equivalent to the $(n - k)$-times transitivity of this group.

Lemma 4. *Let (Q, Ω) be an algebra containing infinitary operations perhaps. If a subset M of Q is k-transitive with $|M| + 1 \leq k$, $|Q \setminus M| \geq 2$, or k-cotransitive with $|Q \setminus M| \geq k + 1$, $|Q \setminus M| \geq 2$, then M is a subalgebra of the given algebra.*

Proof. Since the case of the k-transitivity follows from the case of the k-cotransitivity, we prove only the case of the k-cotransitivity. If M is not a subalgebra, then there exist an operation σ of this algebra and the sequence

$$\langle x_i \,|\, i \in I\rangle \tag{2}$$

(the cardinal number of I and the arity of σ are equal), such that

$$(\forall i \in I)\, x_i \in M, \quad y = \sigma(\langle x_i \,|\, i \in I\rangle) \notin M. \tag{3}$$

But for $|Q\backslash M| \geq 2$ there exists $z \in Q \setminus M$ such that $z \neq y$. Moreover, the k-cotransitivity implies the existence of an automorphism φ of (Q, Ω) for which $\varphi y = z$ and $\varphi x_i = x_i$ for all $i \in I$. Thus

$$z = \varphi y = \varphi\sigma(\langle x_i \,|\, i \in I\rangle) = \sigma(\langle \varphi x_i \,|\, i \in I\rangle) = \sigma(\langle x_i \,|\, i \in I\rangle),$$

which is impossible. □

Corollary 5. *If the automorphism group of an algebra (Q, Ω) is k-transitive and the maximal power of the arities of the operations of the algebra exists and is equal to n, where $n+1 \leq k$, $n+1 < |Q|$, then each non-empty subset of the set Q is a subalgebra.*

Proof. If we assume the contrary, then we get the existence of an operation $\sigma \in \Omega$ and of a collection (2), for which the conditions (3) hold. But this contradicts to the existence of $M = \{x_i \,|\, i \in I\}$ concerning the operation σ, although such existence follows from the previous Lemma. □

Theorem 6. *The automorphism group of an unary quasigroup $(Q; f)$, where $|Q| > 2$, is double-transitive iff f is the identical permutation. In this case the automorphism group is $|Q|$-transitive.*

Proof. If the automorphism group is double-transitive, then f is the identical substitution, by Lemma 4. On the other hand, every substitution of Q commutes with the identical permutation, and in the consequence, it is an automorphism of the respective unary quasigroup. □

Theorem 7. *The automorphism group of the quasigroups $(Q; f)$ with $|Q| = 3$ is triple-transitive iff the quasigroup is idempotent.*

Proof. By Lemma 2, given quasigroup is a linear isotope of a cyclic group. Such triple-transitivity is equivalent to the isomorphism of the given automorphism group to the holomorph of the cyclic group. From results of [4] it follows that such isomorphism is equivalent to idempotency of the quasigroup $(Q; f)$. □

Lemma 8. *Non-one-element quasigroups, in which all one-element and two-element subsets are their subquasigroups, have odd arities and are described by the system of identities $f(u_1, \ldots, u_n) = u_{n+1}$, where metavariables u_1, ..., u_{n+1} accept values in the set of the propositional variables $\{x; y\}$, and, besides u_{n+1} coincides with propositional variable x or y, appearing in the sequence u_1, ..., u_n odd number of times.*

Proof. Indeed, let $\{a; b\}$ be fixed. At once we throw the case away when the arity of the quasigroup is equal to zero, because then the lemma conditions are false. The oddness of the operation arity follows by evident way from the assertion on the operation value, since an operation of an even arity may have each from the elements a and b odd number of times in the role of arguments. And we prove the assertion about the operation value by the induction on the number k of the appearances, for example, of the element b in the role. If $k = 0$, then the assertion follows from Lemma 4. Let with $k = i$ the assertion be true. We have to prove it for $k = i + 1$. By Lemma 4, the operation value on the given collection is equal to either a or b. It remains to take into account that we must get other value, if we replace one of the appearances of b on a, because f is a quasigroup operation.□

Theorem 9. *The automorphism group of a quasigroup $(Q; f)$ with $|Q| = 4$ is quadruple-transitive iff the arity of the operation is odd and the quasigroup is derived from the group $Z_2 \times Z_2$.*

Proof. Let the automorphism group be quadruple-transitive. We de-

fine on the set Q an operation $(+)$ being isomorphic to the operation of the group $Z_2 \times Z_2$. Using Lemmas 4 and 8 we get the oddness of the arity n of the quasigroup $(Q; f)$ and the truth of the formula

$$f(x_1, \ldots, x_n) = x_1 + \ldots + x_n \tag{4}$$

for the case, when $|\{x_1; \ldots; x_n\}| \leq 2$, since in the group $(Q; +)$ the identity $2x = 0$ holds.

We prove (4) for the other cases. We will do it by the induction on the value of the product

$$P = (a+1)(b+1)(c+1)(d+1),$$

where a, b, c and d are numbers of the appearances of each of four elements of Q in the collection of the arguments of the operation f in (4). Without restricting the generality we assume that

$$a \geq b \geq c \geq d,$$

whence we have $c > 0$ (with $c = 0$ the statement has just been proved above). Let $u, v, w \in Q$ correspond to the numbers a, b and c respectively. In the fixed collection of all arguments of the operation f we make three independent changes (in so doing, we receive three individual collections). First: we replace an arbitrary appearance of the element v with the element u. Second: we replace an arbitrary appearance of the element w with the element u. And third: we replace an arbitrary appearance of the element w with the element v. In this case the value of the product P is respectively replaced by the products

$$P_1 = (a+2)b(c+1)(d+1),$$
$$P_2 = (a+2)(b+1)c(d+1),$$
$$P_3 = (a+1)(b+2)c(d+1),$$

which are less than P. By the inductive hypothesis, values of f on three obtained collections are pairwise different and all of them must be different from the value on the given collection, because f is a quasigroup operation. But values of the right side of (4) on all these four collections are also pairwise different. Therefore, taking into account that $|Q| = 4$, we get the truth of the formula (4) on the given collection. The rest follows from the fact that the given automorphism group is isomorphic to $\mathrm{Hol}(Z_2 \times Z_2)$, and the holomorph consists of all substitutions of the basis set. $\square$

3. The general case

Lemma 10. *For all mappings $\alpha_1, \ldots, \alpha_n$ of a group $(Q;+)$ and for the mappings $\beta_1, \ldots, \beta_n$ defined by*

$$\beta_i = \alpha_1 + \ldots + \alpha_i, \qquad \text{where} \quad i = 0, \ldots, n, \tag{5}$$

the equality of the subgroups

$$\{\psi \in Aut(Q;+) \,|\, \psi\beta_i = \beta_i\psi, \;\; i = 1, \ldots, n\} = \\ = \{\psi \in Aut(Q;+) \,|\, \psi\alpha_i = \alpha_i\psi, \;\; i = 1, \ldots, n\}$$

of the group $Aut(Q;+)$ holds.

Proof. Let ψ commute with α_i when $i = 1, \ldots, n$. Then, for each i we have that

$$\psi\beta_i = \psi(\alpha_1 + \ldots + \alpha_i) = \psi\alpha_1 + \ldots + \psi\alpha_i = \\ = \alpha_1\psi + \ldots + \alpha_i\psi = (\alpha_1 + \ldots + \alpha_i)\psi = \beta_i\psi.$$

Now on the contrary, let ψ commute with β_i when $i = 1, \ldots, n$. It is evident that ψ commutes with β_0 as well. Then, for all i, we have that

$$\begin{aligned} \psi\alpha_i \;&= -\psi\beta_{i-1} + \psi\beta_{i-1} + \psi\alpha_i = -\psi\beta_{i-1} + \psi(\beta_{i-1} + \alpha_i) \\ &= -\psi\beta_{i-1} + \psi\beta_i = -\beta_{i-1}\psi + \beta_i\psi = -\beta_{i-1}\psi + (\beta_{i-1} + \alpha_i)\psi \\ &= (-\beta_{i-1} + \beta_{i-1} + \alpha_i)\psi = \alpha_i\psi. \end{aligned}$$

□

We denote by L_c and R_c respectively the left and right translations of the group operation $(+)$, by I_c the inner automorphism $L_c^{-1}R_c$, and by ε the identical permutation.

For shortening of the statement wording we reach agreement about unified notations further in this point (except the end of the article). Namely: let us fix an arbitrary group, denoted as $(Q;+)$, its arbitrary element, denoted as a, an arbitrary integer greater than one, denoted as n, arbitrary n unitary substitutions, denoted as $\alpha_1, \ldots, \alpha_n$. Under these designations let us fix also the notation $(Q;f)$ for the group isotope specified by the equality

$$f(x_1, \ldots, x_n) = \alpha_1 x_1 + \ldots + \alpha_n x_n + a,$$

also the notation $\beta_0, \ldots, \beta_n$ for the mappings of the set Q specified by the equalities (5) (here, it is natural that β_0 is the null-endomorphism of the given group). Finally, let us fix the notation H for the subgroup of $\mathrm{Aut}(Q;+)$, consisting of all automorphisms, stated in Theorem 10, and the notation γ for the mapping, specified by the equality $\gamma = R_a\beta_n - \varepsilon$.

During the conference in Barnaul (1991) F. Sokhatsky announced the following result.

Theorem 11. *A transformation α is an endomorphism of a group isotope $(Q;f)$ iff $\alpha = R_c\theta$ for some endomorphism θ of the group $(Q;+)$ and some element c such that*

$$\theta a + c = \alpha_1 c + \ldots + \alpha_n c + a, \tag{6}$$

$$R_{\alpha_i c} I_{\alpha_1 c + \ldots + \alpha_{i-1} c} \theta \alpha_i = \alpha_i R_c \theta \qquad \text{for all} \quad i = 1, \ldots, n. \tag{7}$$

Theorem 12. *A transformation α is an endomorphism of a group isotope $(Q;f)$ iff $\alpha = R_c\theta$ for some element c and for some endomorphism θ of the group $(Q;+)$ such that*

$$\theta a + c = \beta_n c + a, \tag{8}$$

$$R_{\beta_i c}\theta\beta_i = \beta_i R_c \theta \qquad \text{for all} \quad i = 1, \ldots, n. \tag{9}$$

Proof. The equality (6) is equivalent to (8), therefore by Theorem 11 it is enough to show that (7) is equivalent to (9). Replace the number n by as arbitrary number k and let us prove the equivalence of the obtained systems for all natural k, not greater than n. Make that by the induction on k. For when $k = 1$ we have one equality in both systems only, which are equivalent, because $\beta_1 = \alpha_1$, $I_{\beta_0 c} = \varepsilon$. Assume that for $i = m$ these systems are equivalent. For $i = m + 1$ the equality (9) may be rewritten in the form

$$R_{\alpha_{m+1}c} R_{\beta_m c}\theta(\beta_m + \alpha_{m+1}) = (\beta_m + \alpha_{m+1}) R_c\theta. \tag{10}$$

Since (9) holds when $i = m$, then

$$(\beta_m + \alpha_{m+1}) R_c\theta = \beta_m R_c\theta + \alpha_{m+1} R_c\theta = R_{\beta_m c}\theta\beta_m + \alpha_{m+1} R_c\theta,$$

and hence, (10) may be rewritten in the form

$$R_{\alpha_{m+1}c} R_{\beta_m c}\theta(\beta_m + \alpha_{m+1}) = R_{\beta_m c}\theta\beta_m + \alpha_{m+1} R_c\theta,$$

that is

$$\theta\beta_m + R_{\alpha_{m+1}c}R_{\beta_m c}\theta\alpha_{m+1} = \theta\beta_m + L_{\beta_m c}\alpha_{m+1}R_c\theta,$$

whence after equivalent transformations we have

$$R_{\alpha_{m+1}c}I_{\beta_m c}\theta\alpha_{m+1} = \alpha_{m+1}R_c\theta,$$

which is equivalent to (7) with $i = m+1$. This completes the proof.□

Theorem 13. *The automorphism group of a group isotope $(Q; f)$ is transitive iff for every element $c \in Q$ there exists an automorphism θ of the group $(Q; +)$ such that* (9) *holds and the element $\theta^{-1}\gamma c$ is the image of the element a under the action of some transformation from the group H.*

Proof. Let $\mathrm{Aut}(Q; f)$ be transitive. Then for every $c \in Q$ there exists an automorphism α of of the group isotope $(Q; f)$ which maps the neutral element of $(Q; +)$ to c. By Theorem 12 it means that for each $c \in Q$ there exists an automorphism θ of $(Q; +)$ satisfying (8) and (9). From (8) we have that $\theta^{-1}\gamma c = a$, but the identical automorphism of $(Q; +)$ maps a to itself and commutes with all β_i.

On the other hand, let for every $c \in Q$ there exist an automorphism θ of $(Q; +)$ satisfying (9), and thereto for these c and θ, the element $\theta^{-1}\gamma c$ is the image of a under the action of some automorphism ψ from H. Then for these triples of c, θ and ψ we have

$$\theta\psi a + c = \theta\theta^{-1}(\beta_n c + a - c) + c = \beta_n c + a,$$
$$R_{\beta_i c}\theta\psi\beta_i = R_{\beta_i c}\theta\beta_i\psi = \beta_i R_c\theta\psi \qquad \text{for all} \quad i = 1, \ldots, n, \quad (11)$$

whence taking into account bijectivity of the transformations of $R_c\theta\psi$ we have, by Theorem 12, that they are automorphisms of the group isotope $(Q; f)$. Consequently, for an arbitrary fixed $x, y \in Q$ there are automorphisms θ', ψ', θ'' and ψ'' such that $R_x\theta'\psi'$ and $R_y\theta''\psi''$ are automorphisms of the group isotope $(Q; f)$. But

$$R_y\theta''\psi''(R_x\theta'\psi')^{-1}x = R_y\theta''\psi''(\psi')^{-1}(\theta')^{-1}R_x^{-1}x$$
$$= R_y\theta''\psi''(\psi')^{-1}(\theta')^{-1}0 = R_y 0 = y,$$

whence $\mathrm{Aut}(Q;f)$ is transitive. □

Corollary 14. *If transformations $\beta_1, \ldots, \beta_n$ are endomorphisms (for example, if the group $(Q;+)$ is abelian and its isotope $(Q;f)$ is linear) of a group $(Q;+)$ then the automorphism group of a group isotope $(Q;f)$ is transitive iff one of the following equivalent conditions holds:*

- *the set $Im\gamma$ is a subset of the set of images of a under the action of all transformations of the group H;*
- *for all $x, y \in Im\gamma$ there exists a transformation φ from the group H which maps x to y.*

Proof. If $\beta_1, \ldots, \beta_n$ are endomorphisms of $(Q;+)$, then (9) means that θ belongs to H. Since all groups are non-empty, then by Theorem 13, $\mathrm{Aut}(Q;f)$ is transitive iff for each $c \in Q$ there are transformations θ and ψ from H such that $\psi a = \theta^{-1}\gamma c$, i.e.

$$\delta a = \gamma c, \tag{12}$$

where $\delta = \theta\psi$. Hence, $\mathrm{Aut}(Q;f)$ is transitive iff for every $c \in Q$ there exists a transformation δ from H such that (12) holds, i.e, iff $\mathrm{Im}\gamma$ is a subset of the set of all images of a under the action of all transformations from H. We prove the equivalence of the two conditions of our corollary criterion. Let $\mathrm{Im}\,\gamma$ be a subset of the set of all images of a under the action of all transformations from the group H. Then for all $x, y \in \mathrm{Im}\gamma$ there exist transformations φ_1 and φ_2 from H such that $\varphi_1 a = x$, $\varphi_2 a = y$. Thus $\varphi_2\varphi_1^{-1}x = y$. Hence, the second condition follows from the first one. Let now the second condition holds. Since γ maps the neutral element of $(Q;+)$ to a, then a belongs to $\mathrm{Im}\,\gamma$. Hence, for every $y \in \mathrm{Im}\,\gamma$ there exists $\varphi \in H$, for which $\varphi x = y$. And this is the first of the two conditions of the corollary criterion. □

Corollary 15. *If transformations $\beta_1, \ldots, \beta_n$ are endomorphisms of a group $(Q;+)$ and the group H is transitive on the set $Im\gamma$, then the automorphism group of a group isotope $(Q;f)$ is transitive.* □

Corollary 16. *If $\beta_n = \varepsilon$, transformations β_1, ..., β_{n-1} are endomorphisms of a group $(Q;+)$, and a is central in this group, then the automorphism group of the group isotope $(Q;f)$ is transitive.*

Proof. $\operatorname{Im}\gamma$ has only one element, which under the action of the transformation ε is mapped to itself. Hence, by Corollary 14, the group $\operatorname{Aut}(Q;f)$ is transitive. □

Corollary 17. *The automorphism group of an idempotent group isotope $(Q;f)$, where β_1, ..., β_n are endomorphisms of the group $(Q;+)$, is transitive.* □

Corollary 18. *The automorphism group of an idempotent group isotope $(Q;f)$ is transitive iff for every element $c \in Q$ there exists an automorphism θ of the group $(Q;+)$ such that (9) holds.*

Proof. Idempotency of the isotope $(Q;f)$ gives $\beta_n = \varepsilon$ and $a = 0$. Therefore $\operatorname{Im}\gamma$ contains only the neutral element of $(Q;+)$. Since the identical transformation commutes with all mappings, then Theorem 13 completes our proof. □

Example. Let $(Q;+)$ be a cyclic group Z_6, and

$$n = 3, \quad a = 0, \quad \alpha_1 = \varepsilon,$$

$$\alpha_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 1 & 4 & 5 & 2 & 3 \end{pmatrix}, \quad \alpha_3 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 5 & 2 & 1 & 4 & 3 \end{pmatrix}.$$

Then the group isotope $(Q;f)$ is idempotent. The map:

$$\beta_2 = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 0 & 2 & 0 & 2 & 0 & 2 \end{pmatrix},$$

is not an endomorphism of the group $(Q:+)$ because

$$\beta_2(1+1) = \beta_2 2 = 0 \neq 4 = 2+2 = \beta_2 1 + \beta_2 1.$$

But the group $\operatorname{Aut}(Q;+)$ is transitive. Indeed, by Corollary 18, for verifying of transitivity of this group it is enough to show that for

every $c \in Q$ there exists an automorphism θ of $(Q;+)$ satisfying (9). In the group Z_6 there are two automorphisms: ε and $-\varepsilon$. When $i = 1$ and when $i = 3$, both of them satisfy (9). For $i = 2$ (9) has the form

$$(\forall x \in Q) \quad \theta\beta_2 x + \beta_2 c = \beta_2(\theta x + c).$$

If $c \in \{0;2;4\}$, then $\theta = \varepsilon$ and:

$$\beta_2(\theta x + c) = \beta_2(x + c) = \beta_2 x = \beta_2 x + \beta_2 c = \theta\beta_2 x + \beta_2 c.$$

If $c \in \{1;3;5\}$, then $\theta = -\varepsilon$ and:

$$\beta_2(\theta x + c) = \beta_2(-x + c) = \beta_2(x + c) = 2 - \beta_2 x$$
$$= \beta_2 c - \beta_2 x = -\beta_2 x + \beta_2 c = \theta\beta_2 x + \beta_2 c.$$

This proves that $\mathrm{Aut}(Q;f)$ is transitive. □

Theorem 19. *A transitive automorphism group of a group isotope $(Q;f)$ with $|Q| > 2$ is double-transitive iff $(Q;f)$ is idempotent, the group H is transitive on the set of all non-neutral elements of the group $(Q;+)$.*

Proof. While proving Lemma 4 in the both directions, we can consider that $(Q;f)$ is idempotent. Then, by Corollary 18, for every $c \in Q$ there exists an automorphism θ of $(Q;+)$ satisfying (9). Since $\beta_n = \varepsilon$, and $a = 0$ (because $(Q;f)$ is idempotent), then for every c and for every automorphism θ of $(Q;+)$ (8) holds. Hence, by Theorem 12 the mapping α is an automorphism of the group isotope $(Q;f)$ iff $\alpha = R_c\theta$ for some c and some automorphism θ of $(Q;+)$ satisfying (9). Let $\mathrm{Aut}(Q;f)$ be double-transitive, then for all non-neutral $x, y \in Q$ there exist c and an automorphism θ of $(Q;+)$ such that (9) holds and also

$$R_c\theta 0 = 0, \quad R_c\theta x = y.$$

From the first of these equalities we obtain that $c = 0$, and hence, $\theta x = y$. From (9) follows that θ belongs to the group H. It is also obvious that θ maps all non-neutral elements of $(Q;+)$ to non-neutral, and in the consequence, the group H is transitive on $Q\backslash\{0\}$. Let now $x, y, c \in Q$ and $x \neq 0$, $y \neq c$. By the above, there exists an automorphism θ of $(Q;+)$ satisfying (9). Since the group H is transitive on $Q\backslash\{0\}$, then there exists $\psi \in H$, for which $\psi x = \theta^{-1}(y - c)$. Then we

have (11) and $\alpha 0 = c$, $\alpha x = y$, where the mapping $\alpha = R_c\theta\psi$ is an automorphism of the group isotope $(Q; f)$. If now we take arbitrary different elements $z, t \in Q$, then, analogously as in previous case, we obtain the existence of an automorphism β of the group isotope $(Q; f)$, for which $\beta 0 = z$, $\beta x = t$. Then for the automorphism $\beta\alpha^{-1}$ of the group isotope $(Q; f)$ we have

$$\beta\alpha^{-1}c = \beta 0 = z, \quad \beta\alpha^{-1}y = \beta x = t.$$

Hence, the group $\mathrm{Aut}(Q; f)$ is double-transitive. □

Theorem 20. *The automorphism group of a group isotope $(Q; f)$, where $|Q| > 3$, is triple-transitive iff n is odd, $(Q; f)$ is derived from $(Q; +)$ and $(Q; +)$ is an abelian group of period 2 whose automorphism group is double-transitive on the set of all non-neutral elements of the group $(Q; +)$.*

Proof. Assume that $\mathrm{Aut}(Q; +)$ is triple-transitive. By Lemmas 4 and 8 the number n is odd, the group isotope is idempotent, and

$$f(\underbrace{0, \ldots, 0,}_{(i-1)-times} x, 0, \ldots, 0) = x \qquad \text{for all} \quad i = 1, \ldots, n,$$

$$f(x, x, 0, \ldots, 0) = 0.$$

Thus $\alpha_i = \varepsilon$ and $2x = 0$, because from idepotency of $(Q; f)$ we have that $a = 0$. This means that $(Q; +)$ is abelian. Then by Theorem 12 all automorphisms of the group isotope $(Q; f)$ are transformations of the form $R_c\theta$, where $c \in Q$, and θ is an automorphism of $(Q; +)$. If the automorphism group of the group isotope $(Q; f)$ is triple-transitive, then for $x_1, x_2, y_1, y_2 \in Q$ such that $|\{0; x_1; x_2\}| = |\{0; y_1; y_2\}| = 3$ there exist c and an automorphism θ of $(Q; +)$, for which

$$R_c\theta 0 = 0, \quad R_c\theta x_1 = y_1, \quad R_c\theta x_2 = y_2.$$

From the first equality we obtain $c = 0$, and hence, $\theta x_1 = y_1$, $\theta x_2 = y_2$, which means that $\mathrm{Aut}(Q; +)$ is double-transitive on $Q\backslash\{0\}$. A contrary, let $\mathrm{Aut}(Q; +)$ be double-transitive on $Q\backslash\{0\}$, and x_1, x_2, x_3, y_1, y_2, $y_3 \in Q$ be such that $|\{x_1; x_2; x_3\}| = |\{y_1; y_2; y_3\}| = 3$. Then there exists an automorphism θ of $(Q; +)$, for which

$$\theta(x_2 - x_1) = y_2 - y_1, \quad \theta(x_3 - x_1) = y_3 - y_1.$$

This for $c = y_1 - \theta x_1$ gives the automorphism $R_c\theta$ of group isotope $(Q; f)$ such that

$$\begin{gathered} R_c\theta x_1 = \theta x_1 + (y_1 - \theta x_1) = y_1, \\ R_c\theta x_2 = \theta(x_2 - x_1) + R_c\theta x_1 = (y_2 - y_1) + y_1 = y_2, \\ R_c\theta x_3 = \theta(x_3 - x_1) + R_c\theta x_1 = (y_3 - y_1) + y_1 = y_3. \end{gathered}$$

This proves that the group $\mathrm{Aut}(Q; +)$ is triple-transitive. □

Theorem 21. *The automorphism group of a non-unary quasigroup $(Q; f)$ with $|Q| > 4$ is not quadruple-transitive.*

Proof. If it is not quadruple-transitive, then by Lemmas 4 and 8, for arbitrary $a, b, c \in Q$ we have

$$\begin{gathered} f(a, c, \ldots, c) = a, \\ f(a, a, c, \ldots, c) = c, \\ f(c, b, c, c, \ldots, c) = b. \end{gathered}$$

Thus $f(a, b, c, \ldots, c) \notin \{a; b; c\}$, which is impossible by Lemma 4. □

Note. It is easy to see that every automorphism of an operation f is an automorphism of an arbitrary diagonal operation induced by f, i.e. the operation of the arity k defined by the term $f(x_{\gamma_1}, \ldots, x_{\gamma_n})$, where γ is a permutation of {1,...,n} on the set consisting of k indexes. Whence, the k-transitivity of the automorphism group of $(G; f)$ implies the k-transitivity of the automorphism group of each diagonal operation induced by f.

References

[1] **M. Hall**: *The group theory*, Moscou 1962.

[2] **A. P. Il'inykh**: *The classification of the finite groupoids with a 2-transitive automorphism group*, (Russian) Mat. Sbornik **185** (1994), 51 – 78.

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

[4] **F. Sokhatskyj, P. Syvakivskyj**: *On linear isotopes of cyclic groups*, Quasigroups and Related Systems **1** (1994), 66 – 76.

Department of Algebra
Vinnytsia State Pedagogical University
Vinnytsia 287100
Ukraine

Received 15 September 1997