Quasigroups and Related Systems **17** (2009), 205 – 228

Skew endomorphisms on some n-ary groups

Wieslaw A. Dudek and *Nikolay A. Shchuchkin*

Abstract. We characterize n-ary groups defined on a cyclic group and describe a group of their automorphisms induced by the skew operation. Finally, we consider splitting automorphisms.

1. Introduction

The idea of investigations of n*-ary groupoids*, i.e., algebras of the form (G, f), where G is a non-empty set and $f : G^n \to G$, $(n > 2)$, seems to be going back to E. Kasner's lecture [21] at the fifty-third annual meeting of the American Association for the Advancement of Science in 1904 where the subsets of groups closed under group multiplication of n elements are considered. But the first paper containing significant results on some n-ary groupoids, called now n*-ary groups*, was written (under inspiration of Emmy Noether) by W. Dörnte [2]. In this paper Dörnte observed that any n-ary groupoid (G, f) with the operation of the form $f(x_1, x_2, \ldots, x_n) = x_1 \circ x_2 \circ \ldots \circ x_n$, where $(G, \circ)$ is a group, is an n-ary group but for every $n > 2$ there are n-ary groups which are not of this form.

In recent years, n-ary operations find interesting applications in physics. For example, Y. Nambu [23] proposed in 1973 the generalization of classical Hamiltonian mechanics based on the Poisson bracket to the case when the new bracket, called the *Nambu bracket*, is an n-ary operation on classical observables. The author of [33] suspects that different n-ary structures such as n-Lie algebras, Lie ternary systems and linear spaces with additional internal n-ary operations, might clarify many important problems of modern mathematical physics (Yang-Baxter equation, Poisson-Lie groups, quantum

2000 Mathematics Subject Classification: 20N15, 08N05
Keywords: n-ary group, skew element, endomorphism, automorphism.
The second author wish to express their sincere thanks to Institute of Mathematics and Computer Science, Wroclaw University of Technology. The institute provided comfortable time to our joint research.

groups). For example, ternary $\mathbb{Z}_3$–graded algebras are important (cf. [22]) for their applications in physics of elementary interactions.

2. Preliminaries

An n-ary groupoid (G, f) is *solvable at the place* i if for all $a_1, ..., a_n, b \in G$ there exists $x_i \in G$ such that

$$f(a_1, ..., a_{i-1}, x_i, a_{i+1}, ..., a_n) = b\,. \tag{1}$$

If this solution is unique, we say that this groupoid is *uniquely* i*-solvable*. An n-ary groupoid which is uniquely i-solvable for every $i = 1, 2, \ldots, n$ is called an n*-ary quasigroup* or n*-quasigroup* (cf. [1]).

An n-ary groupoid (G, f) is called (i, j)*-associative* if

$$f(x_1, \ldots, x_{i-1}, f(x_i, \ldots, x_{n+i-1}), x_{n+i}, \ldots, x_{2n-1}) = f(x_1, \ldots, x_{j-1}, f(x_j, \ldots, x_{n+j-1}), x_{n+j}, \ldots, x_{2n-1})$$

holds for all $x_1, \ldots, x_{2n-1} \in G$. If this identity holds for all $1 \leqslant i < j \leqslant n$, then we say that the operation f is *associative* and (G, f) is called an n*-ary semigroup*. An associative n-ary quasigroup is called an n*-ary group*. Note that for $n = 2$ it is an arbitrary group.

It is worth to note that in the definition of an n-ary group, under the assumption of the associativity of the operation f, it suffices to postulate the existence of a solution of (1) at the places $i = 1$ and $i = n$ or at one place i other than 1 and n. Then one can prove uniqueness of the solution of (1) for all $i = 1, \ldots, n$ (cf. [25], p.213[17]).

Proposition 2.1. (Dudek, Głazek, Gleichgewicht, 1977)
An n-ary groupoid (G, f) is an n-ary group if and only if (at least) one of the following conditions is satisfied:

- (a) *the $(1, 2)$-associative law holds and the equation (1) is solvable for $i = n$ and uniquely solvable for $i = 1$,*
- (b) *the $(n-1, n)$-associative law holds and the equation (1) is solvable for $i = 1$ and uniquely solvable for $i = n$,*
- (c) *the $(i, i+1)$-associative law holds for some $i \in \{2, ..., n-2\}$ and the equation (1) is uniquely solvable for i and some $j > i$.* □

In some n-ary groups exists an element e (called a *neutral element*) such that

$$f(\underbrace{e,\ldots,e}_{i-1},x,\underbrace{e,\ldots,e}_{n-i})=x$$

for all $x\in G$ and for all $i=1,\ldots,n$. There are n-ary groups without neutral elements and n-ary groups with two, three and more neutral elements. The set of all neutral elements of a given n-ary group (if it is non-empty) forms an n-ary subgroup (cf. [9] or [16]).

Directly from the definition of an n-ary group (G,f) it follows that for every $x\in G$ there exists only one $z\in G$ satisfying the equation

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

This element is called *skew* to x and is denoted by $\overline{x}$.

One can prove (cf. [2]) that in any n-ary group (G,f) the following two identities are satisfied

$$f(y,\underbrace{x,\ldots,x}_{n-j-1},\bar{x},\underbrace{x,\ldots,x}_{j-1})=y \qquad (1\leqslant j\leqslant n-1) \tag{2}$$

$$f(\underbrace{x,\ldots,x}_{i-1},\bar{x},\underbrace{x,\ldots,x}_{n-i-1},y)=y \qquad (1\leqslant i\leqslant n-1) \tag{3}$$

Thus, in some sense, the skew element is a generalization of the inverse element in binary groups. In some n-ary groups we have $\overline{\overline{x}}=x$, but there are n-ary groups in which one fixed element is skew to all elements (see Theorem 2.3 below) and n-ary groups in which any element is skew to itself.

A very nice description of n-ary groups is given by the following theorem.

Theorem 2.2. (Hosszú, 1963)
An n-ary group (G,f), $n>2$, has the form

$$f(x_1,\ldots,x_n)=x_1\circ\varphi(x_2)\circ\varphi^2(x_3)\circ\varphi^3(x_4)\circ\ldots\circ\varphi^{n-1}(x_n)\circ b, \tag{4}$$

where $(G,\circ)$ is a some group, b – a fixed element of G, φ – an automorphism of $(G,\circ)$ such that $\varphi(b)=b$ and $\varphi^{n-1}(x)\circ b=b\circ x$ for every $x\in G$. □

In connection with this fact we say that any n-ary group (G,f) is (φ,b)-*derived* from some group $(G,\circ)$. In the case when φ is the identity mapping, we say that an n-ary group (G,f) is b-*derived* from $(G,\circ)$. If e is the identity of $(G,\circ)$, then an n-ary group e-derived from $(G,\circ)$ is called *reducible* to $(G,\circ)$ or *derived* from $(G,\circ)$. An n-ary group is reducible if and only if it contains at least one neutral element (cf. [2]).

One can prove (cf. for example [14] or [32]) that for a given n-ary group (G,f) the group $(G,\circ)$ from the above theorem is determined uniquely up to isomorphism and can be identified with the group $(G,\cdot) = ret_a(G,f)$, where $x\cdot y = f(x,a,\ldots,a,\overline{a},y)$. Fixing in an n-ary operation f arbitrary $n-2$ internal elements we obtain a new operation which depends only on two external elements. Choosing different sequences $a_2,\ldots,a_{n-1}$ we obtain different binary groupoids $(G,\diamond)$ of the form $x\diamond y = f(x,a_2,\ldots,a_{n-1},y)$. For a given n-ary group (G,f) all these groupoids are groups. Moreover, all these groups are isomorphic to the *retract* $ret_a(G,f)$.

An n-ary group having a commutative retract is called *semicommutative*. It satisfies the identity

$$f(x_1,x_2,\ldots,x_{n-1},x_n) = f(x_n,x_2,\ldots,x_{n-1},x_1).$$

An n-group (G,f) satisfying the identity

$$f(x_1,x_2,\ldots,x_n) = f(x_{\sigma(1)},x_{\sigma(2)},\ldots,x_{\sigma(n)}),$$

where σ is an arbitrary permutation of the set $\{1,2,\ldots,n\}$, is called *commutative*. In view of Theorem 2.2 any commutative n-ary group is b-derived from some abelian group.

An *n-ary power* of x in an n-ary group (G,f) is defined in the following way: $x^{<0>} = x$ and $x^{<k+1>} = f(x,\ldots,x,x^{<k>})$ for all $k>0$. $x^{<-k>}$ is an element z such that $f(x^{<k-1>},x,\ldots,x,z) = x^{<0>} = x$ (cf. [25]). Then $\overline{x} = x^{<-1>}$ and

$$f(x^{<k_1>},\ldots,x^{<k_n>}) = x^{<k_1+\ldots+k_n+1>} \tag{5}$$

$$(x^{<k>})^{<t>} = x^{<kt(n-1)+k+t>}. \tag{6}$$

The order of the smallest subgroup of (G,f) containing an element x of G is called the *n-ary order of* x and is denoted by $\mathrm{ord}_n(x)$. It is the smallest positive integer k such that $x^{<k>} = x$ (cf. [25]). If $\mathrm{ord}_n(x) = k$, then the smallest subgroup of (G,f) containing x has the form

$$\langle x\rangle = \{x,x^{<1>},x^{<2>},\ldots,x^{<k-1>}\}.$$

It is called *cyclic*. From (5) it follows that a cyclic n-ary group is commutative. A cyclic n-ary group of order k can be identified with the n-ary group $(\mathbb{Z}_k, f_1)$, where

$$f_1(x_1, \ldots, x_n) = (x_1 + x_2 + \ldots + x_n + 1)(\text{mod } k).$$

The n-ary group $(\mathbb{Z}_k, f_1)$ is generated by 0. In the case when all n-ary powers of x are different, we say that x has an infinite n-ary order. The smallest n-ary subgroup containing all these n-ary powers is called the *infinite cyclic n-ary group generated by* x. It is isomorphic to $(\mathbb{Z}, g_1)$, where

$$g_1(x_1, \ldots, x_n) = x_1 + x_2 + \ldots + x_n + 1. \tag{7}$$

This isomorphism has the form $h(x^{<s>}) = s$.

Observe also that according to Theorem 2.2 any cyclic n-ary group (G, f) generated by a can be considered as an n-ary group $a^{<1-n>}$-derived from a cyclic group $(G, *)$, where $x * y = f(x, a, \ldots, a, y)$. Then $\overline{a}$ is the identity of $(G, *)$ and $a^{<k>} = a^{k+1}$ in $(G, *)$, which means that $(G, *)$ and (G, f) are generated by the same element a.

Consider the sequence of elements: x, $\overline{x}$, $\overline{x}^{(2)}$, $\overline{x}^{(3)}, \ldots$, where $\overline{x}^{(k+1)}$ denotes the element skew to $\overline{x}^{(k)}$ and $\overline{x}^{(0)} = x$. All these elements belong to the same n-ary subgroup generated by x. Moreover, in view of (6) and $\overline{x} = x^{<-1>}$, we have

$$\overline{x}^{(2)} = (x^{<-1>})^{<-1>} = x^{<n-3>},$$
$$\overline{x}^{(3)} = (\,(x^{<-1>})^{<-1>})^{<-1>},$$

and so on. Generally: $\overline{x}^{(m)} = (\overline{x}^{(m-1)})^{<-1>}$ for all $m \geqslant 1$. This implies that

$$\overline{x}^{(m)} = x^{<S_m>} \quad \text{for} \quad S_m = -\sum_{i=0}^{m-1}(2-n)^i = \frac{(2-n)^m - 1}{n-1} \tag{8}$$

(cf. [6] and [10]). If $\text{ord}_n(x) = k$ is finite, then $\overline{x} = x^{<k-1>}$, $\overline{x}^{(2)} = x^{<n-3>}$, $\overline{x}^{(3)} = x^{<2-n>}$. Since $\overline{x}$ belongs to the n-ary subgroup generated by x, from Lagrange's theorem for finite n-ary groups (cf. [25], p.222), we obtain

$$\text{ord}_n(x) \geqslant \text{ord}_n(\overline{x}) \geqslant \text{ord}_n(\overline{x}^{(2)}) \geqslant \text{ord}_n(\overline{x}^{(3)}) \geqslant \ldots$$

In fact, $\text{ord}_n(\overline{x})$ is a divisor of $\text{ord}_n(x)$ (cf. [3]). Moreover, if $\text{ord}_n(x) < \infty$, then $\text{ord}_n(\overline{x}) = \text{ord}_n(x)$ if and only if $\text{ord}_n(x)$ and $n-2$ are relatively prime.

In this case $\operatorname{ord}_n(\overline{x}^{(s)}) = \operatorname{ord}_n(x)$ for every s. Thus $\lim\limits_{s\to\infty} \operatorname{ord}_n(\overline{x}^{(s)}) = 1$ if and only if $\operatorname{ord}_n(x)$ is a divisor of $n-2$ (cf. [3]). Obviously $\overline{x}^{(t)} \neq \overline{y}^{(t)}$ means that also $\overline{x}^{(s)} \neq \overline{y}^{(s)}$ for every $0 \leqslant s < t$.

Note by the way, that in some n-ary groups (described in [5] and [8]) we have $x^{<s>} = \overline{x}^{(n-s-1)}$. Such n-ary groups are the set-theoretic union of disjoint cyclic n-ary subgroups of order k isomorphic to the subgroup

$$\{x, \overline{x}, \overline{x}^{(2)}, \dots, \overline{x}^{(k-1)}\}.$$

The problem when one fixed element is skew to others was solved by the following theorem proved in [7].

Theorem 2.3. (Dudek, 1990)
$\overline{x} = \overline{y}$ for all elements x, y of an n-ary group (G, f) if and only if (G, f) is derived from a binary group of the exponent $t|n-2$. □

Generally, as it was observed in [28], from Theorem 2.2 it follows that $\overline{x} = \overline{y}$ if and only if the sequences $\underbrace{x, \dots, x}_{n-2}$ and $\underbrace{y, \dots, y}_{n-2}$ are equivalent in the sense of Post (cf. [25]).

3. Skew endomorphisms of n-ary groups

In [17] was proved that in semiabelian n-ary groups we have

$$\overline{f(x_1, \dots, x_n)} = f(\overline{x}_1, \dots, \overline{x}_n),$$

i.e., the operation $^- : x \to \overline{x}$ is an endomorphism. In this case also $h(x) = \overline{x}^{(s)}$ is an endomorphism for every $s \geqslant 0$. The converse is not true since, for example, in all ternary ($n = 3$) groups $\overline{\overline{x}} = x$ and $\overline{f(x, y, z)} = f(\overline{z}, \overline{y}, \overline{x})$ (cf. [2]). So, $h(x) = \overline{\overline{x}}$ is an endomorphism, but $^- : x \to \overline{x}$ is an endomorphism only for ternary groups satisfying the identity $f(x, y, z) = f(z, y, x)$.

This means that $h(x) = \overline{x}^{(s)}$ is an automorphism of semiabelian n-ary groups in which $\overline{x}^{(k)} = x$ holds for all $x \in G$ and some fixed k.

Any map of the form $h(x) = \overline{x}^{(s)}$, where $s > 0$, is called a skew map or a *skew endomorphism* if it is an endomorphism.

The natural question (posed in [6], see also [10]) is:

When $h(x) = \overline{x}$ is an endomorphism?

The first partial answer was given in [10]. The full, rather complicated, characterization of n-ary groups for which $h(x) = \overline{x}$ is an endomorphism is presented in [31]. It is based on two identities. Later it was proved that such n-ary groups can be characterized by one identity containing $n+2$ variables [27].

Below we present new characterizations of such n-ary groups .

Theorem 3.1. *The map $h(x)=\overline{x}^{(s)}$ is an automorphism of a cyclic n-ary group of order k if and only if k and $n-2$ are relatively prime.*

Proof. A cyclic n-ary group of order k is isomorphic to the n-ary group $(\mathbb{Z}_k, f_1)$ in which the skew element has the form $\overline{x}=((2-n)x-1)(\operatorname{mod} k)$. Since $(\mathbb{Z}_k, f_1)$ is commutative, $h(x)=\overline{x}^{(s)}$ is an endomorphism.

Assume that $h(x)=\overline{x}^{(s)}$ is an automorphism and $\gcd(k, n-2)=d$. Then $k=dv$ and $n-2=du$ for some u, v. Since

$$f_1(v,\ldots,v,\overline{0})=(n-2)v+v=duv+v=ku+v=v(\operatorname{mod} k),$$

we have $\overline{0}=\overline{v}$. Thus $h(k)=h(0)=\overline{0}^{(s)}=\overline{v}^{(s)}=h(v)$. Hence $k=v$ and $d=1$, i.e., k and $n-2$ are relatively prime.

Conversely, if k and $n-2$ are relatively prime, then $h(u)=h(v)$ implies $(2-n)^s(u-v)=0(\operatorname{mod} k)$. Hence $u=v$. So, $h(x)=\overline{x}^{(s)}$ is an automorphism. □

Corollary 3.2. *If each element of an n-ary group (G,f) has a finite n-ary order, then $h(x)=\overline{x}^{(s)}$ is a bijective map if and only if for every $x\in G$* $\gcd(\operatorname{ord}_n(x), n-2)=1$.

Proof. If $h(x)=\overline{x}^{(s)}$ is a bijection, then the restriction of h to an arbitrary cyclic n-ary subgroup $\langle a\rangle$ of (G,f) is an automorphism. Hence, by Theorem 3.1, $\operatorname{ord}_n(a)$ and $n-2$ are relatively prime.

Conversely, let $\overline{a}^{(s)}=\overline{c}^{(s)}$ for some $a,c\in G$. If $\operatorname{ord}_n(a)=k<\infty$ and $n-2$ are relatively prime, then $\operatorname{ord}_n(a)=\operatorname{ord}_n(\overline{a})=\operatorname{ord}_n(\overline{a}^{(s)})=\operatorname{ord}_n(\overline{c}^{(s)})=\operatorname{ord}_n(\overline{c})$ and $\langle a\rangle=\langle\overline{a}\rangle=\langle\overline{a}^{(s)}\rangle=\langle\overline{c}^{(s)}\rangle=\langle\overline{c}\rangle=\langle c\rangle$ since $\overline{x}^{(t)}\in\langle x\rangle$ for every t. Thus $c=a^{<m>}$ for some $0<m\leqslant k$. Hence, by (8), for some S we have $\overline{c}^{(s)}=c^{<S>}=(a^{<m>})^{<S>}=(a^{<S>})^{<m>}=(\overline{a}^{(s)})^{<m>}=(\overline{c}^{(s)})^{<m>}$, which implies $m=k$. So, $c=a^{<k>}=a$. This proves that $h(x)=\overline{x}^{(s)}$ is a bijection. □

Corollary 3.3. *If each element of a semiabelin n-ary group (G,f) has finite n-ary order, then the skew map $h(x)=\overline{x}^{(s)}$ is an automorphism of (G,f) if and only if* $\gcd(\operatorname{ord}_n(x), n-2)=1$ *for every $x\in G$.* □

Corollary 3.4. *The skew map $h(x)=\overline{x}^{(s)}$ is an automorphism of a semiabelian n-ary group of finite order k if and only if k and $n-2$ are relatively prime.* □

Corollary 3.5. *For $n>3$ an n-ary group b-derived from an infinite cyclic group has no non-trivial skew endomorphisms.*

Proof. Let (G,f) be an n-ary group b-derived from a cyclic group generated by a. Then $b=a^t$ for some t and $\overline{a^m}^{(s)}=a^{m(2-n)^s+T}$ for every $a^m\in\langle a\rangle$, where $T=-t(2-n)^{s-1}-t(2-n)^{s-2}-\ldots-t$. So, if $h(x)=\overline{x}^{(s)}$ is a non-trivial automorphism, then for every $a^p\in\langle a\rangle$ there exists $a^m\in\langle a\rangle$ such that $a^p=h(a^m)$. In particular, for a^{1+T} there exists a^k such that $a^{1+T}=h(a^k)=a^{k(2-n)^s+T}$, which implies $1=k(2-n)^s$. Thus $n=3$. So, for $n>3$ no non-trivial skew endomorphisms. □

A ternary group b-derived from an infinite cyclic group has a non-trivial skew endomorphism. Indeed, in such ternary groups $x\neq\overline{x}$, $x=\overline{\overline{x}}$ and $\overline{f(x,y,z)}=f(\overline{z},\overline{y},\overline{x})=f(\overline{x},\overline{y},\overline{z})$ (cf. [2]). So, $h(x)=\overline{x}$ is a non-trivial skew automorphism of this group.

All n-ary groups b-derived from finite cyclic groups have non-trivial skew endomorphisms since, as it is not difficult to see, $h(x)=\overline{x}=x^{2-n}b^{-1}$ is such endomorphism.

4. Precyclic n-ary groups

In this section we describe n-ary groups (φ,b)-derived from cyclic groups. Such n-ary groups are called *semicyclic* or *precyclic*.

An infinite cyclic group has only two automorphisms: $\varphi(x)=x$ and $\varphi(x)=x^{-1}$. Hence, according to Theorem 2.2, on an infinite group $\langle a\rangle$ we can define two types of n-ary groups. The operation of an n-ary group of the first type is induced by the identity automorphism $\varphi(x)=x$ and has the form

$$f(a^{s_1},a^{s_2},a^{s_3},\ldots,a^{s_{n-1}},a^{s_n})=a^{s_1+s_2+s_3+\ldots+s_{n-1}+s_n+l}. \tag{9}$$

The operation of an n-ary group of the second type is induced by the automorphism $\varphi(x)=x^{-1}$. Since, by Theorem 2.2, $\varphi^{n-1}(x)=x$ for all $x\in\langle a\rangle$, n must be odd. Moreover, in this case for $b=a^l$ should be $\varphi(a^l)=a^l$, which means that b must be the identity of $\langle a\rangle$. Thus, in this case

$$f(a^{s_1},a^{s_2},a^{s_3},\ldots,a^{s_{n-1}},a^{s_n})=a^{s_1-s_2+s_3-s_4+\ldots-s_{n-1}+s_n}, \tag{10}$$

where n is odd.

In the first case we say that this n-ary group id $(1,l)$-*derived* from an infinite cyclic group, in the second case that it is $(-1,0)$-*derived*.

Now, consider n-ary groups (φ,b)-derived from finite cyclic groups. Automorphisms of a cyclic group of order $2<k<\infty$ have the form $\varphi(x)=x^m$, where $0<m<k$ and $\gcd(m,k)=1$. So, the operation of an n-ary group defined on a cyclic group $\langle a\rangle$ of order k has the form

$$f(a^{s_1},a^{s_2},\ldots,a^{s_{n-1}},a^{s_n})=a^{s_1+ms_2+m^2s_3+m^3s_4+\ldots+m^{n-2}s_{n-1}+s_n+l}, \quad (11)$$

where $0<m<k$, $\gcd(m,k)=1$, $m^{n-1}=1(\operatorname{mod} k)$, $0\leqslant l<k$ and $lm\equiv l(\operatorname{mod} k)$. We say that such n-ary group is (m,l)-*derived* from a finite cyclic group of order k.

It is clear that n-ary groups (φ,b)-derived from the same group may be isomorphic. The answer to the question when two n-ary groups (φ,b)-derived fom cyclic groups of the same order are isomorphic can be deduced from the existence of some special isomorphisms of their retracts (cf. [15] or [12]) or from the following theorem proved in [14].

Theorem 4.1. (Dudek, Michalski, 1982)
Let an n-ary group (A,f) be (φ,a)-derived from a group $(A,\cdot)$ and an n-ary group (B,g) be (ψ,b)-derived from a group $(B,\circ)$. Then (A,f) and (B,g) are isomorphic if and only if there exists an isomorphism $\beta:(A,\cdot)\to(B,\circ)$ of groups and an element $c\in B$ such that

$$\beta(a)=c\circ\psi(c)\circ\ldots\circ\psi^{n-2}(c)\circ b \quad \text{and} \quad \beta(\varphi(x))\circ c=c\circ\psi(\beta(x))$$

for all $x\in A$. □

As a consequence of the above theorem we obtain two important characterizations of n-ary groups defined on the same infinite cyclic group.

Corollary 4.2. *Two n-ary groups $(1,l_1)$ and $(1,l_2)$-derived from the additive group $(\mathbb{Z},+)$ are isomorphic if and only if $l_1\equiv l_2(\operatorname{mod}(n-1))$ or $l_1\equiv -l_2(\operatorname{mod}(n-1))$.* □

Corollary 4.3. *On an infinite cyclic group one can defined $[\frac{n-1}{2}]$ non-isomorphic commutative n-ary groups. Each such n-ary group is isomorphic to one of the n-ary groups $(1,l)$-derived $(0\leqslant l\leqslant\frac{n-1}{2})$ from the group $(\mathbb{Z},+)$.* □

Below, for the simplicity of formulations of our results for n-ary groups (m,l)-derived from finite cyclic groups, by $S(m)$ we will denote the sum $1+m+m^2+\ldots+m^{n-2}$.

We start from one arithmetical lemma. The proof of this lemma is analogous to the proof of Lemma A in [18].

Lemma 4.4. *Let* $0<l_1,l_2,m<k$. *Then for* $k,n>2$ *the congruence*

$$xl_1\equiv(yS(m)+l_2)(\operatorname{mod}k),$$

where $\gcd(m,k)=1$*, has a solution in* x *and* y *if and only if*

$$\gcd(l_1,S(m),k)=\gcd(l_2,S(m),k). \qquad \square$$

Using this lemma and Theorem 4.1 we can prove

Theorem 4.5. *Two* n*-ary groups* (m_1,l_1) *and* (m_2,l_2)*-derived from a cyclic group of a finite order* k *are isomorphic if and only if*

$$gcd(l_1,S(m_1),k)=gcd(l_2,S(m_2),k)\ \text{ and }\ m_1=m_2. \qquad \square$$

Corollary 4.6. *Any* k*-element* n*-ary group defined on a cyclic group is isomorphic to one of the* n*-ary groups* (m,l)*-derived from the group* $(\mathbb{Z}_k,+)$*, where* l *is a divisor of* $gcd(S(m),k)$*.* $\square$

Proposition 4.7. *For* $n>3$*, a precyclic* n*-ary group has a non-trivial skew endomorphism if and only if it is finite and non-idempotent.*

Proof. A precyclic n-ary group is semiabelian, hence $h(x)=\overline{x}$ is its skew endomorphism. It is non-trivial only in the case when an n-ary group is non-idempotent.

If a precyclic n-ary group is infinite, then its operation f is defined by (9) or (10). In the first case it is commutative. Hence, by Corollary 3.5, for $n>3$ it has no non-trivial skew endomorphism. In the second case it is idempotent and has only trivial skew endomorphism. $\square$

Any ternary non-idempotent group has a non-trivial skew endomorphism. Since in ternary groups $\overline{\overline{x}}=x$, a skew endomorphism is an automorphism. An infinite precyclic n-ary group has no non-trivial skew automorphisms.

Corollary 4.8. *A skew endomorphism of a precyclic* n*-ary group of a finite order* k *is its automorphism if and only if* $gcd(n-2,k)=1$*.*

Proof. It follows from Corollary 3.4. $\square$

5. Subgroups of n-ary precyclic groups

It is not difficult to verify that in an n-ary group (G,f) which is (m,l)-derived from a finite cyclic group $\langle a\rangle$, each coset $a^r\langle a^v\rangle$ of $\langle a\rangle$, where $rS(m)+l\equiv 0(\operatorname{mod} v)$, is an n-ary subgroup of (G,f). But not all n-ary subgroups of (G,f) are of this form. For example, in a 5-ary group $(1,0)$-derived from a cyclic group $\langle a\rangle$ of order 4 two 5-ary subgroups $S_0=\{a^0,a^2\}$ and $S_1=\{a^1,a^3\}$ are cosets of $\langle a\rangle$ with respect to S_0. Subgroups $\{a^0\}$, $\{a^1\}$, $\{a^2\}$, $\{a^3\}$ are cosets of $\langle a\rangle$ with respect to $\{a^0\}$ but not with respect to S_0.

Obviously, each n-ary subgroup of an n-ary group (G,f) is a subgroup of some retract of (G,f). Indeed, if H is an n-ary subgroup of an n-ary group (G,f), then $ret_a(H,f)$ is a subgroup of $ret_a(G,f)$ for every $a\in H$. This means that any n-ary subgroup of a precyclic n-ary group $(\langle a\rangle,f)$ is normal subgroup of some cyclic group isomorphic to $\langle a\rangle$.

In any precyclic n-ary group (G,f) the map $h(x)=\overline{x}$ is an endomorphism. So, $h(G)=G^{(1)}=\{\overline{x}\,|\,x\in G\}$ is an n-ary subgroup of (G,f). Also $h^2(G)=G^{(2)}=\{\overline{\overline{x}}\,|\,x\in G\}$ is an n-ary subgroup of (G,f). In this way we obtain the sequence of n-ary subgroups

$$G\supseteq G^{(1)}\supseteq G^{(2)}\supseteq G^{(3)}\supseteq\ldots$$

In finite n-ary groups $G^{(k)}=G^{(k+1)}=\ldots$ for some natural k, but there are n-ary groups for which $G^{(k)}\neq G^{(k+1)}$ for all k. Moreover, $G^{(1)}$ is an n-ary subgroup also in some n-ary groups for which $h(x)=\overline{x}$ is not an endomorphism. For example, in a 4-ary group (G,f) derived from the symmetric group $\mathbb{S}_3$ we have $\overline{x}=x$ for $x^3=e$ and $\overline{x}=e$ for $x^2=e$. Thus $G^{(1)}=\mathbb{A}_3$ is a subgroup of (G,f) but $h(x)=\overline{x}$ is not an endomorphism of (G,f) because $\overline{f(y,z,y,z)}\neq f(\overline{y},\overline{z},\overline{y},\overline{z})$ for $y=(1\,2)$ and $z=(1\,2\,3)$.

The list of unsolved problems connected with $G^{(k)}$ one can find in [6] and [10].

If $h(x)=\overline{x}$ is an endomorphism of (G,f), then the relation

$$x\rho y\Longleftrightarrow\overline{x}=\overline{y}\qquad(12)$$

is a congruence on (G,f). We say that this relation is *determined by the skew endomorphism*. Obviously, ρ is a congruence on any precyclic n-ary group.

It is not difficult to see that a congruence τ of an n-ary group (G,f) is a congruence of its retract $ret_a(G,f)$. The converse is not true. A congruence θ of a group $(G,\circ)$ is a congruence of an n-ary group (φ,b)-derived from

$(G, \circ)$ only in the case when for all $x, y \in G$ from $x\theta y$ it follows $\varphi(x)\theta\varphi(y)$, or equivalently, if $\varphi(H) \subseteq H$ for a normal subgroup H of $(G, \circ)$ determining θ. Thus, a relation θ defined on an n-ary group (G, f) b-derived from a group $(G, \circ)$ is a congruence if and only if it is a congruence on $(G, \circ)$. The similar result is valid for precyclic n-ary group since for any automorphism φ and any subgroup $\langle a^m \rangle$ of a cyclic group $\langle a \rangle$ holds $\varphi(\langle a^m \rangle) \subseteq \langle a^m \rangle$.

Thus we have proved

Proposition 5.1. *A relation θ defined on a precyclic group is a congruence if and only if it is a congruence of the corresponding cyclic group.* □

For relation defined by (12) we have stronger result.

Proposition 5.2. *On an n-ary group (m, l)-derived from a cyclic group $\langle a \rangle$ of order k the relation ρ determined by its skew endomorphism is a congruence which coincides with the congruence on $\langle a \rangle$ induced by the subgroup $\langle a^{\frac{k}{d}} \rangle$, where $d = gcd(S(m) - 1, k)$. In this case, the class $[a^s]_\rho$ coincides with the coset $a^s \langle a^{\frac{k}{d}} \rangle$.*

Proof. At first we consider the case $m = 1$. In this case $d = gcd(n-2, k)$, i.e., $n - 2 = dd_1$ and $k = dk_1$ for some natural d_1, k_1 such that $gcd(d_1, k_1) = 1$. Since an n-ary group (G, f) is $(1, l)$-derived from a cyclic group $\langle a \rangle$ of order k, we have $\overline{a^s} = a^{s(2-n)-l}$ for every $a^s \in \langle a \rangle$. Thus $a^{s_1} \rho\, a^{s_2}$ if and only if $s_1(n - 2) \equiv s_2(n - 2)(\bmod\, k)$, i.e., if and only if $s_1 dd_1 \equiv s_2 dd_1 (\bmod\, dk_1)$. This is equivalent to $s_1 d_1 \equiv s_2 d_1 (\bmod\, k_1)$. In view of $gcd(d_1, k_1) = 1$, the last congruence means that $s_1 \equiv s_2 (\bmod\, \frac{k}{d})$. So, $a^{s_1} \rho\, a^{s_2}$ if and only if $a^{s_1 - s_2} \in \langle a^{\frac{k}{d}} \rangle$.

Now let $m \neq 1$, $gcd(m, k) = 1$ and $d = gcd(S(m) - 1, k)$. Then $a^{s_1} \rho\, a^{s_2}$ if and only if $s_1(S(m) - 1) \equiv s_2(S(m) - 1)(\bmod\, k)$, i.e., if and only if $s_1 \frac{m^{n-2}-1}{m-1} \equiv s_2 \frac{m^{n-2}-1}{m-1}$ (mod k). Since $S(m) - 1 = m \frac{m^{n-2}-1}{m-1} = mdm_1$ and $k = dk_1$, where $gcd(m_1, k_1) = 1$. The last congruence, similarly as in the first part of this proof, means that $s_1 \equiv s_2 (\bmod\, \frac{k}{d})$. So, $a^{s_1} \rho\, a^{s_2}$ if and only if $a^{s_1 - s_2} \in \langle a^{\frac{k}{d}} \rangle$. □

As is well known in binary groups one equivalence class of any congruence is a subgroup. This class coincides with a normal subgroup determining this congruence. For n-ary group it is not true. In a ternary group 1-derived from the additive group $\mathbb{Z}_2$ the congruence ρ defined by (12) has two equivalence classes: $[0]_\rho$ and $[1]_\rho$. These classes are not ternary subgroups. But the same congruence defined on a ternary group 2-derived from the group $\mathbb{Z}_4$ has two classes which are not ternary subgroups and two classes which are ternary subgroups. So, the natural question is: *how many* (*and which*) *the classes are n-ary subgroups*. For precyclic n-ary groups the answer is given by the following theorem.

Theorem 5.3. *Let $(\langle a\rangle, f)$ be an n-ary group (m,l)-derived from a cyclic group $\langle a\rangle$ of order k. If $gcd(S(m),k)$ divides l, then the congruence determined by the skew endomorphism of $(\langle a\rangle, f)$ has exactly $gcd(S(m),k)$ equivalence classes which are n-ary subgroups. These classes are defined by elements a^s, where $sS(m)\equiv 0(\text{mod}\frac{k}{gcd(S(m)-1,k)})$. In the case $gcd(S(m),k)\nmid l$ no such classes.*

Proof. According to Proposition 5.2, in an n-ary group (m,l)-derived from a cyclic group $\langle a\rangle$ of order k the equivalence class $[a^s]_\rho$ coincides with the coset $a^s\langle a^{\frac{k}{d}}\rangle$, where $d = gcd(S(m)-1,k)$. As it is easy to see, this coset is an n-ary subgroup only in the case when

$$sS(m)+l\equiv 0(\text{mod}\frac{k}{d}). \tag{13}$$

At first we consider the case when $m = 1$. In this case $S(m) = n-1$ and (13) has the form

$$s(n-1)+l\equiv 0(\text{mod}\frac{k}{d}), \tag{14}$$

where $d = gcd(n-2,k)$.

Since $n-1$ and $n-2$ are relatively prime, $gcd(n-1,k) = gcd(n-1,\frac{k}{d})$. Thus $gcd(n-1,k)$ is a divisor of $n-1$ and $\frac{k}{d}$. This together with (14) proves that $gcd(n-1,k)$ is a divisor of l. So, $gcd(l,n-1,k) = gcd(0,n-1,k)$. Hence, by Theorem 4.5, this n-ary group is isomorphic to the n-ary group $(1,0)$-derived from a cyclic group $\langle a\rangle$ of order k. But in the last n-ary group the equivalence class $[a^s]_\rho$ is an n-ary subgroup only in the case when $s(n-1)\equiv 0(\text{mod}\frac{k}{d})$.

Since $gcd(n-1,n-2) = 1$, the equation $x(n-1)\equiv 0(\text{mod}\frac{k}{d})$ has $gcd(n-1,k)$ solutions. So, exactly $gcd(n-1,k)$ classes of the form $[a^s]_\rho$ are n-ary subgroups. In the case $gcd(n-1,k)\nmid l$ no s satisfying (14).

This completes the proof for $m = 1$.

Now let $m\neq 1$. In this case we have $gcd(S(m),k) = gcd(S(m),\frac{k}{d})$, where $d = gcd(S(m)-1,k)$. Indeed, since $k = dk_1$, for any common divisor

$p>1$ of $S(m)=\frac{m^{n-1}-1}{m-1}$ and k, in view of $gcd(m,k)=1$,

$$S(m)-1=m\frac{m^{n-2}-1}{m-1} \quad \text{and} \quad S(m)=\frac{m^{n-2}-1}{m-1}+m^{n-2},$$

from $p|d$ it follows $p|\frac{m^{n-2}-1}{m-1}$. Hence $p|m$ which is a contradiction because $gcd(m,k)=1$. Thus $p\nmid d$, i.e., $p|k_1=\frac{k}{q}$. So, $gcd(S(m),k)=gcd(S(m),\frac{k}{q})$.

If $gcd(S(m),k)|l$, then, according to Theorem 4.5, an n-ary group (m,l)-derived from a cyclic group of order k is isomorphic to some n-ary group $(m,0)$-derived from this group. In this n-ary group the class $[a^s]_\rho$ is an n-ary subgroup only in the case when $sS(m)\equiv 0(\mathrm{mod}\frac{k}{d})$.

Further argumentation is similar to the argumentation used in the first part of this proof. □

Corollary 5.4. *If an n-ary group (G,f) is (m,l)-derived from a cyclic group $\langle a\rangle$ of order k, then the image of G under the skew endomorphism $h(x)=\overline{x}$ of (G,f) coincides with the coset $a^{-l}\langle a^d\rangle$ of $\langle a\rangle$, where $d=gcd(S(m)-1,k)$.*

Proof. Indeed, $h(G)=\{\overline{a^s}\mid a^s\in\langle a\rangle\}=\{a^{-l-s(S(m)-1)}\}=a^{-l}\langle a^d\rangle$, where $d=gcd(S(m)-1,k)$. □

6. Automorphisms of precyclic n-ary groups

Theorem 6.1. *Any endomorphism ψ of a precyclic n-ary group $(\langle a\rangle,f)$ can be presented in the form $\psi(x)=\varphi(x)a^t$, where φ is an endomorphism of a group $\langle a\rangle$ and $a^t=\psi(e)$.*

Proof. Let $\varphi(x)=\psi(x)a^{-t}$, where $a^t=\psi(e)$. Since ψ is an endomorphism of n-ary group (m,l)-derived from a cyclic group $\langle a\rangle$, we have $\psi(\overline{x})=\overline{\psi(x)}$ for every $x\in\langle a\rangle$ and $\overline{e}=\overline{a^0}=a^{-l}$. Thus $\psi(\overline{e})=\psi(a^{-l})=a^{-(n-2)t-l}$ for $m=1$, and $\psi(a^{-l})=a^{-\frac{m(m^{n-2}-1)}{m-1}t-l}$ for $m\neq 1$. Hence in the case $m=1$ for all a^{s_1}, $a^{s_2}\in\langle a\rangle$ we have

$$\begin{aligned}\varphi(a^{s_1}a^{s_2})&=\psi(a^{s_1}a^{s_2})a^{-t}=\psi(f(a^{s_1},e,\ldots,e,\overline{e},a^{s_2}))a^{-t}\\&=f(\psi(a^{s_1}),\psi(e),\ldots,\psi(e),\psi(\overline{e}),\psi(a^{s_2}))a^{-t}\\&=f(\psi(a^{s_1}),a^t,\ldots,a^t,a^{-(n-2)t-l},\psi(a^{s_2}))a^{-t}\\&=\psi(a^{s_1})a^{-t}\psi(a^{s_2})a^{-t}=\varphi(a^{s_1})\varphi(a^{s_2}),\end{aligned}$$

which proves that φ is an endomorphism of $\langle a\rangle$.

For $m \neq 1$ the proof is analogous. Similarly for infinite precyclic n-ary groups. □

Since in the above theorem ψ is bijective if and only if φ is bijective, we obtain

Corollary 6.2. *If ψ is an automorphism of a precyclic n-ary group $(\langle a\rangle, f)$, then $\varphi(x) = \psi(x)a^{-t}$ with $a^t = \psi(e)$, is an automorphism of a group $\langle a\rangle$.* □

Theorem 6.3. *If $\varphi(x) = x^w$ is an automorphism of a cyclic group $\langle a\rangle$ of order k, then $\psi(x) = \varphi(x)a^t$ is an automorphism of an n-ary group $(\langle a\rangle, f)$ (m, l)-derived from $\langle a\rangle$ if and only if $tS(m) \equiv l(w-1)(\mathrm{mod}\, k)$.*

Proof. The map ψ is a bijection because φ is an automorphism of $\langle a\rangle$. We prove that ψ is an endomorphism of an n-ary group $(\langle a\rangle, f)$.

Since $(\langle a\rangle, f)$ is (m, l)-derived from $\langle a\rangle$, for $\psi(x) = \varphi(x)a^t$ and $m \neq 1$ we obtain

$$\psi(f(a^{s_1}, \ldots, a^{s_n})) = \psi(a^{s_1+ms_2+\ldots+m^{n-2}s_{n-1}+s_n+l}) =$$
$$= a^{w(s_1+ms_2+\ldots+m^{n-2}s_{n-1}+s_n+l)+t} = a^{ws_1+wms_2+\ldots+wm^{n-2}s_{n-1}+ws_n+t}a^{wl}$$

and

$$f(\psi(a^{s_1}), \ldots, \psi(a^{s_n})) = a^{ws_1+t}a^{m(ws_2+t)} \ldots a^{m^{n-2}(ws_{n-1}+t)}a^{ws_n+t}a^l$$
$$= a^{ws_1+wms_2+\ldots+wm^{n-2}s_{n-1}+ws_n+t}a^{t(1+m+\ldots+m^{n-2})+l}.$$

This means that ψ is an endomorphism of an n-ary group $(\langle a\rangle, f)$ if and only if $wl \equiv (t(1+m+\ldots+m^{n-2})+l)(\mathrm{mod}\, k)$, i.e., if and only if $tS(m) \equiv l(w-1)(\mathrm{mod}\, k)$.

For $m = 1$ the proof is analogous. □

Corollary 6.4. *Any automorphism ψ of an n-ary group (m, l)-derived from a cyclic group $\langle a\rangle$ of order k can be presented in the form $\psi(a^s) = a^{ws+t}$, where $gcd(w, k) = 1$ and $tS(m) \equiv l(w-1)(\mathrm{mod}\, k)$.*

Proof. Let ψ be an arbitrary automorphism of an n-ary group (m, l)-derived from a cyclic group $\langle a\rangle$ of order k. Then, according to Theorem 6.1, the map $\varphi : a^s \to \psi(a^s)a^{-t}$, where $\psi(e) = a^t$, is an automorphism of $\langle a\rangle$. Thus $\psi(a^s) = \varphi(a^s)a^t = a^{ws+t}$ for some w relatively prime to k and $tS(m) \equiv l(w-1)(\mathrm{mod}\, k)$. □

This means that any automorphism of an n-ary group (m, l)-derived from a finite cyclic group is uniquely determined by two numbers: w and t. Hence, it will be denoted by $\psi_{w,t}$.

Corollary 4.6 shows that each precyclic n-ary group of order k is isomorphic to some n-ary group (m,l)-derived from the group $\mathbb{Z}_k$, where l is a divisor of $d=gcd(S(m),k)$. For such defined l and d

$$A^*_{d/l}=\{w\in\mathbb{Z}^*_k\,|\,w\equiv 1(\mathrm{mod}\,\frac{d}{l})\}$$

is a subgroup of the multiplicative group $\mathbb{Z}^*_k$ of the ring $(\mathbb{Z}_k,+,\cdot)$.

We use this subgroup to the description of the automorphism group of finite precyclic n-ary groups.

Theorem 6.5. *The automorphism group of an n-ary group (m,l)-derived from a cyclic group of order k is isomorphic to the extension of a cyclic group of order $\frac{k}{d}$, where $d=gcd(S(m),k)$, by the multiplicative group $A^*_{d/l}$.*

Proof. Let $(\langle a\rangle,f)$ be an n-ary group (m,l)-derived from a cyclic group $\langle a\rangle$ of order k. Then $\langle a^{\frac{k}{d}}\rangle$, where $d=gcd(S(m),k)$, is a group of order d contained in $\langle a\rangle$.

Consider the homomorphism $\zeta: A^*_{d/l}\to Aut\langle a^{\frac{k}{d}}\rangle$ such that $\zeta(w)=\varphi_r$, where r is the remainder of w after dividing by d. In this way, we obtain the extension $A^*_{d/l}\,\langle a^{\frac{k}{d}}\rangle$ of the group $\langle a^{\frac{k}{d}}\rangle$ by the group $A^*_{d/l}$ (see for example [19]) with the group operation

$$w_1a^{v_1\frac{k}{d}}\cdot w_2a^{v_2\frac{k}{d}}=(w_1w_2)a^{(w_2v_1+v_2)\frac{k}{d}}. \tag{15}$$

The map $\tau: Aut(\langle a\rangle,f)\to A^*_{d/l}\,\langle a^{\frac{k}{d}}\rangle$, where $\tau(\psi_{w,v})=wa^{v\frac{k}{d}}$, is a bijection. Moreover, for $\psi_{w_1,v_1},\psi_{w_2,v_2}\in Aut(\langle a\rangle,f)$ and $a^s\in\langle a\rangle$ we have

$$\begin{aligned}\psi_{w_1,v_1}\circ\psi_{w_2,v_2}(a^s)&=\psi_{w_2,v_2}(\psi_{w_1,v_1}(a^s))=\psi_{w_2,v_2}(a^{sw_1+t_1})\\&=a^{(sw_1+t_1)w_2+t_2}=a^{sw_1w_2+t_1w_2+t_2}\\&=a^{sw_1w_2+(t_1'w_2+t_2')+(w_2v_1+v_2)\frac{k}{d}}\\&=\psi_{w_1w_2,w_2v_1+v_2}(a^s),\end{aligned}$$

for $t_1=t_1'+v_1\frac{k}{d}$, $t_2=t_2'+v_2\frac{k}{d}$ and $(t_1'w_2+t_2')\frac{S(m)}{d}\equiv\frac{l(w_1w_2-1)}{d}(\mathrm{mod}\frac{k}{d})$. Thus

$$\psi_{w_1,v_1}\circ\psi_{w_2,v_2}=\psi_{w_1w_2,w_2v_1+v_2}.$$

This together with (15), implies

$$\tau(\psi_{w_1,v_1}\circ\psi_{w_2,v_2})=(w_1w_2)a^{(w_2v_1+v_2)\frac{k}{d}}=\tau(\psi_{w_1,v_1})\cdot\tau(\psi_{w_2,v_2}).$$

So, τ is an isomorphism. Therefore $Aut(\langle a\rangle,f)\cong A^*_{d/l}\,\langle a^{\frac{k}{d}}\rangle$. □

Corollary 6.6. *The automorphism group of a cyclic n-ary group of a finite order k is isomorphic to the direct sum $A_d^* \bigoplus \langle a^{\frac{k}{d}} \rangle$, where $d = gcd(n-1, k)$.*

Proof. Any cyclic n-ary group of order $k < \infty$ can be identified with $(\mathbb{Z}_k, f_1)$. So, it is $(1,1)$-derived from $\mathbb{Z}_k$. Its automorphism group is isomorphic to $A_d^* \langle a^{\frac{k}{d}} \rangle$, where $d = gcd(n-1, k)$ and $A_d^* = \{w \in \mathbb{Z}_k^* \,|\, w \equiv 1 (\mathrm{mod}\, d)\}$.

Since A_d^* and $\langle a^{\frac{k}{d}} \rangle$ are subgroups of $A_d^* \langle a^{\frac{k}{d}} \rangle$ which can be identified with $A_d^* \times \langle a^0 \rangle$ and $\{1\} \times \langle a^{\frac{k}{d}} \rangle$, respectively, and $1a^{v\frac{k}{d}} \cdot wa^{0\frac{k}{d}} = wa^{0\frac{k}{d}} \cdot 1a^{v\frac{k}{d}}$ for all $w \in A_d^*$, $a^{v\frac{k}{d}} \in \langle a^{\frac{k}{d}} \rangle$ we obtain $A_d^* \langle a^{\frac{k}{d}} \rangle \cong A_d^* \bigoplus \langle a^{\frac{k}{d}} \rangle$. □

Corollary 6.7. *The automorphism group of a cyclic n-ary group of a prime order p is isomorphic to $\mathbb{Z}_p^*$ or to $\mathbb{Z}_p^* \times \mathbb{Z}_p$.*

Proof. In this case $d = 1$ or $d = p$. If $d = 1$, then $A_d^* = \mathbb{Z}_p^*$ and $\langle a^{\frac{p}{d}} \rangle = \{a^0\}$. Thus, $A_d^* \langle a^{\frac{k}{d}} \rangle \cong \mathbb{Z}_p^*$. For $d = p$ we obtain $A_d^* = \mathbb{Z}_p^*$ and $\langle a^{\frac{p}{d}} \rangle = \langle a \rangle \cong \mathbb{Z}_p$. Hence $A_d^* \langle a^{\frac{k}{d}} \rangle \cong \mathbb{Z}_p^* \times \mathbb{Z}_p$. □

Corollary 6.8. *If $S(m)$ and k are relatively prime, then the automorphism group of an n-ary group $(m,1)$-derived from a cyclic group of order k is isomorphic to the multiplicative group $\mathbb{Z}_k^*$.*

Proof. Indeed, in this case $d = gcd(S(m), k) = 1$, $A_{d/l}^* = \mathbb{Z}_k^*$ and $\langle a^{\frac{k}{d}} \rangle = \langle a^k \rangle = \{a^0\}$. Hence $A_{d/l}^* \langle a^{\frac{k}{d}} \rangle = A_{d/l}^* = \mathbb{Z}_k^*$. □

Theorem 6.9. *A commutative precyclic n-ary group of infinite order has at most two automorphisms.*

Proof. Any infinite precyclic n-ary group is isomorphic to some n-ary group (m,l)-derived from the additive group $\mathbb{Z}$ of all integers. If it is commutative, then, by Corollary 4.3, there exists $0 \leqslant l \leqslant \left[\frac{n-1}{2}\right]$ for which this n-ary group is isomorphic to an n-ary group $(1,l)$-derived from the group $\mathbb{Z}$. But, by Theorem 6.1, for any automorphism ψ of an n-ary group $(1,l)$- derived from the group $\mathbb{Z}$ the map $\varphi(x) = \psi(x) - t$, where $t = \psi(0)$, is an automorphism of $(\mathbb{Z}, +)$. Thus $\psi(x) = x + t$ or $\psi(x) = -x + t$.

Let $\psi(x) = x + t$. Then $\psi(f(0,\ldots,0)) = l + t$ and $f(\psi(0),\ldots,\psi(0)) = nt + l$, which implies $l + t = l + nt$. Thus $t = 0$. Hence $\psi(x) = x$.

In the case $\psi(x) = -x + t$ we obtain $\psi(f(0,\ldots,0)) = -l + t$ and $f(\psi(0),\ldots,\psi(0)) = nt + l$. Thus $\frac{n-1}{2}(-t) = l$. If $l = 0$, then also $t = 0$. So, an n-ary group $(1,0)$-derived from the group $\mathbb{Z}$ has two automorphisms: $\psi(x) = x$ and $\psi(x) = -x$.

If $l = \frac{n-1}{2}$ (in this case n must be odd), then $t = -1$. This means that an n-ary group $(1, \frac{n-1}{2})$-derived from the group $\mathbb{Z}$ has two automorphisms: $\psi(x) = x$ and $\psi(x) = -x - 1$.

For $0 < l < \frac{n-1}{2}$ no $t \in \mathbb{Z}$ such that $\frac{n-1}{2}(-t) = l$. So, in this case is only one automorphism: $\psi(x) = x$. □

Corollary 6.10. *For $0 < l < \frac{n-1}{2}$, an n-ary group $(1, l)$-derived from an infinite cyclic group has no non-trivial automorphisms.* □

Corollary 6.11. *An infinite cyclic n-ary group has no non-trivial automorphisms.*

Proof. Indeed, an infinite cyclic n-ary group is isomorphic to the n-ary group $(\mathbb{Z}, g_1)$, where g_1 is defined by (7). Hence, it is isomorphic to an n-ary group $(1, l)$-derived from the group $\mathbb{Z}$, which , by Corollary 6.10 has no non-trivial automorphisms. □

Lemma 6.12. *A non-commutative n-ary group $(\langle a \rangle, f)$ of infinite order has infinitely many automorphisms. All these automorphism have the form $a^s \to a^{s+t}$ or $a^s \to a^{-s+t}$, where t is an arbitrary fixed integer.*

Proof. A non-commutative n-ary group $(\langle a \rangle, f)$ of infinite order exists only for odd n. Its operation is defined by (10).

By Theorem 6.1, any automorphism ψ of such n-ary group induces on $\langle a \rangle$ an automorphism $\varphi(x) = \psi(x)a^{-t}$, where $a^t = \psi(a^0)$. Thus, $\psi(x) = \varphi(x)a^t$, i.e., $\psi(a^s) = a^{s+t}$ or $\psi(a^s) = a^{-s+t}$. □

Theorem 6.13. *The automorphism group of an infinite non-commutative precyclic n-ary group is isomorphic to the holomorph of the group $(\mathbb{Z}, +)$.*

Proof. Consider the holomorph $\mathbb{Z}^*\mathbb{Z}$ of the group $(\mathbb{Z}, +)$ with the group operation

$$w_1 t_1 \cdot w_2 t_2 = (w_1 w_2)(w_2 t_1 + t_2),$$

where $w_1, w_2 \in \mathbb{Z}^* = \{-1, 1\}$ (see for example [19]). Since any automorphism of an n-ary group $(-1, 0)$-derived from the infinite cyclic group $\langle a \rangle$ has the form $\psi_{w,t}(a^s) = a^{ws+t}$, where $w = \pm 1$, $t \in \mathbb{Z}$, (Lemma 6.12) the map $\tau : Aut(\langle a \rangle, f) \to \mathbb{Z}^*\mathbb{Z}$ defined by $\tau(\psi_{w,t}) = wt$ is a bijection.

Moreover, for all $\psi_{w_1,t_1}, \psi_{w_2,t_2} \in Aut(\langle a \rangle, f)$ and $a^s \in \langle a \rangle$ we have

$$\psi_{w_1,t_1} \circ \psi_{w_2,t_2}(a^s) = \psi_{w_2,t_2}(\psi_{w_1,t_1}(a^s)) = \psi_{w_2,t_2}(a^{w_1 s + t_1})$$
$$= a^{w_2(w_1 s + t_1) + t_2} = a^{w_1 w_2 s + w_2 t_1 + t_2},$$

which means that $\psi_{w_1,t_1} \circ \psi_{w_2,t_2} = \psi_{w_1 w_2, w_2 t_1 + t_2}$.

Thus

$$\tau(\psi_{w_1,t_1} \circ \psi_{w_2,t_2}) = (w_1 w_2)(w_2 t_1 + t_2) = \tau(\psi_{w_1,t_1}) \cdot \tau(\psi_{w_2,t_2}).$$

Hence $Aut(\langle a \rangle, f) \cong \mathbb{Z}^* \mathbb{Z}$. □

7. Splitting automorphisms

In some n-ary groups $h(x) = \overline{x}$ is an automorphism satisfying for every $i = 1, 2, \ldots, n$ the identity

$$h((f(x_1, \ldots, x_n)) = f(x_1, \ldots, x_{i-1}, h(x_i), x_{i+1}, \ldots, x_n).$$

Such n-ary groups are called *distributive* (cf. [8] and [5]). Any distributive n-ary group is a set theoretic union of disjoint cyclic n-ary subgroups of the same order. But it is not precyclic, in general.

An endomorphism ψ of an n-ary groupoid (G, f) is called *splitting* (cf. [24]) if for every $i = 1, \ldots, n$ the identity

$$\psi(f(x_1, \ldots, x_n)) = f(x_1, \ldots, x_{i-1}, \psi(x_i), x_{i+1}, \ldots, x_n) \qquad (16)$$

is satisfied.

It is not difficult to see that the set of all splitting endomorphisms of a given n-ary groupoid (G, f) forms a commutative semigroup. Moreover, for every splitting endomorphisms of (G, f) holds $\psi^n = \psi$.

Proposition 7.1. *Any splitting endomorphism of an n-ary group is its automorphism.*

Proof. Let ψ be a splitting endomorphism of an n-ary group (G, f). If $\psi(x) = \psi(y)$ for some $x, y \in G$, then

$$f(\psi(x), x_2, x_3, \ldots, x_n) = f(\psi(y), x_2, x_3, \ldots, x_n)$$

for all $x_2, x_3, \ldots, x_n \in G$. This, by (16), gives

$$f(x, \psi(x_2), x_3, \ldots, x_n) = f(y, \psi(x_2), x_3, \ldots, x_n).$$

Hence $x = y$. So, ψ is one-to-one.

Since (G, f) is an n-ary group, for all $z, \psi(x_2), x_3, \ldots, x_n \in G$ there exists $y \in G$ such that $z = f(y, \psi(x_2), x_3, \ldots, x_n) = \psi(f(y, x_2, x_3, \ldots, x_n))$. Thus, for every $z \in G$ there exists $x = f(y, x_2, x_3, \ldots, x_n) \in G$ such that $z = \psi(x)$. So, ψ is onto. Consequently it is an automorphism. □

Corollary 7.2. *$\psi^{n-1} = \mathrm{id}_G$ for any splitting automorphism ψ of an n-ary group (G, f).* □

Proposition 7.3. *A non-trivial splitting automorphism of an n-ary group has no fixed points.*

Proof. Indeed, if $\psi(a) = a$ for some $a \in G$, then, according to (2), for every $x \in G$ we obtain

$$\psi(x) = \psi(f(x, a, \ldots, a, \overline{a})) = f(x, \psi(a), a, \ldots, a, \overline{a}) = f(x, a, \ldots, a, \overline{a}) = x,$$

which means that ψ is a trivial automorphism. □

Corollary 7.4. *An n-ary group with only one idempotent has no non-trivial splitting automorphisms.*

Proof. Indeed, if a is an idempotent, then $\psi(a)$ also is an idempotent. Hence, in the case when (G, f) has only one idempotent, we obtain $\psi(a) = a$. Thus ψ is the identity mapping. □

Theorem 7.5. *The mapping $\psi : G \to G$ is a non-trivial splitting automorphism of an n-ary group (G, f) (φ, b)-derived from a group $(G, \circ)$ with the identity e if and only if $\psi(e) \neq e$ and*

(i) $\psi(e)$ *belongs to the center of* $(G, \circ)$,

(ii) $\psi(x) = x \circ \psi(e)$ *for every* $x \in G$,

(iii) $\psi(e) = \varphi\psi(e)$,

(iv) $\underbrace{\psi(e) \circ \psi(e) \circ \ldots \circ \psi(e)}_{n-1} = e$.

Proof. Let (G, f) be an n-ary group (φ, b)-derived from a group $(G, \circ)$ with the identity e. Then, according to Theorem 2.2, $\varphi(b^{-1}) = b^{-1}$. Moreover, since $\varphi^{n-1}(x) \circ b = b \circ x$ holds for all $x \in G$, the equation (4) can be written in more useful form

$$f(x_1, \ldots, x_n) = x_1 \circ \varphi(x_2) \circ \varphi^2(x_3) \circ \varphi^3(x_4) \circ \ldots \circ \varphi^{n-2}(x_{n-1}) \circ b \circ x_n. \quad (17)$$

Thus

$$\psi(x) = \psi(x \circ e) = \psi(f(x, b^{-1}; e, \ldots, e)) = f(x, b^{-1}; e, \ldots, e, \psi(e)) = x \circ \psi(e)$$

for every splitting automorphism ψ of (G, f) and every $x \in G$. This proves (ii).

Similarly, using (17), we obtain

$$\psi(x)=\psi(e\circ x)=\psi(f(e,\overset{(-1)}{b},e,\ldots,e,x))=f(\psi(e),\overset{(-1)}{b},e,\ldots,e,x)=\psi(e)\circ x,$$

which together with the previous identity gives $x\circ\psi(e)=\psi(e)\circ x$. So, $\psi(e)$ belongs to the center of $(G,\circ)$.

Further, from $f(\psi(x),e,\ldots,e)=\psi(f(x,e,\ldots,e))=f(x,\psi(e),e,\ldots,e)$ and (17) we conclude (*iii*).

Now, using (17) and (*iii*) we obtain

$$\psi(b)=\psi(f(e,\ldots,e))=f(\psi(e),\ldots,\psi(e))=\psi(e)\circ\ldots\circ\psi(e)\circ b\circ\psi(e),$$

which together with (*ii*) implies (*iv*).

Hence, any splitting automorphism ψ of (G,f) satisfies (*i*), (*ii*), (*iii*) and (*iv*). By (*ii*), it is non-trivial if and only if $\psi(e)\neq e$.

The converse statement is obvious. □

Corollary 7.6. *A splitting automorphism of an n-ary group (φ,b)-derived from a group $(G,\circ)$ commutes with φ.*

Proof. By Theorem 7.5, for every $x\in G$ we have

$$\psi\varphi(x)=\varphi(x)\circ\psi(e)=\varphi(x)\circ\varphi\psi(e)=\varphi(x\circ\psi(e))=\varphi\psi(x). \qquad \square$$

Corollary 7.7. *An infinite precyclic an n-ary group has no non-trivial splitting endomorphisms.*

Proof. It follows from Theorem 7.5 (*iv*) and (*ii*) or Corollary 6.11. □

Corollary 7.8. *An n-ary group (φ,b)-derived from the centerless group has no non-trivial splitting endomorphisms.*

Proof. Indeed, in such n-ary group $\psi(e)=e$ for every splitting endomorphism ψ. This, by Proposition 7.3, means that ψ is trivial. □

As a simple consequence of the above theorem we obtain the following characterization of skew splitting automorphisms firstly proved in [8].

Theorem 7.9. *The mapping $h(x)=\overline{x}$ is a splitting automorphism of an n-ary group (G,f) if and only if on G we can define a group $(G,\circ)$ with the identity e and an automorphism φ such that*

$$f(x_1,\ldots,x_n)=x_1\circ\varphi(x_2)\circ\varphi^2(x_3)\circ\ldots\circ\varphi^{n-2}(x_{n-1})\circ x_n\circ b,$$

$\varphi(b)=b$, $b^{n-1}=e$, $x\circ\varphi(x)\circ\varphi^2(x)\circ\ldots\circ\varphi^{n-2}(x)=e$ and $\varphi^{n-1}(x)=x$ for all $x,x_1,\ldots,x_n\in G$ and some b from the center of $(G,\circ)$.

Proof. Directly from the definition of the skew element it follows that in an n-ary group (φ, b)-derived from a group $(G, \circ)$ we have $h(e) = \overline{e} = b^{-1}$. In this case also $\varphi(b) = b$ and $\varphi^{n-1}(x) \circ b = b \circ x$ (see Theorem 2.2).

If $h(x) = \overline{x}$ is a splitting automorphism, then, in view of Theorem 7.5, $b^{-1} = h(e)$ belongs to the center of $(G, \circ)$, $b^{n-1} = (h(e))^{n-1} = e$ and $h(x) = x \circ b^{-1}$. Hence also b belongs to this center. Consequently $\varphi^{n-1}(x) = x$. From $f(x, \ldots, x, \overline{x}) = x$ it follows $x \circ \varphi(x) \circ \varphi^2(x) \circ \ldots \circ \varphi^{n-2}(x) = e$.

Conversely, from (17) it follows that in an n-ary group (G, f) we have

$$\overline{x} \circ \varphi(x) \circ \varphi^2(x) \circ \ldots \circ \varphi^{n-2}(x) \circ b = e$$

for every $x \in G$. Hence $\overline{x} = b^{-1} \circ (\varphi(x) \circ \varphi^2(x) \circ \ldots \circ \varphi^{n-2}(x))^{-1}$. Thus in an n-ary group satisfying the conditions mentioned in this theorem holds $\overline{x} = b^{-1} \circ x = x \circ b^{-1}$. Therefore $\overline{e} = b^{-1}$ and $\overline{x} = x \circ \overline{e}$. This means that the mapping $h(x) = \overline{x}$ satisfies the conditions (i) and (ii) from Theorem 7.5. The last two conditions also are satisfied. Hence, $h(x) = \overline{x}$ is a splitting automorphism. □

Corollary 7.10. *An n-ary group containing at least one idempotent has no non-trivial splitting skew endomorphisms.* □

Proof. Suppose that an n-ary group (G, f) has an idempotent a. If it has a splitting skew endomorphism, then, by Theorem 7.9, $a = f(a, \ldots, a) = a \circ b$. Thus $b = e$. Consequently, $f(x, \ldots, x) = e \cdot x \cdot e = x$ for every $x \in G$. Hence (G, f) is an idempotent n-ary group. It has no non-trivial skew endomorphisms. □

Corollary 7.11. *A non-trivial splitting skew endomorphisms there are only in irreducible n-ary groups.* □

Proposition 7.12. *The mapping ψ is a non-trivial splitting automorphism of an n-ary group (m, l)-derived from a cyclic group $\langle a \rangle$ of order k if and only if $\psi(x) = xa^t$ for some $0 < t < k$ such that $t(m-1) \equiv t(n-1) \equiv 0 (\mathrm{mod}\, k)$.*

Proof. The proof is based on Theorem 7.5. From (ii) it follows that any splitting automorphism of a precyclic n-ary group has the form $\psi(x) = xa^t$, where $a^t = \psi(e)$ and $t \neq 0$. Thus $0 < t < k$. From (iii) we obtain $t(m-1) \equiv 0 (\mathrm{mod}\, k)$. In the same way, (iv) implies $t(n-1) \equiv 0 (\mathrm{mod}\, k)$.

On the other hand, it is not difficult to see that $\psi(x) = xa^t$ with t satisfying the above conditions is a non-trivial splitting automorphism. □

References

[1] **V. D. Belousov**, *n-ary quasigroups*, (Russian), Ştiinţa, Kishinev 1972.

[2] **W. Dörnte**, *Untersuchungen über einen verallgemeinerten Gruppenbegriff*, Math. Zeitschr. **29** (1928), 1 – 19.

[3] **I. M. Dudek and W. A. Dudek**, *On skew elements in n-groups*, Demonstratio Math. **14** (1981), 827 – 833.

[4] **W. A. Dudek**, *Remarks on n-groups* Demonstratio Math. **13** (1980), 165 – 181.

[5] **W. A. Dudek**, *Autodistributive n-groups*, Commentationes Math. Annales Soc. Math. Polonae, Prace Matematyczne **23** (1983), 1 – 11.

[6] **W. A. Dudek**, *Medial n-groups and skew elements*, Proceedings of the V Universal Algebra Symposium "Universal and Applied Algebra", Turawa 1988, World Scientific, Singapore 1989, 55 – 80.

[7] **W. A. Dudek**, *On n-ary group with only one skew element*, Radovi Matematički (Sarajevo) **6** (1990), 171 – 175.

[8] **W. A. Dudek**, *On distributive n-ary groups*, Quasigroups and Related Systems **2** (1995), 132 – 151.

[9] **W. A. Dudek**, *Idempotents in n-ary semigroups*, Southeast Asian Bull. Math. **25** (2001), 97 – 104.

[10] **W. A. Dudek**, *On some old and new problems in n-ary groups* Quasigroups and Related Systems **8** (2001), 15 – 36.

[11] **W. A. Dudek**, *Remarks to Glazek's results on n-ary groups*, Discussiones Math., General Algebra Appl. **27** (2007), 199 – 233.

[12] **W. A. Dudek and K. Glazek**, *Around the Hosszú-Gluskin Theorem for n-ary groups*, Discrete Math. **308** (2008), 4861 – 4876.

[13] **W. A. Dudek, K. Głazek and B. Gleichgewicht**, *A note on the axioms of n-groups*, Colloquia Math. Soc. J. Bolyai 29 "Universal Algebra", Esztergom (Hungary) 1977, 195 – 202 (North-Holland, Amsterdam 1982).

[14] **W. A. Dudek, J. Michalski**, *On a generalization of Hosszú Theorem*, Demonstratio Math. **15** (1982), 783 – 805.

[15] **W. A. Dudek and J. Michalski**, *On retrakts of polyadic groups*, Demonstratio Math. **17** (1984), 281 – 301.

[16] **A. M. Gal'mak**, *An n-ary subgroup of identities*, (Russian), Vestsi Nats. Akad. Navuk Belarussi Ser. Fiz.-Mat. Navuk **2** (2003), 25 – 30.

[17] **K. Głazek and B. Gleichgewicht**, *Abelian n-groups*, Colloquia Math. Soc. J. Bolyai **29** "Universal Algebra", Esztergom (Hungary) 1977, 321 – 329 (North-Holland, Amsterdam 1982).

[18] **K. Głazek, J. Michalski and I. Sierocki**, *On evaluation of some polyadic groups*, Contributions to General Algebra **3** (1985), 157 – 171.

[19] **M. Hall, Jr.**, *The theory of groups*, Macmillan Co., New York, 1959.

[20] **M. Hosszú**, *On the explicit form of n-group operations*, Publ. Math. (Debrecen) **10** (1963), 88 – 92.

[21] **E. Kasner**, *An extension of the group concept*, Bull. Amer. Math. Soc. **10** (1904), 290 – 291.

[22] **R. Kerner**, *Ternary structures and Z_3-grading*, Generalized Symmetries in Physics, World Scientific, Singapore 1994, 375 – 394.

[23] **Y. Nambu**, *Generalized Hamiltonian mechanics*, Phys. Rev. D7 (1973), 2405 – 2412.

[24] **J. Plonka**, *On splitting-automorphisms of algebras*, Bull. Soc. Roy. Sci. Liége **42** (1973), 303 – 306.

[25] **E. L. Post**, *Poliadic groups*, Trans. Amer. Math. Soc. **48** (1940), 208 – 350.

[26] **N. A. Shchuchkin**, *An interconnection between n-groups and groups*, (Russian), Chebyshevskii Sb. **4** (2003), 125 – 141.

[27] **N. A. Shchuchkin**, *Skew endomorphisms on n-ary groups*, Quasigroups and Related Systems **14** (2006), 217 – 226.

[28] **N. A. Shchuchkin**, *The bijectivity of the skew mapping in n-ary groups*, (Russian), Trudy Inst. Mat., Minsk, **16** (2008), no.1, 106 – 112.

[29] **N. A. Shchuchkin**, *Subgroups of semicyclic n-ary groups*, (Russian), Fundam. Prikl. Mat. **15** (2009), 211 – 222.

[30] **N. A. Shchuchkin**, *Semicyclic n-ary groups*, (Russian), Izv. Gomel State Univ. **3(54)** (2009), 186 – 194.

[31] **F. M. Sokhatsky**, *On Dudek's problems on the skew operation in polyadic groups*, East Math. J. **19** (2003), 63 – 71.

[32] **E. I. Sokolov**, *On the Gluskin-Hosszú theorem for Dörnte n-groups*, (Russian), Mat. Issled. **39** (1976), 187 – 189.

[33] **L. Takhtajan**, *On foundation of the generalized Nambu mechanics*, Commun. Math. Phys. **160** (1994), 295 – 315.

Received September 19, 2009

W.A.Dudek
Institute of Mathematics and Computer Science, Wroclaw University of Technology, Wyb. Wyspiańskiego 27, 50-370 Wrocław, Poland.
E-mail: dudek@im.pwr.wroc.pl

N.A.Shchuchkin
Volgograd State Pedagogical University, Lenina prosp., 27, 400131 Volgograd, Russia
E-mail: shchuchkin@fizmat.vspu.ru