Quasigroups and Related Systems **6** (1999), 1 – 11

Transversals in groups. 2. Loop transversals in a group by the same subgroup

Eugene A. Kuznetsov

Abstract

Connections between different loop transversals in an arbitrary group G of the same subgroup H are demonstrated. It is shown that any loop transversal in an arbitrary group G of its subgroup H can be represented through one fixed loop transversal of H in G by the determined way. The case of a group transversal of H in G is described.

1. Introduction

This article is a continuation of [6]. The connections between different loop transversals in an arbitrary group G of the same subgroup H are described. These transversals play very a important role in solving some well-known problems. For example, the problem of existence of a finite projective plane of order n is reduced to the existence of a loop transversal of $St_{ab}(S_n)$ in S_n (see [7]).

We give some necessary definitions and notations:

E is a set of indexes (E contains the distinguished element 1, left (right) cosets in a group G by its subgroup H is indexed by the elements from E);

e is the unit of a group G;

1991 Mathematics Subject Classification: 20N15
Keywords: group, loop, transversal, permutation

$Core_G(H)$ is the maximal proper subgroup of G contained in H, which is normal in G;

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

Definition 1. Let G be a group and H its proper subgroup. A complete system $T = \{t_i\}_{i \in E}$ of representatives of the left (right) cosets of H ($e = t_1 \in T$) is called a *left (right) transversal* of H in G (or *"to" H in G* – see [4]). (A system of representatives of left cosets of H is complete if $t, u \in T$, $u^{-1}t \in H$ implies that $t = u$.)

Let T be a left transversal of H in G. We can correctly introduce the following operation on the set E:

$$x \overset{(T)}{\cdot} y = z \quad \overset{def}{\Longleftrightarrow} \quad t_x t_y = t_z h, \quad h \in H.$$

Lemma 1. *System* $< E, \overset{(T)}{\cdot}, 1 >$ *is a right quasigroup with two-sided unit* 1.

Proof. See Lemma 1 in [6]. □

Definition 2. Let T be a left (right) transversal of H in G. If the system $< E, \overset{(T)}{\cdot}, 1 >$ is a loop (group), then T is called a *loop (group) transversal* of H in G.

Remark 1. As we can see in [6], Lemma 10, a loop transversal T of H in G is a two-sided transversal of H in G, i.e. it is both left and right transversal of H in G. So we can simply say "loop transversal".

According to Cayley theorem any group K can be represented as a permutation group of degree $m = card\ K$ and this representation is regular. So any group K can be represented as a group transversal of $St_1(S_m)$ in S_m..

Lemma 2. *The following conditions are equivalent for any left transversal of H in G:*

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

Proof. See [1] and [4]. □

In the sequel the case $Core_G(H) = \{e\}$ will be considered. According to [5], Theorem 12.2.1, in this case we have $\hat{G} \cong G$, where $\hat{G}$ is a permutation representation of the group G. If H is a subgroup of G, then

$$\hat{g}(x) = y \quad \overset{def}{\Longleftrightarrow} \quad gt_xH = t_yH.$$

Lemma 3. *If T is a left transversal of H in G, then*

1) $\hat{h}(1) = 1 \quad \forall h \in H$,
2) *For any* $x, y \in E$ $\hat{t}_x(y) = x \overset{(T)}{\cdot} y, \quad \hat{t}_1(x) = \hat{t}_x(1) = x,$
   $\hat{t}_x^{-1}(y) = x \overset{(T)}{\backslash} y, \quad \hat{t}_x^{-1}(1) = x \overset{(T)}{\backslash} 1, \quad \hat{t}_x^{-1}(x) = 1,$
   where $\overset{(T)}{\backslash}$ *is a left division in the system* $< E, \overset{(T)}{\cdot}, 1 >$.
3) *The following conditions are equivalent:*
   a) *T is a loop transversal of H in G,*
   b) *$\hat{T} = \{\hat{t}_x\}_{x \in E}$ is a sharply transitive set of permutations on E.*

Proof. See Lemma 4 in [6]. □

2. Connection between loop transversals

Let T be an arbitrary fixed left transversal of a subgroup H in a group G. It is evident (see [6], equation (8)), that any other left transversal of H in G can be represented in the following form

$$s_x = t_x h_x^{(T \to S)}, \quad h_x^{(T \to S)} \in H, \quad x \in E.$$

Lemma 4. *The system $< E, \overset{(S)}{\cdot}, 1 >$ can be obtained from the system $< E, \overset{(T)}{\cdot}, 1 >$ in the following way*

$$x \overset{(S)}{\cdot} y = x \overset{(T)}{\cdot} \hat{h}_x^{(T \to S)}(y). \tag{1}$$

Proof. See Lemma 13 in [6]. □

Lemma 5. *The system $< E, \overset{(S)}{\cdot}, 1 >$ is a loop iff the operations $\overset{(T)}{\cdot}$ and $B(x, y) = (\hat{h}_x^{(T \to S)})^{-1}(y)$ are orthogonal.*

Proof. (see also Theorem 2 from [3]) According to Lemma 1 the system $< E, \overset{(S)}{\cdot}, 1 >$ is a right quasigroup with the two-sided unit 1. So it is sufficient to prove the existence and uniqueness of solution of the equation

$$x \overset{(S)}{\cdot} a = b$$

for any fixed $a, b \in E$. We have

$$x \overset{(S)}{\cdot} a = b \iff x \overset{(T)}{\cdot} \hat{h}_x^{(T\to S)}(a) = b \iff \begin{cases} \hat{h}_x^{(T\to S)}(a) = z \\ x \overset{(T)}{\cdot} z = b \end{cases}$$

$$\iff \begin{cases} (\hat{h}_x^{(T\to S)})^{-1}(z) = a \\ x \overset{(T)}{\cdot} z = b \end{cases} \iff \begin{cases} B(x,z) = a \\ x \overset{(T)}{\cdot} z = b \end{cases}$$

So the existence and uniqueness of solution of the equation $x \overset{(S)}{\cdot} a = b$ is equivalent to the existence and uniqueness of solution of the last system, which gives the orthogonality of $\overset{(T)}{\cdot}$ and $B(x, z)$. □

This means that if T is a fixed left transversal of H in G, then any loop transversal S of H in G may be represented through T by formula (1) according to the orthogonality condition from Lemma 5.

V.D. Belousov proved in [2] (Lemma 3) the following criterion

Lemma 6. *An operation $A(x, y)$ defined on the set E is orthogonal to the operation $C(x, y)$ iff $C(x, y)$ can be represented in the form:*

$$C(x, y) = K(B(x, y), A(x, y)), \tag{2}$$

where $B(x, y)$ is an operation orthogonal to $A(x, y)$, and $K(x, y)$ is a left invertible operation on the set E (i.e. $K(x, a) = b$ has a unique solution in E for any fixed $a, b \in E$). □

For a given left transversal T of H in G the problem of the choice of a set $\{h_x\}_{x\in E}$ such that the operations $\overset{(T)}{\cdot}$ and $B(x, y) = \hat{h}_x^{-1}(y)$ are orthogonal is not solved. But if the transversal T of H in G is a loop transversal, then according to Lemma 2, $\pi T \pi^{-1}$ is a loop transversal for any $\pi \in G$. Fixing some $h_0 \in H \setminus \{e\}$ and choosing

$$T^{h_0} = \{r_{x'} = h_0 t_x h_0^{-1} \mid t_x \in T\},$$

we obtain a new loop transversal T^{h_0} of H in G which does not coincide with T, because $Core_G(H) = \{e\}$.

Lemma 7. *The permutation $\hat{h}_0 : E \to E$ is an isomorphism of the systems $< E, \overset{(T)}{\cdot}, 1 >$ and $< E, \overset{(T^{h_0})}{\cdot}, 1 >$.*

Proof. According to the definition of T^{h_0}, we obtain:

$$\begin{aligned} x \overset{(T)}{\cdot} y = z &\Longleftrightarrow t_x t_y = t_z h, \quad h \in H \\ &\Longleftrightarrow (h_0 t_x h_0^{-1})(h_0 t_y h_0^{-1}) = (h_0 t_z h_0^{-1})(h_0 h h_0^{-1}), \quad h \in H \\ &\Longleftrightarrow r_{x'} r_{y'} = r_{z'} h', \quad h' = (h_0 h h_0^{-1}) \in H \\ &\Longleftrightarrow x' \overset{(T^{h_0})}{\cdot} y' = z'. \end{aligned}$$

Since

$$x' = \hat{r}_{x'}(1) = \hat{h}_0 \hat{t}_x \hat{h}_0^{-1}(1) = \hat{h}_0 \hat{t}_x(1) = \hat{h}_0(x), \tag{3}$$

then we obtain

$$\hat{h}_0(x) \overset{(T^{h_0})}{\cdot} \hat{h}_0(y) = \hat{h}_0(z) = \hat{h}_0(x \overset{(T)}{\cdot} y), \tag{4}$$

i.e. permutation $\hat{h}_0$ is an isomorphism of the systems $< E, \overset{(T)}{\cdot}, 1 >$ and $< E, \overset{(T^{h_0})}{\cdot}, 1 >$. $\square$

According to Lemma 4 there exists the set $\{h_x^{(T \to T^{h_0})}\}_{x \in E}$ such that the operation $\overset{(T^{h_0})}{\cdot}$ may be obtained from the operation $\overset{(T)}{\cdot}$ by

$$x \overset{(T^{h_0})}{\cdot} y = x \overset{(T)}{\cdot} \hat{h}_x^{(T \to T^{h_0})}(y). \tag{5}$$

Lemma 8. *The operation $B_1(x, y) = (\hat{h}_x^{(T \to T^{h_0})})^{-1}(y)$ has the form*

$$B_1(x, y) = x \overset{(T^{h_0})}{\backslash} (x \overset{(T)}{\cdot} y). \tag{6}$$

Proof. Let $\hat{h}_x^{(T \to T^{h_0})}(y) = z$. Then $y = (\hat{h}_x^{(T \to T^{h_0})})^{-1}(z)$. So (5) can be rewritten in the form

$$x \overset{(T^{h_0})}{\cdot} (\hat{h}_x^{(T \to T^{h_0})})^{-1}(z) = x \overset{(T)}{\cdot} z.$$

As the system $< E, \overset{(T^{h_0})}{\cdot}, 1 >$ is a loop, we obtain from the last equality

$$(\hat{h}_x^{(T\to T^{h_0})})^{-1}(z) = x \overset{(T^{h_0})}{\backslash} (x \overset{(T)}{\cdot} z).$$

Then we have

$$B_1(x,y) \leftrightharpoons (\hat{h}_x^{(T\to T^{h_0})})^{-1}(y) = x \overset{(T^{h_0})}{\backslash} (x \overset{(T)}{\cdot} y)\,, \tag{7}$$

which completes the proof of the Lemma. □

According to Lemma 5, $B_1(x,y) = (\hat{h}_x^{(T\to T^{h_0})})^{-1}(y)$ and $\overset{(T)}{\cdot}$ are orthogonal operations. So, according to Lemma 6, any operation $C(x,y)$, being orthogonal to $\overset{(T)}{\cdot}$ may be written in the form:

$$C(x,y) = K(B_1(x,y), x \overset{(T)}{\cdot} y), \tag{8}$$

where $B_1(x,y)$ is the operation from (7) and $K(x,y)$ is a left invertible operation on the set E.

Let $P = \{p_x\}_{x\in E}$ be an arbitrary left transversal of H in G. The operation $\overset{(P)}{\cdot}$ is connected with $\overset{(T)}{\cdot}$ by the the formula (1) and $< E, \overset{(P)}{\cdot}, 1 >$ is a loop iff the corresponding set $\{h_x^{(T\to P)}\}_{x\in E}$ satisfies

$$(\hat{h}_x^{(T\to P)})^{-1}(y) = C(x,y) = K(B_1(x,y), x \overset{(T)}{\cdot} y), \tag{9}$$

where $B_1(x,y)$ is the operation from (7) and $K(x,y)$ is a some left invertible operation on the set E.

Because $K(x,y)$ is left invertible on the set E, we can write it as

$$K(x,y) = \varphi_y(x),$$

where φ_y is a permutation on E (for any $y \in E$). Using (7), we can rewrite (9) in the form

$$(\hat{h}_x^{(T\to P)})^{-1}(y) = \varphi_{x \overset{(T)}{\cdot} y}(x \overset{(T^{h_0})}{\backslash} (x \overset{(T)}{\cdot} y))\,. \tag{10}$$

But by (1)

$$x \overset{(P)}{\cdot} y = x \overset{(T)}{\cdot} \hat{h}_x^{(T\to P)}(y),$$

where set $\{h_x^{(T\to P)}\}_{x\in E}$ satisfies (10).

Let $\hat{h}_x^{(T\to P)}(y) = z$. Then $y = (h_x^{(T\to P)})^{-1}(z)$ and

$$x \overset{(P)}{\cdot} (h_x^{(T\to P)})^{-1}(z) = x \overset{(T)}{\cdot} z,$$

$$(h_x^{(T\to P)})^{-1}(z) = x \overset{(P)}{\backslash} (x \overset{(T)}{\cdot} z).$$

According to (10), we have

$$x \overset{(P)}{\backslash} (x \overset{(T)}{\cdot} z) = \varphi_{x \overset{(T)}{\cdot} z}(x \overset{(T^{h_0})}{\backslash} (x \overset{(T)}{\cdot} z)),$$

which for $u = x \overset{(T)}{\cdot} z$ gives

$$x \overset{(P)}{\backslash} u = \varphi_u(x \overset{(T^{h_0})}{\backslash} u). \tag{11}$$

So for the loop transversal $P = \{p_x\}_{x\in E}$ and any $x \in E$ we have

$$\hat{p}_x^{-1}(y) = \varphi_y(x \overset{(T^{h_0})}{\backslash} y)\,. \tag{12}$$

Lemma 9. *The the following conditions hold for all $x \in E$:*

1) $\varphi_x(1) = 1$,

2) $\varphi_x(x) = x$,

3) $\alpha_x(y) = \varphi_y(x \overset{(T^{h_0})}{\backslash} y)$ *is a permutation from the group $\hat{G}$.*

Proof. 1) Because $\hat{p}_x^{-1}(x) = 1$ for any $x \in E$, we obtain from (12)

$$1 = \hat{p}_x^{-1}(x) = \varphi_x(x \overset{(T^{h_0})}{\backslash} x) = \varphi_x(1).$$

2) As $\hat{p}_1^{-1}(x) = x$ for any $x \in E$, then

$$x = \hat{p}_1^{-1}(x) = \varphi_x(1 \overset{(T^{h_0})}{\backslash} x) = \varphi_x(x).$$

3) Since for any $x \in E$ the reflection $\hat{p}_x$ is a permutation from the group $\hat{G}$, then according to (12), the reflection $\alpha_x(y) = \varphi_y(x \overset{(T^{h_0})}{\backslash} y)$ is a permutation from the group $\hat{G}$. □

Now we can prove

Theorem 1. *Let $T = \{t_x\}_{x\in E}$ be a loop transversal of H in G. If a left transversal $P = \{p_x\}_{x\in E}$ of H in G is connected with T by* (1), *then the following statements are equivalent:*

1) *P is a loop transversal,*
2) *P is connected with T by* (12), *where φ_x is as in Lemma* 9 *and $\overset{(T^{h_0})}{\backslash}$ is as in Lemma* 7. *Operations $\overset{(P)}{\cdot}$ and $\overset{(T^{h_0})}{\cdot}$ are connected by* (11).

Proof. 1) $\Longrightarrow$ 2) If P is a loop transversal of H in G, then (by Lemma 5) operations $\overset{(T)}{\cdot}$ and $B(x,y) = (\hat{h}_x^{(T\to P)})^{-1}(y)$ are orthogonal and (according to Lemma 6)

$$(\hat{h}_x^{(T\to P)})^{-1}(y) = K(B_1(x,y), x \overset{(T)}{\cdot} y),$$

where $B_1(x,y)$ is the operation from (7) and $K(x,y)$ is left invertible on the set E.

Because $K(x,y)$ is left invertible on E, we can write it in the form

$$K(x,y) = \varphi_y(x),$$

where φ_y is a permutation on E (for any $y \in E$). The rest follows Lemma 9.

2) $\Longrightarrow$ 1) If the conditions of the statement 2 hold, then there exists a set $\{h_x^{(T\to P)}\}_{x\in E}$ such that

$$p_x = t_x h_x^{(T\to P)}, \qquad h_x^{(T\to P)} \in H,$$
$$x \overset{(P)}{\cdot} y = x \overset{(T)}{\cdot} \hat{h}_x^{(T\to P)}(y).$$

So we have

$$p_x^{-1} = (h_x^{(T\to P)})^{-1} t_x^{-1},$$

which by Lemma 3 implies

$$\varphi_y(x \overset{(T^{h_0})}{\backslash} y) = \hat{p}_x^{-1}(y) = (\hat{h}_x^{(T\to P)})^{-1}\hat{t}_x^{-1}(y) = (\hat{h}_x^{(T\to P)})^{-1}(x \overset{(T)}{\backslash} y)\,.$$

This for $y = x \overset{(T)}{\cdot} z$ gives

$$\varphi_{x \overset{(T)}{\cdot} z}(x \overset{(T^{h_0})}{\backslash} (x \overset{(T)}{\cdot} z)) = (\hat{h}_x^{(T\to P)})^{-1}(z)\,.$$

Since operations $\overset{(T)}{\cdot}$ and $B_1(x,z) = x \overset{(T^{h_0})}{\backslash} (x \overset{(T)}{\cdot} z) = (\hat{h}_x^{(T\to T^{h_0})})^{-1}(z)$ are orthogonal (see Lemma 8), the last equality may be written as

$$(\hat{h}_x^{(T\to P)})^{-1}(z) = K(B_1(x,z), x \overset{(T)}{\cdot} z),$$

where $K(x,y) = \varphi_y(x)$ is a left invertible operation E.

But by Lemma 6 operations $\overset{(T)}{\cdot}$ and $B_2(x,z) = (\hat{h}_x^{(T\to P)})^{-1}(z)$ are orthogonal. Thus by Lemma 5 the system $< E, \overset{(P)}{\cdot}, 1 >$ is a loop, i.e. P is a loop transversal of H in G. □

3. A group transversal

As a simple consequence of our Theorem 1 we obtain

Theorem 2. *Let $T = \{t_x\}_{x\in E}$ be a group transversal of H in G. If a left transversal $P = \{p_x\}_{x\in E}$ of H in G is connected with T by* (1), *then the following statements are equivalent:*

1) *P is a loop transversal,*
2) *P is connected with T by the formula*

$$\hat{p}_x^{-1}(y) = \varphi_y(x^{-1} \overset{(T^{h_0})}{\cdot} y)\,, \tag{13}$$

where φ_x is as in Lemma 9 and x^{-1} is the inverse of x in the group $< E, \overset{(T^{h_0})}{\cdot}, 1 >$, which is isomorphic to $< E, \overset{(T)}{\cdot}, 1 >$. Corresponding operations $\overset{(P)}{\cdot}$ and $\overset{(T^{h_0})}{\cdot}$ are connected by

$$x \overset{(P)}{\backslash} y = \varphi_y(x^{-1} \overset{(T^{h_0})}{\cdot} y)\,. \tag{14}$$

From this Theorem we obtain the criterion of the existence of a loop transversal of H in G.

Theorem 3. *If $Core_G(H) = \{e\}$, $d = (G : H) = card\ E$, then the following statements are equivalent:*

1) *There exists a loop transversal of H in G.*
2) *There exists a set $\{\varphi_x\}_{x\in E}$ of permutations on E such that*

   a) $\varphi_x \in St_{1,x}(S_d) \quad \forall x \in E$,

   b) For any $x \in E$ the reflection $\alpha_x(y) = \varphi_y(y \overset{(T^{h_0})}{-} x)$ (where the operation $\overset{(T^{h_0})}{-}$ is the inverse operation in the fixed group $< Z_d, \overset{(T^{h_0})}{+}, 1 >$, which is isomorphic to the group $< Z_d, +, 0 >$) is a permutation from the group $\hat{G}$.

Proof. 1) $\Longrightarrow$ 2) Let $P = \{p_x\}_{x\in E}$ be a loop transversal of H in G. Using a permutation representation $\hat{G}$ of the group G we see that $\hat{P} = \{\hat{p}_x\}_{x\in E}$ is a loop transversal of $\hat{H}$ in $\hat{G}$. According to Lemma 3, the set $\hat{P}$ is a sharply transitive set of permutations on the set E; so $\hat{P} = \{\hat{p}_x\}_{x\in E}$ is a loop transversal of $H^* = St_1(S_d)$ in the symmetric group S_d (see [6]).

By the help of the regular representation of left translations the abelian group $< Z_d, +, 0 >$ may be represented as a group transversal T of $H^* = St_1(S_d)$ in S_d (see Remark 1). According to Theorem 2, the loop transversal $\hat{P} = \{\hat{p}_x\}_{x\in E}$ may be represented as the group transversal T^{h_0} by the formula

$$\hat{p}_x^{-1}(y) = \varphi_y(-x \overset{(T^{h_0})}{+} y) = \varphi_y(y \overset{(T^{h_0})}{-} x)\,, \tag{15}$$

where permutations $\{\varphi_x\}_{x\in E}$ are as in Lemma 9.

By Lemma 7 operations $\overset{(T)}{+}$ and $\overset{(T^{h_0})}{+}$ are isomorphic. Moreover $p_x^{-1} \in G$ implies $\hat{p}_x^{-1} \in \hat{G}$. Thus putting $\alpha_x(y) = \hat{p}_x^{-1}(y)$, we see that the conditions a and b from statement 2 hold.

2 $\Longrightarrow$ 1) Let $P = \{p_x\}_{x\in E}$ be a set of permutations defined by the formula:

$$\hat{p}_x^{-1}(y) \overset{def}{=} \varphi_y(-x \overset{(T^{h_0})}{+} y).$$

Then we have for any $x \in E$

$$\hat{p}_x^{-1}(x) = \varphi_x(-x \overset{(T^{h_0})}{+} x) = \varphi_x(1) = 1 \implies p_x(1) = x,$$

$$\hat{p}_1^{-1}(x) = \varphi_x(-1 \overset{(T^{h_0})}{+} x) = \varphi_x(x) = x \implies p_1(x) = x.$$

This means that $P = \{p_x\}_{x \in E}$ is a left transversal of H in G.

Using the analogous method as in the proof of sufficiency of Theorem 1 we can prove the existence of a loop transversal of H in G. □

References

[1] **R. Baer**: *Nets and groups. 1*, Trans. Amer. Math. Soc. **46** (1939), 110 − 141.

[2] **V. D. Belousov**: *On properties of binary operations* (Russian), Uch. zapiski Beltskogo Gospedinstituta **5** (1960), 9 − 28.

[3] **V. D. Belousov**: *Crossed isotopies of quasigroups* (Russian), Mat. issled. **113** (1990), 14 − 20.

[4] **K. W. Johnson**: *S-rings over loops, right mapping groups and transversals in permutation groups*, Math. Proc. Camb. Phil. Soc. **89** (1981), 433 − 443.

[5] **M. I. Kargapolov and Yu. I. Merzlyakov**: *Foundations of the group theory* (Russian), Moscow, 1982.

[6] **E. A. Kuznetsov**: *Transversals in groups. 1. Elementary properties*, Quasigroups and Related Systems **1** (1994), 22 − 42.

[7] **E. A. Kuznetsov**: *Sharply k-transitive sets of permutations and loop transversals in S_n*, Quasigroups and Related Systems **1** (1994), 43 − 50.

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 September 10, 1999

Quasigroups and Related Systems **6** (1999), 13 – 22

Free R-n-modules

Lăcrimioara Iancu

Abstract

We define the canonical presentation of an R-n-module, in terms of its largest n-submodule with zero and of an idempotent commutative n-group. We give a construction for the free R-n-module with zero, as well as a canonical presentation for the free R-n-module. We give the number of zero-idempotents of a finitely generated free R-n-module. The last theorem states that, for $n \geqslant 3$, free R-n-modules are isomorphic if and only if their free generating sets have the same cardinality.

1. Notations and preliminary results

In [1], N. Celakoski has defined n-modules as a natural generalization of the usual binary notion; however, for his further results he imposed a strong restriction, namely that the commutative n-group involved has a *unique* neutral element. In [4] we restart the study of n-modules by dropping this restriction.

In this section we shall briefly recall some of the definitions and results in [4] and we shall make some additional comments. We use the following conventional notation: the sequence $a_i, \ldots, a_j$ of $j-i+1$ terms of an n-ary sum is denoted by a_i^j and if $a_i = a_{i+1} = \ldots = a_j = a$ then the sequence is denoted by $\overset{(j-i+1)}{a}$; if $i > j$, then a_i^j denotes an empty sequence. Denote by $a^{\langle k \rangle}$ the k-th power of a, which is defined

1991 Mathematics Subject Classification: 20N15, 16D10, 16D40
Keywords: free n-module, canonical presentation

by:

$$a^{\langle 0\rangle} = a \quad \text{and} \quad a^{\langle k\rangle} = [a^{\langle k-1\rangle}, \overset{(n-1)}{a}]_+, \quad k \in \mathbb{Z}$$

In particular, $a^{\langle -1\rangle} = \overline{a}$, where $\overline{a}$ denotes the querelement of a.

Throughout this paper R denotes an associative ring with unity $1 \neq 0$.

Definition 1.1. We call *left R-n-module* a commutative n-group $(M, [\,]_+)$ together with an external operation $\mu\colon R \times M \to M$ which satisfies the axioms:

A1) $\mu(r, [x_1^n]_+) = \big[\mu(r, x_1), \ldots, \mu(r, x_n)\big]_+$

A2) $\mu\big((r_1 + \cdots + r_n), x\big) = \big[\mu(r_1, x), \ldots, \mu(r_n, x)\big]_+$

A3) $\mu(r \cdot r', x) = \mu\big(r, \mu(r', x)\big)$

A4) $\mu(1, x) = x$

for all $x, x_1, \ldots, x_n \in M$ and all $r, r', r_1, \ldots, r_n \in R$.

We describe a *right R-n-module* by replacing in the above definition axiom A3) by A3') $\mu(r \cdot r', x) = \mu\big(r', \mu(r, x)\big)$. As in the binary case, the theory of right n-modules can be deduced from the theory of left n-modules and conversely. For this reason, we shall deal in the sequel with left n-modules, and by R-n-modules we shall always understand left R-n-modules.

Since we are dealing with left n-modules, denote the element $\mu(r, x)$ by rx. As immediate consequences of the axioms, note:

$$(r_1+r_2)x = [r_1x, r_2x, \overset{(n-2)}{0x}]_+, \qquad (-r)x = [0x, 0x, \overset{(n-3)}{rx}, r\overline{x}]_+,$$

$$\overline{rx} = r\overline{x}, \qquad \overline{x} = (-n+2)x = \big((-1) + \cdots + (-1)\big)x.$$

The empty n-group may be regarded as an R-n-module for any ring R. If M is a non-empty R-n-module, then it necessarily has at least one neutral element; indeed, for every $x \in M$, the element $0x$ is a neuter in $(M, [\,]_+)$ (or an idempotent, since the two notions coincide in commutative n-groups). Note that $0x^{\langle k\rangle} = 0x$, $\forall x \in M$, $\forall k \in \mathbb{Z}$ (in particular $0x = 0\overline{x}$).

n-Submodules, congruences and homomorphisms are defined in the obvious way. If S is a non-empty n-submodule of an R-n-module M, then the relation ρ_S defined by $x\rho_S y \Leftrightarrow \exists s_2^n \in S : y = [x, s_2^n]_+$ is a congruence on M. This correspondence is not a bijection, still it allows us to define the factor module $M/S = M/\rho_S$.

The set of all neuters of the n-group $(M, [\,]_+)$ is denoted by $\mathcal{N}_M$ (or simply by $\mathcal{N}$) and the set of all neuters of the form $0x$, for some $x \in M$, is denoted by $\mathcal{N}_{0M}$ (or sometimes just $\mathcal{N}_0$). $\mathcal{N}_0$ is an n-submodule of $\mathcal{N}$ and they are both n-submodules of M. The elements of $\mathcal{N}_0$ are characterized by the following: $e \in \mathcal{N}_0 \Leftrightarrow re = e, \forall r \in R$. The elements of $\mathcal{N}_0$ will be called *zero-idempotents*; in particular, if $\mathcal{N}_0$ consists of exactly one element, then this element is called a *zero* of the n-module and it is denoted by 0.

If $f : M_1 \to M_2$ is a homomorphism of R-n-modules, then:

1) $f(\mathcal{N}_1) \subseteq \mathcal{N}_2$ and $f(\mathcal{N}_{01}) \subseteq \mathcal{N}_{02}$;

2) $f(\overline{x}) = \overline{f(x)}, \forall x \in M_1$;

3) the set $\operatorname{Ker} f = \{x \in M_1 \mid f(x) \in \mathcal{N}_{02}\}$ is an n-submodule of M_1 and $\mathcal{N}_{01} \subseteq \operatorname{Ker} f$.

2. The canonical presentation

2.1. We have introduced in [4] a class of n-submodules of an R-n-module which will play an important role in the study of n-modules. Let M be an R-n-module. For each $e \in \mathcal{N}_0$, the set

$$M_e = \{x \in M \mid 0x = e\}$$

is an n-submodule with zero (the element e) of M. The n-submodules M_e are all isomorphic and they form a partition of M. Note that $M/\mathcal{N}_0 \simeq M_e$. In fact, the whole structure of an R-n-module is determined by: the structure of an R-n-module with zero (M_e) and the structure of an idempotent commutative n-group ($\mathcal{N}_0$).

Indeed, if we start from an R-n-module $(B, [\,], \mu)$ with zero 0 and an idempotent commutative n-group $(A, [\,]_\circ)$, we can build an R-n-module M (unique up to isomorphism) such that $M_e \simeq B, \forall e \in \mathcal{N}_{0M}$ and $\mathcal{N}_{0M} \simeq A$, as follows:

- the set M is defined as the disjoint union, indexed by A, of copies of the set B: $M = \overset{\circ}{\bigcup\limits_{e \in A}} B_e$; denote by (x, e) the elements of B_e;
- the external operation $\nu\colon R \times M \to M$ is defined by
$$\nu\big(r, (x, e)\big) = \big(\mu(r, x), e\big)\,;$$
- n-ary addition is defined by
$$\big[(x_1, e_1), \ldots, (x_n, e_n)\big]_+ = \big([x_1^n], [e_1^n]_\circ\big).$$

A straightforward computation shows that $(M, [\,]_+, \nu)$ is an R-n-module such that

$$\mathcal{N}_{0M} = \{(0, e) \mid e \in A\} \simeq A \text{ and } M_{(0,e)} = \{(x, e) \mid x \in B\} \simeq B,$$

for each $(0, e) \in \mathcal{N}_{0M}$. Moreover, given an R-n-module T and performing the above construction by using some T_e instead of B and $\mathcal{N}_{0T}$ instead of A one obtains an R-n-module M which is isomorphic to T. A very natural isomorphism to consider is

$$\varphi\colon T \to M, \quad \varphi(x) = \big([x, \overset{(n-2)}{0x}, e]_+, 0x\big).$$

This shows that an R-n-module M is completely described by its largest n-submodule(s) with zero M_e and by $\mathcal{N}_{0M}$. This way of describing an R-n-module will be called *canonical presentation.* We have used disjoint union in order to construct an R-n-module with a given canonical presentation, because this was the natural way to make the connections with the M_e's and with $\mathcal{N}_0$. Yet, for practical reasons, it is simpler to consider the R-n-module being described as the Cartesian product $B \times A$, together with the operations defined above. Note that the map $p_1\colon B \times A \to B$, $p_1\big((x, e)\big) = x$ is a homomorphism of R-n-modules, and the map $p_2\colon B \times A \to A$, $p_2\big((x, e)\big) = e$ is a homomorphism of n-groups.

2.2. The canonical presentation of an R-n-module will prove its usefulness in the study of n-submodules and in the study of homomorphisms. Indeed, let M be an R-n-module with the canonical presentation $(B, [\,], \mu)$ and $(A, [\,]_\circ)$, as above. Then any n-submodule of M has a canonical presentation of the form $(B', [], \mu)$ and $(A', []_\circ)$, where B' is an n-submodule of B and A' is an n-subgroup of A.

Now let $f\colon M_1 \to M_2$ be a homomorphism of R-n-modules and take an arbitrary zero-idempotent $e \in \mathcal{N}_{01}$. Then $\varphi\colon \mathcal{N}_{01} \to \mathcal{N}_{02}$, $\varphi(x) = f(x)$ and $\psi\colon M_{1e} \to M_{2f(e)}$, $\psi(x) = f(x)$ are both homomorphisms. Moreover, the converse also holds, namely: if $\varphi\colon A_1 \to A_2$ is a homomorphism of n-groups and $\psi\colon B_1 \to B_2$ is a homomorphism of R-n-modules, then the map $f\colon M_1 \to M_2$ defined by

$$f\left((x,e)\right) = (\psi(x), \varphi(e))$$

is a homomorphism of R-n-modules (where M_1 and M_2 have the canonical presentations B_1, A_1 and B_2, A_2 respectively).

Injective and surjective homomorphisms can be also characterized in terms of the data of the canonical presentation.

Proposition 2.3. *Let $f\colon M_1 \to M_2$ be a homomorphism of R-n-modules. Then*

1) *f is injective iff* $\operatorname{Ker} f = \mathcal{N}_{01}$ *and the restriction $f|_{\mathcal{N}_{01}}$ is injective;*
2) *f is surjective iff for each $e' \in \mathcal{N}_{02}$ there exists $e \in \mathcal{N}_{01}$ such that $M_{2e'} = f(M_{1e})$.*

Proof. 1) Suppose f is injective and $x \in \operatorname{Ker} f$, i.e. $f(x) \in \mathcal{N}_{02}$. Then $f(x) = 0f(x) = f(0x)$, which implies $x = 0x$ and hence $x \in \mathcal{N}_{01}$.

Conversely, if $\operatorname{Ker} f = \mathcal{N}_{01}$ and the restriction $f|_{\mathcal{N}_{01}}$ is injective, let $f(x_1) = f(x_2)$. Then, for an arbitrary $e \in \mathcal{N}_{01}$, we have

$$f\big([x_1, \overset{(n-3)}{x_2}, \overline{x_2}, e]_+\big) = f(e) \in \mathcal{N}_{02},$$

i.e. $[x_1, \overset{(n-3)}{x_2}, \overline{x_2}, e]_+ \in \operatorname{Ker} f = \mathcal{N}_{01}$. Since $f|_{\mathcal{N}_{01}}$ is injective, it follows that $[x_1, \overset{(n-3)}{x_2}, \overline{x_2}, e]_+ = e$, hence $x_1 = x_2$.

2) Suppose f is surjective and $e' \in \mathcal{N}_{02}$. Then there exists $x \in M_1$ such that $e' = f(x)$; but $e' = 0e' = 0f(x) = f(0x) \in f(\mathcal{N}_{01})$. Denote $0x$ by $e \in \mathcal{N}_{01}$ and let $y \in M_{2e'}$ (this means $0y = e'$). Now there exists $u \in \mathcal{N}_{01}$ and $z \in M_{1u}$ such that $y = f(z)$. The element $[z, \overset{(n-2)}{u}, e]_+$ belongs to M_{1e} and $f\big([z, \overset{(n-2)}{u}, e]_+\big) = f(z) = y$. Thus, we have proved that for each $e' \in \mathcal{N}_{02}$ there exists $e \in \mathcal{N}_{01}$ such that $M_{2e'} \subseteq f(M_{1e})$; the other inclusion is obvious. The converse follows immediately from the fact that the n-submodules $M_{2e'}$ form a partition of M_2. $\square$

3. Free n-modules with zero

R-n-modules with zero can be regarded as universal algebras having as domain of operations: an n-ary operation, a nullary operation and a family of unary operations, indexed by R, all of which satisfy the axioms A1)–A4). The class of R-n-modules with zero is a variety — it is closed under taking homomorphic images, subalgebras and direct products. This ensures the existence of free R-n-modules with zero. In this section we will provide a construction, very similar to the binary case, of the free R-n-module with zero having an arbitrary free generating set X.

Let A be an R-n-module with zero. The elements $a_1, \ldots, a_k \in A$, where $k \equiv t (\mathrm{mod} n{-}1)$, are called *linearly independent* if

$$[r_1a_1, \ldots, r_ka_k, \overset{(n-t)}{0}]_+ = 0 \quad \text{implies} \quad r_1 = \ldots = r_k = 0$$

and *linearly dependent* otherwise. A subset X of A is *linearly independent* if any finite subset of X is linearly independent. X is a *basis* of A if X is not empty, if X generates A, and if X is linearly independent. It is easy to prove that if X is a basis of A, then in particular $A \neq \{0\}$ if $R \neq \{0\}$ and every element of A has a unique expression as a linear combination of elements of X.

Proposition 3.1. *An R-n-module A with zero, which has a basis X, is free on X in the variety of R-n-modules with zero.*

Proof. Let T be an R-n-module with zero and a mapping $\alpha\colon X \to T$. Every element $a \in A$ has a unique expression of the form:

$$a = [r_1x_1, \ldots, r_kx_k, \overset{(n-t)}{0_A}]_+$$

where $k \equiv t (\mathrm{mod}\, n{-}1)$ and $r_1, \ldots, r_k \in R$, $x_1, \ldots, x_k \in X$.

Define $\widetilde{\alpha}\colon A \to T$ by $\widetilde{\alpha}(a) = [r_1\alpha(x_1), \ldots, r_k\alpha(x_k), \overset{(n-t)}{0_T}]_+$; a simple computation shows that $\widetilde{\alpha}$ is a homomorphism of R-n-modules and $\widetilde{\alpha} \circ i = \alpha$. Moreover, $\widetilde{\alpha}$ is the unique homomorphism with this property. □

Corollary 3.2. *Two R-n-modules with zero, having bases whose cardinalities are equal, are isomorphic.*

For this reason, we denote the R-n-module with zero free on X by

$F_0(X)$.

Let $X \neq \emptyset$ be an arbitrary set and a mapping $f\colon X \to R$. As usual, define

$$\operatorname{supp} f = \{x \in X \mid f(x) \neq 0\}$$

and

$$R^{(X)} = \{f \in R^X \mid |\operatorname{supp} f| < \infty\}.$$

We define a natural structure of R-n-module with zero on $R^{(X)}$ as follows:

$$[f_1, \ldots, f_n]_+(x) = f_1(x) + \cdots + f_n(x),\ (rf)(x) = r \cdot f(x).$$

The zero element is the function $o\colon X \to R$, $o(x) = 0$, $\forall x \in X$.

Proposition 3.3. *If $R \neq \{0\}$ is a ring and $X \neq \emptyset$ is an arbitrary set, then $R^{(X)}$ has a basis of the same cardinality as X.*

Proof. A basis of $R^{(X)}$ is the set $B = \{f_x \mid x \in X\}$, where $f_x\colon X \to R$ is defined by $f_x(y) = \begin{cases} 1, & y = x \\ 0, & y \neq x \end{cases}$.

One can easily check that B is linearly independent; furthermore, if $f \in R^{(X)}$ with $\operatorname{supp} f = \{x_1, \ldots, x_k\}$, where $k \equiv t (\mathrm{mod}\, n-1)$, then $f = [f(x_1) \cdot f_{x_1}, \ldots, f(x_k) \cdot f_{x_k}, \overset{(n-t)}{o}]_+$. □

Like in the binary case (see [5]), one can easily prove that if $F_0(X) \simeq F_0(Y)$ and X is infinite, then Y is infinite too and $|X| = |Y|$.

4. Free n-modules

The class of all R-n-modules is again a variety, so free R-n-modules exist. We will give in this final section a canonical presentation for the free R-n-module on an arbitrary set as well as a theorem concerning the number of zero-idempotents of a free R-n-module with a finite free generating set.

Note that, similar to the case of R-n-modules with zero, two free R-n-modules having free generating sets whose cardinalities are equal, are isomorphic.

Theorem 4.1. *Let $X \neq \emptyset$ be an arbitrary set and F be the R-n-module having the following canonical presentation:*

(*a*) *$F_0(X)$ as largest n-submodule with zero;*

(*b*) *the abelian n-group G with the presentation*

$$\left\langle X \mid [\overset{(n)}{x}]_+ = x, \forall x \in X \right\rangle$$

as idempotent commutative n-group.

Then the R-n-module F is free and X is its free generating set.

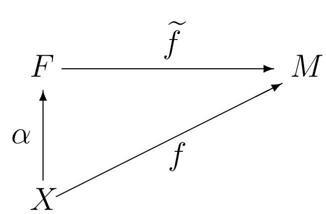
Proof. First, let us make some necessary remarks.
1) The n-group G described in *(b)* is the free idempotent abelian n-group with the free generating set X (it is easy to see that the class of idempotent abelian n-groups is a variety; as for the construction of free abelian n-groups, see the paper of F. M. Sioson [6]).
2) By 2.1, the elements of F have the form (y, g), where $y \in F_0(X)$ and $g \in G$. We shall identify each $x \in X$ with the pair $(x, x) \in F$; in other words, we define an "inclusion" $\alpha\colon X \to F$, by $\alpha(x) = (x, x)$.

Let M be an arbitrary R-n-module having the canonical presentation B, A, where B is an R-n-module with zero and A is an idempotent abelian n-group, as in 2.1. This means that we will describe the elements of M as pairs $(b, a) \in B \times A$. Let now $f\colon X \to M$ be an arbitrary map. We will use f for defining two other maps u and v as:

$$u\colon X \to B, \quad u(x) = p_1\left(f(x)\right) \tag{1}$$

$$v\colon X \to A, \quad v(x) = p_2\left(f(x)\right) \tag{2}$$

Since $F_0(X)$ is the free R-n-module with zero on X and B is an R-n-module with zero, it follows that there exists a unique homomorphism $\widetilde{u}\colon F_0(X) \to B$ such that $\widetilde{u}(x) = u(x)$, $\forall x \in X$. By using a similar argument, it follows that there exists a unique homomorphism of n-groups $\tilde{v}\colon G \to A$ such that $\widetilde{v}(x) = v(x)$, $\forall x \in X$. We are now able to define the homomorphism $\widetilde{f}$ which makes the following diagram commutative:



namely, for all $(y,g) \in F$, put $\widetilde{f}((y,g)) = (\widetilde{u}(y), \widetilde{v}(g))$. We have seen in 2.2 that a map defined in the above way is a homomorphism of R-n-modules. Further, for all $x \in X$ we have

$$(\widetilde{f} \circ \alpha)(x) = \widetilde{f}\big((x,x)\big) = \big(p_1\big(f(x)\big), p_2\big(f(x)\big)\big) = f(x)$$

which shows that $\widetilde{f} \circ \alpha = f$. The uniqueness of $\widetilde{f}$ follows from the uniqueness of $\widetilde{u}$ and $\widetilde{v}$ and from 2.2. □

Corollary 4.2. *Let X, Y be two non-empty sets. If $F(X) \simeq F(Y)$ and X is infinite, then Y is infinite too and $|X| = |Y|$.*

Proof. It follows immediately from the preceding theorem and from the similar result for free R-n-modules with zero. □

Lemma 4.3. *Let n be an integer, $n \geqslant 3$, X a set with $|X| = k$, $k \geqslant 1$ and $F(X)$ the R-n-module free on X. Then $\mathcal{N}_{0F(X)}$ has $(n{-}1)^{k-1}$ elements.*

Proof. Indeed, $\mathcal{N}_0$ is equal to

$$\{[\overset{(t_1)}{0}x_1, \overset{(t_2)}{0}x_2, \dots, \overset{(t_k)}{0}x_k]_+ \mid 0 \leqslant t_i \leqslant n{-}2,\ t_1 + \cdots + t_k \equiv 1(\mathrm{mod}\, n{-}1)\}$$

or, equivalently, $\mathcal{N}_0 \simeq G$, where G is the idempotent abelian n-group described in Theorem 4.1. Every element of $\mathcal{N}_0$ can be described by a uniquely determined function $f\colon \{1, \dots, k{-}1\} \to \{0, 1, \dots, n{-}2\}$ as follows:

$$e = [\,\overset{(f(1))}{0}x_1\,, \dots,\ \overset{(f(k-1))}{0}x_{k-1}\,,\ \overset{(n-r)}{0}x_k\,]_+$$

where $f(1) + \cdots + f(k{-}1) = t(n{-}1) + r$, $2 \leqslant r \leqslant n$. This correspondence between elements of $\mathcal{N}_0$ and such functions is obviously a bijection and so $|\mathcal{N}_0| = (n{-}1)^{k-1}$. □

Corollary 4.4. *Let n be an integer, $n \geqslant 3$ and X, Y two non-empty sets. If $F(X) \simeq F(Y)$ and X is finite, then Y is finite too and $|X| = |Y|$.*

Proof. It follows from 2.2, Theorem 4.1 and the preceding lemma. □

The following theorem is a direct consequence of the preceding results in this section.

Theorem 4.5. *Let n be an integer, $n \geqslant 3$, and let X, Y be two non-empty sets. Then $F(X) \simeq F(Y)$ iff $|X| = |Y|$.*

Acknowledgements. This paper was written while the author was a visitor at Université Paris VII, in 1999. Thanks go to the members of the "Equipe des Groupes Finis" for their hospitality and support. The stay was supported by a scholarship from the Noesis Foundation, which is gratefully acknowledged.

References

[1] **N. Celakoski**, *On n-modules*, Godisen Zb. Elektro–Mas. Fak. Univ. Skopje **3** (1969), 15 – 26.

[2] **P. M. Cohn**, *Universal algebra*, Second edition, Mathematics and its Applications **6**, D. Reidel Publishing Co., Dordrecht – Boston, Mass. , 1981.

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

[4] **L. Iancu**, *Redefining n-modules*, Bul. Şt. Univ. Baia Mare, Ser. B, Mat.–Inf. **14** (1998)

[5] **I. Purdea**, *Tratat de algebră modernă*, Vol.II, (Romanian) (*Treatise on modern algebra. Vol.II*) Ed. Academiei RSR, Bucharest, 1982.

[6] **F. M. Sioson**, *Free Abelian m-Groups, I, II, III*, Proc. Japan Acad. **43** (1967), 876 – 888.

Received January 27, 1999

North University of Baia Mare
Victoriei 7
RO–4800 Baia Mare
Romania
e-mail: liancu@ubm.ro

current address:
Institut Girard Desargues
Bat. 101, Université Lyon 1
43 Bd du 11 Novembre 1918
F-69622 Villeurbanne Cedex
France
e-mail: iancu@desargues.univ-lyon1.fr

Quasigroups and Related Systems **6** (1999), 23 – 42

On n-modules with chain conditions

Lăcrimioara Iancu

Abstract

We show that the maximal n-submodules of an n-module are determined by the maximal n-subgroups of the n-group of its zero-idempotents and by the maximal n-submodules of its maximal n-submodule with zero. We state some results concerning R-n-modules with chain conditions analogous to the Jordan–Hölder Theorem, to Fitting's Lemma, to Krull–Remack–Schmidt Theorem.

1. Introduction

R-n-modules are defined as a natural generalization of the usual binary notion. In [5] and [6] we restart the study of n-modules by dropping the restriction imposed by N. Celakoski in [1], namely that the commutative n-group involved has a *unique* neutral element. In this paper we continue our investigation on R-n-modules by studying the maximal n-submodules of an n-module in terms of its canonical presentation and by retrieving some of the results on modules with chain conditions for the n-ary case.

In the sequel, we use the same conventional notations as in [5] and [6]: the sequence $a_i, \ldots, a_j$ of $j-i+1$ terms of an n-ary sum is denoted by a_i^j and if $a_i = a_{i+1} = \ldots = a_j = a$ then the sequence is denoted by $\overset{(j-i+1)}{a}$; if $i > j$, then a_i^j denotes an empty sequence. Denote by $a^{\langle k \rangle}$ the k-th power of a, which is defined by:

$$a^{\langle 0 \rangle} = a \quad \text{and} \quad a^{\langle k \rangle} = [a^{\langle k-1 \rangle}, \overset{(n-1)}{a}]_+, \quad k \in \mathbb{Z}$$

1991 Mathematics Subject Classification: 20N15, 16D10, 16D40
Keywords: R-n-module, maximal n-submodule, chain condition

In particular, $a^{\langle -1\rangle} = \overline{a}$, where $\overline{a}$ denotes the querelement of a.

The purpose of this introductory section is to recall some of the definitions and results in [5] and [6], which will be used in the sections to follow.

Throughout this paper R denotes an associative ring with unity $1 \neq 0$. For reasons similar to the ones employed in the binary case, we deal only with left n-modules and so by R-n-module we will always understand left R-n-module.

Definition 1.1. We call *left R-n-module* a commutative n-group $(M, [\,]_+)$ together with an external operation $\mu\colon R \times M \to M$ which satisfies the axioms:

A1) $\mu(r, [x_1^n]_+) = \big[\mu(r, x_1), \dots, \mu(r, x_n)\big]_+$,

A2) $\mu\big((r_1 + \dots + r_n), x\big) = \big[\mu(r_1, x), \dots, \mu(r_n, x)\big]_+$,

A3) $\mu(r \cdot r', x) = \mu\big(r, \mu(r', x)\big)$,

A4) $\mu(1, x) = x$

for all $x, x_1, \dots, x_n \in M$ and all $r, r', r_1, \dots, r_n \in R$.

Denote the element $\mu(r, x)$ by rx and as immediate consequences of the axioms, note:

$$(r_1{+}r_2)x = [r_1x, r_2x, \overset{(n-2)}{0x}]_+\,, \qquad (-r)x = [0x, 0x, \overset{(n-3)}{rx}, r\overline{x}]_+\,,$$
$$\overline{rx} = r\overline{x}\,, \qquad \overline{x} = (-n{+}2)x = \big((-1){+}\dots{+}(-1)\big)x.$$

The empty n-group may be regarded as an R-n-module for any ring R. If M is a non-empty R-n-module, then it necessarily has at least one neutral element; indeed, for every $x \in M$, the element $0x$ is a neuter in $(M, [\,]_+)$ (or an idempotent, since the two notions coincide in commutative n-groups). Note that $0x^{\langle k\rangle} = 0x$, $\forall x \in M$, $\forall k \in \mathbb{Z}$ (in particular $0x = 0\overline{x}$).

n-Submodules, congruences and homomorphisms are defined in the obvious way. If S is a non-empty n-submodule of an R-n-module M, then the relation ρ_S defined by $x\rho_S y \Leftrightarrow \exists s_2^n \in S : y = [x, s_2^n]_+$ is a congruence on M. This correspondence is not a bijection, still it allows us to define the factor module $M/S = M/\rho_S$.

The set of all neuters of the n-group $(M, [\,]_+)$ is denoted by $\mathcal{N}_M$ (or simply by $\mathcal{N}$) and the set of all neuters of the form $0x$, for some $x \in M$, is denoted by $\mathcal{N}_{0M}$ (or sometimes just $\mathcal{N}_0$). $\mathcal{N}_0$ is a n-submodule of $\mathcal{N}$ and they are both n-submodules of M. The elements of $\mathcal{N}_0$ are called *zero-idempotents* and they are characterized by:

$$e \in \mathcal{N}_0 \Longleftrightarrow re = e, \quad \forall r \in R,$$

which shows that the n-submodules of $\mathcal{N}_0$ coincide with the n-subgroups of $\mathcal{N}_0$. If $\mathcal{N}_0$ consists of exactly one element, then this element is called a *zero* of the n-module and it is denoted by 0.

If $f\colon M_1 \to M_2$ is a homomorphism of R-n-modules, then:

1) $f(\mathcal{N}_1) \subseteq \mathcal{N}_2$ and $f(\mathcal{N}_{01}) \subseteq \mathcal{N}_{02}$,
2) $f(\overline{x}) = \overline{f(x)}$, $\forall x \in M_1$,
3) the set $\operatorname{Ker} f = \{x \in M_1 \mid f(x) \in \mathcal{N}_{02}\}$ is an n-submodule of M_1 and $\mathcal{N}_{01} \subseteq \operatorname{Ker} f$.

The set $\operatorname{Hom}_R(M_1, M_2)$ is a commutative n-group with respect to the operation:

$$[f_1, \ldots, f_n]_+(x) = \big[f_1(x), \ldots, f_n(x)\big]_+ .$$

Any homomorphism α with $\alpha(M_1) \subseteq \mathcal{N}_{02}$ is called *nullary homomorphism* and it is a neutral element of this n-group. For each $e \in \mathcal{N}_{02}$, denote by θ_e the homomorphism given by $\theta_e(x) = e$, $\forall x \in M_1$. The set $\operatorname{End}_R M$ is an $(n, 2)$-ring with respect to the above addition and to the usual multiplication of maps. An endomorphism f of M is called *nilpotent* if there exists an integer $k \geq 1$ such that f^k is a nullary endomorphism.

We have introduced in [5] a class of n-submodules and a class of automorphisms of an R-n-module which play an important role in the study of n-modules. Let M be an R-n-module. For each $e \in \mathcal{N}_0$, the set $M_e = \{x \in M \mid 0x = e\}$ is an n-submodule with zero (the element e) of M. The n-submodules M_e are all isomorphic and they form a partition of M. The maps $\varphi_{e,f}\colon M \to M$, $\varphi_{e,f}(x) = [x, \overset{(n-2)}{e}, f]_+$ are all automorphisms, for each pair of zero-idempotents $e, f \in \mathcal{N}_0$, and $\varphi_{e,f}(M_e) = M_f$. Note that $M/\mathcal{N}_0 \simeq M_e$. In fact, the whole structure of an R-n-module is determined by: the structure of an R-n-module with zero (M_e) and the structure of an idempotent commutative n-group ($\mathcal{N}_0$). This is called the canonical presentation of the R-n-

module M (see [6]).

Injective and surjective homomorphisms are characterized in [6] in terms of the data of the canonical presentation.

Proposition 1.2. *Let $f\colon M_1 \to M_2$ be a homomorphism of R-n-modules. Then f is*

(1) *injective iff* $\operatorname{Ker} f = \mathcal{N}_{01}$ *and the restriction $f|_{\mathcal{N}_{01}}$ is injective,*

(2) *surjective iff for each $e' \in \mathcal{N}_{02}$ there exists $e \in \mathcal{N}_{01}$ such that $M_{2e'} = f(M_{1e})$.*

2. Maximal submodules of an n-module

We study in this section the maximal submodules of an R-n-module, in terms of the canonical presentation of the R-n-module considered.

Theorem 2.1. *Let M be an R-n-module. Then:*

(1) *If N is a maximal n-subgroup of $\mathcal{N}_0$, then there exists a unique maximal n-submodule S of M such that $\mathcal{N}_{0S} = N$.*

(2) *If S is a maximal n-submodule of M, which does not contain $\mathcal{N}_0$, then $\mathcal{N}_{0S}$ is a maximal n-subgroup of $\mathcal{N}_0$.*

Proof. (1) It is easy to check that the set $S = \bigcup\limits_{e\in N} M_e$ is an n-submodule of M, with $\mathcal{N}_{0S} = N$.

Take now an n-submodule T of M with $S \subset T \subseteq M$ and let $x \in T \setminus S$. Then $e = 0x \in T$ and $e \notin S$ (since $e \in S$ implies $x \in S$). This shows that $\mathcal{N}_{0T} \supset \mathcal{N}_{0S} = N$, hence $\mathcal{N}_{0T} = \mathcal{N}_0$.

For any $y \in M$ one of the following holds: (a) $f = 0y \in N$ (and so $y \in S \subset T$) or (b) $f \in \mathcal{N}_0 \setminus N$ (and so $y \notin S$). We show that even in the latter case, we still have $y \in T$. Indeed, $\forall s \in S\, \exists!\, t \in \mathcal{N}_{0S} \subset S$ such that: $y = [f, \overset{(n-2)}{s}, t]_+$. Since $f \in T$, $s, t \in S \subset T$ it follows that $y \in T$. Hence $T = M$ and so S is maximal.

Let V be a maximal n-submodule of M, with $\mathcal{N}_{0V} = N = \mathcal{N}_{0S}$. Then $V \subseteq S$ (indeed, if $x \in V$ then $0x \in \mathcal{N}_{0V} = \mathcal{N}_{0S} = N$, so $x \in S$) which, together with maximality of V, implies $V = S$.

(2) Let S be a maximal n-submodule of M with $\mathcal{N}_0 \setminus S \neq \emptyset$, i.e. $\mathcal{N}_{0S} \subset \mathcal{N}_0$. Consider an n-submodule A of $\mathcal{N}_0$ such that $\mathcal{N}_{0S} \subset A \subseteq$

$\mathcal{N}_0$ and let $e \in A \setminus \mathcal{N}_{0S}$. Then $\langle S \cup \{e\} \rangle = M$ and $\forall a \in \mathcal{N}_0 \, \exists \, k \in \mathbb{N}$ and $s_{k+1}^n \in S$ such that $a = [\overset{(k)}{e}, s_{k+1}^n]_+$. By multiplying with zero, we obtain: $a = 0a = [\overset{(k)}{e}, e_{k+1}^n]_+$, with $e_i = 0s_i$, $i = 1, \ldots, n$ and $e \in M$, $e_i \in \mathcal{N}_{0S} \subset A$, $i = k+1, \ldots, n$. Now, since A is an n-submodule, we deduce that $a \in A$ and so $A = \mathcal{N}_0$. □

The above theorem shows that there exists a bijective correspondence between the set of maximal n-submodules of $\mathcal{N}_0$ and the set of maximal n-submodules of M which do not contain $\mathcal{N}_0$. A natural question arises: what can one say about the maximal n-submodules of M which *do* contain $\mathcal{N}_0$?

Theorem 2.2. *Let M be an R-n-module with the canonical presentation: $B \simeq M_e$, $A \simeq \mathcal{N}_0$. Then:*

(1) *If B has a maximal n-submodule, then M has a maximal n-submodule which contains $\mathcal{N}_0$.*

(2) *If M has a maximal n-submodule which contains $\mathcal{N}_0$, then B has a maximal n-submodule.*

Proof. (1) Let V be a maximal n-submodule of B and take an arbitrary zero-idempotent $e \in \mathcal{N}_0$. Since $B \simeq M_e$, it follows that M_e has a maximal n-submodule S_e which is isomorphic to V. Then for every $f \in \mathcal{N}_0$, the set $S_f = \varphi_{e,f}(S_e)$ is a maximal n-submodule of M_f. Define the subset S of M by: $S = \bigcup\limits_{f \in \mathcal{N}_0} S_f$. We will show that S is a maximal n-submodule of M which contains $\mathcal{N}_0$. Clearly $\mathcal{N}_0 \subseteq S$ (since $f \in S_f$, $\forall f \in \mathcal{N}_0$); equality holds when $V = \{0\}$.

Let $x \in S$; then $\exists f \in \mathcal{N}_0$ such that $x \in S_f$. Since S_f is an n-submodule it follows that $rx \in S_f$, $\forall r \in R$ and so $rx \in S$, $\forall r \in R$.

Let $x_1, \ldots, x_n \in S$; then $\exists f_i \in \mathcal{N}_0$ such that $x_i \in S_{f_i}$ and, consequently, $\exists y_i \in S_e$ such that $x_i = [y_i, \overset{(n-2)}{e}, f_i]_+$. Now we have

$$\begin{aligned} [x_1^n]_+ &= [y_1, \overset{(n-2)}{e}, f_1, \ldots, y_n, \overset{(n-2)}{e}, f_n]_+ \\ &= [[y_1^n]_+, \overset{(n-2)}{e}, [f_1^n]_+]_+ \in \varphi_{e,[f_1^n]_+}(S_e) = S_{[f_1^n]_+} \subseteq S \end{aligned}$$

and so S is an n-submodule of A.

Let T be an n-submodule of M, $S \subset T \subseteq M$ and take $x \in T \setminus S$. Define $u = 0x$ and we have $x \in M_u \setminus S_u$. Then $\tilde{x} = \varphi_{u,e}(x) \in M_e \setminus S_e$ (if $\tilde{x} \in S_e$ then $\varphi_{e,u}(\tilde{x}) = (\varphi_{e,u} \circ \varphi_{u,e})(x) = x \in S_u$, contradiction) and $\tilde{x}_f = \varphi_{e,f}(\tilde{x}) \in M_f \setminus S_f$, $\forall f \in \mathcal{N}_0$ (if $\tilde{x}_f \in S_f$ then $\exists z \in S_e$ such that $\tilde{x}_f = \varphi_{e,f}(z)$, or $\varphi_{e,f}(\tilde{x}) = \varphi_{e,f}(z)$ which implies $\tilde{x} = z \in S_e$, contradiction). Hence T contains at least one such element $\tilde{x}_f$ for each set $M_f \setminus S_f$, $f \in \mathcal{N}_0$ and so $M_f = \langle S_f \cup \{\tilde{x}_f\}\rangle$, $\forall f \in \mathcal{N}_0$. Now $\forall y \in M$ $\exists f \in \mathcal{N}_0$ such that $y \in M_f$; then there exists $k \in \mathbb{N}$ and $s_{k+1}, \ldots, s_n \in S_f$ such that: $y = [\overset{(k)}{\tilde{x}_f}, s_{k+1}^n]_+$. Since $\tilde{x}_f \in T$ and $s_{k+1}, \ldots, s_n \in S_f \subseteq S \subset T$, it follows that $y \in T$ and this shows that $T = M$.

(2) Let $S \subset M$ be a maximal n-submodule of M which contains $\mathcal{N}_0$. For each $e \in \mathcal{N}_0$ define the subset S_e of S by: $S_e = \{x \in S \mid 0x = e\}$. Clearly, $S_e = S \cap M_e$ and so S_e is an n-submodule of M_e (and of S). Moreover, $S = \bigcup\limits_{e \in \mathcal{N}_0} S_e$.

We show that, for any $e \in \mathcal{N}_0$, the n-submodule S_e is maximal in M_e. For this, let T be an n-submodul of M_e, $S_e \subset T \subseteq M_e$ and take $x \in T \setminus S_e$. Then $x \notin S$ and so $\langle S \cup \{x\}\rangle = M$. It follows that $\forall y \in M_e$ $\exists k \in \mathbb{N}$ and $s_{k+1}, \ldots, s_n \in S$ such that

$$y = [\overset{(k)}{x}, s_{k+1}^n]_+ = [\overset{(k)}{x}, \overset{(n-k-1)}{e}, [\overset{(k)}{e}, s_{k+1}^n]_+]_+.$$

By multiplying with 0 we obtain that the element $[\overset{(k)}{e}, s_{k+1}^n]_+ \in S$ belongs to M_e, which means that $[\overset{(k)}{e}, s_{k+1}^n]_+ \in S_e$. Since $x \in T$ and $e, [\overset{(k)}{e}, s_{k+1}^n]_+ \in S_e \subset T$, then $y \in T$. Hence $T = M_e$. □

The above theorem shows that an n-module M has maximal n-submodules which contain $\mathcal{N}_0$ if and only if the n-submodules M_e have maximal n-submodules.

Definition 2.3. An R-n-module M is *simple* if its only congruences are the equality and the universal relation.

Remark 2.4. 1) M is simple iff its only non–void n-submodules are: $\{e\}$, with $e \in \mathcal{N}_0$ and M itself.
2) M is simple iff it has one of this canonical presentations:

(a) a simple R-n-module with zero and $\mathcal{N}_0 = \{0\}$,
(b) the R-n-module with zero is $B = \{0\}$ and $\mathcal{N}_0$ is a simple idempotent commutative n-group.

Theorem 2.5. *Let M be an R-n-module and $S \subset M$ be a non-void n-submodule. S is maximal iff M/S is simple.*

Proof. Suppose M/S is simple and let T be an n-submodule of M, with $S \subseteq T \subseteq M$. Then T/S is an n-submodule of M/S and so T/S either consists of exactly one coset (which is obviously S, since $T \supseteq S$), or $T/S = M/S$. Now $T/S = M/S$ implies that $\forall x \in M$, $\exists t \in T$, $s_1^{n-1} \in S \subseteq T$ such that $x = [t, s_1^{n-1}]_+$, i.e. $x \in T$. This shows that either $T = S$ or $T = M$.

Suppose S is maximal and consider two cases: $\mathcal{N}_0 \subseteq S$ or $\mathcal{N}_0 \setminus S \neq \emptyset$. If $\mathcal{N}_0 \subseteq S$ then M/S is an n-module with zero. Let now T be an n-submodule of M/S. Then $p^{-1}(T)$ is an n-submodule of M which contains S, so we have either $p^{-1}(T) = S$ or $p^{-1}(T) = M$. This shows that T is either the zero n-submodule or $T = M/S$.

If $\mathcal{N}_0 \setminus S \neq \emptyset$, then M/S does not have a zero element; we prove first that each coset $\hat{x} \in M/S$ contains at least one idempotent $e \in \mathcal{N}_0$ or, equivalently, that each coset is an n-submodule of M. Take now a coset $\hat{y} \in M/S$, $\hat{y} \neq S$ and a zero-idempotent $e \in \mathcal{N}_0 \setminus S$. Then $S \subset \langle S \cup \{e\} \rangle$ and so $\langle S \cup \{e\} = M$, hence y can be expressed as $y = [\overset{(k)}{e}, s_{k+1}^n]_+$, with $k \geq 1, s_{k+1}^n \in S$, and further

$$y = \big[[\overset{(k)}{e}, \overset{(n-k)}{f}]_+, \overset{(k-1)}{f}, s_{k+1}^n\big]_+ = [e', \overset{(k-1)}{f}, s_{k+1}^n]_+,$$

for any $f \in \mathcal{N}_0 \cap S$. This shows that $e' \in \hat{y}$.

Thus we have proved that each coset $\hat{x} \in M/S$ is an n-submodule of M. If $\hat{e} \in M/S$ and $f \in \mathcal{N}_0 \cap S$, then $\varphi_{f,e}(S)$ is a maximal n-submodule of M, which is contained in $\hat{e}$, hence $\varphi_{f,e}(S) = \hat{e}$. Take now an n-submodule T of M/S. If T consists of more than one element, say $\hat{e}, \hat{f} \in T$, then we have $\hat{e} \subset p^{-1}(T) \subseteq M$. This implies, since $\hat{e}$ – as n-submodule of M – is maximal, that $p^{-1}(T) = M$, and so $T = M/S$. □

Proposition 2.6. *If M is a simple R-n-module, then every endomorphism of M is either of type θ_e or an automorphism.*

Proof. If M is simple, then by Remark 2.4 it follows that either M

has a zero element and exactly two n-submodules: $\{0\}$ and M, or $M = \mathcal{N}_{0M}$ and its submodules are: $\{x\}$, $\forall x \in M$ and M. In the first case, if $f \in \mathrm{End}_R(M)$ then either $\mathrm{Ker}\, f = \{0\}$ or $\mathrm{Ker}\, f = M$, i.e. f is either injective or the zero endomorphism. If f is injective, then $\mathrm{Im} f = M$.

In the second case, either $\mathrm{Im} f = M$ or $\mathrm{Im} f = \{e\}$, $e \in M$, i.e. either f is surjective or $f = \theta_e$. If f is surjective, let $e \in M$. Then $f^{-1}(e)$ is a non–void n-submodule of M, so it is either a one–element set or the whole of M. Since f is surjective, it follows that $\forall e \in M$, the set $f^{-1}(e)$ consists of one element only. □

3. Artinian and Noetherian n-modules

Definition 3.1. An R-n-module M is called *Artinian* if the set of its n-submodules satisfies the DCC (Descending Chain Condition), and it is called *Noetherian* if the set of its n-submodules satisfies the ACC (Ascending Chain Condition).

Note that every n-submodule of an Artinian (Noetherian) n-module is Artinian (Noetherian) too.

As in the binary case, the following characterization of a Noetherian n-module holds:

Proposition 3.2. *An R-n-module is Noetherian iff any n-submodule of M is finitely generated.*

Proof. Similar to the one for the binary case (see [8]). If M is Noetherian and S is an n-submodule of M, it follows that the set of all finitely generated n-submodules of S contains a maximal element A. Since A is finitely generated, it follows that $\forall x \in S$, the n-submodule $\big[\overset{(n-1)}{A}, Rx\big]_+$ of S is finitely generated which, together with the maximality of A, implies $\big[\overset{(n-1)}{A}, Rx\big]_+ = A$, and so $x \in A$. This proves that $S = A$. For the converse, see the proof for the binary case. □

Proposition 3.3. *If $A \xrightarrow{f} B \xrightarrow{g} C \to 0$, is an exact sequence of R-n-modules and the homomorphism f is injective, then:*

1) *B is Artinian iff A and C are Artinian,*

2) *B is Noetherian iff A and C are Noetherian.*

Proof. 1) Suppose B is Artinian. Since f is injective, it follows that A is isomorphic to the n-submodule $f(A)$ of B, and hence it is Artinian. Let $C_1 \supseteq C_2 \supseteq C_3 \supseteq \dots$ be a descending chain of n-submodules of C. Then $g^{-1}(C_1) \supseteq g^{-1}(C_2) \supseteq g^{-1}(C_3) \supseteq \dots$ is a descending chain of n-submodules of B (with $g^{-1}(C_k) \neq \emptyset$, if $C_k \neq \emptyset$). Since B is Artinian, it follows that there exists $k > 0$ such that $g^{-1}(C_m) = g^{-1}(C_k)$, for $m > k$. But this implies – since g is surjective – that $C_m = C_k$, for $m > k$.

Conversely, assume A and C are Artinian and let

$$B_1 \supseteq B_2 \supseteq B_3 \supseteq \dots \tag{dc}$$

be a descending chain of n-submodules of B. By intersecting the terms of the chain *(dc)* with $f(A)$, we obtain a descending chain of n-submodules of $f(A)$:

$$B_1 \cap f(A) \supseteq B_2 \cap f(A) \supseteq B_3 \cap f(A) \supseteq \dots .$$

Since $f(A)$ is Artinian, it follows that there exists $k > 0$ such that $B_m \cap f(A) = B_k \cap f(A)$, for $m > k$. By applying g to the terms of the chain *(dc)* we obtain the descending chain of n-submodules of C:

$$g(B_1) \supseteq g(B_2) \supseteq g(B_3) \supseteq \dots,$$

so there exists $l > 0$ such that $g(B_m) = g(B_l)$, for $m > l$. Define $t = \max\{k, l\}$; we show that $B_m = B_t$, for $m > t$. Note that if $g(B_l) = \emptyset$, then $B_l = \emptyset$, hence $B_m = B_l = \emptyset$, for $m > l$; similarly, if $B_k \cap f(A) = \emptyset$, then $B_k \cap \mathcal{N}_{0B} = \emptyset$ (because $f(A) = \operatorname{Ker} g \supseteq \mathcal{N}_{0B}$), hence $B_k = \emptyset$, i.e. $B_m = B_k = \emptyset$, for $m > k$. We may therefore assume that $B_k \cap f(A) \neq \emptyset$ and $g(B_l) \neq \emptyset$. Let $b \in B_t$; $g(B_t) = g(B_m)$ implies that $\exists b' \in B_m$ such that $g(b) = g(b')$. For $e \in B_m \cap \mathcal{N}_{0B}$ (such an element exists, since $B_m \neq \emptyset$) we have:

$$\big[g(b), \overset{(n-3)}{g(b')}, g(\overline{b'}), g(e)\big]_+ = g(e) \in \mathcal{N}_{0C}$$

and hence $[b, \overset{(n-3)}{b'}, \overline{b'}, e]_+ \in \operatorname{Ker} g$. Since $m > t$, we have $B_m \subseteq B_t$ and

$$[b, \overset{(n-3)}{b'}, \overline{b'}, e]_+ \in B_t \cap \operatorname{Ker} g = B_t \cap f(A) = B_m \cap f(A).$$

Now $[b, \overset{(n-3)}{b'}, \overline{b'}, e]_+ \in B_m$, $b', e \in B_m$ implies $b \in B_m$. This shows that $B_t \subseteq B_m$.

2) The fact that if B is Noetherian then A and C are Noetherian is proved by a similar argument as above.

For the converse, we make the same constructions and use the same notations (of course by using an ascendant chain this time). We will show that $B_m = B_t$, for $m > t$. Let $b \in B_m$; $g(B_t) = g(B_m)$ implies that $\exists b' \in B_t$ such that $g(b) = g(b')$. For $e \in B_t \cap \mathcal{N}_{0B}$ we have $\big[g(b), \overset{(n-3)}{g(b')}, g(\overline{b'}), g(e)\big]_+ = g(e) \in \mathcal{N}_{0C}$ and hence $[b, \overset{(n-3)}{b'}, \overline{b'}, e]_+ \in \operatorname{Ker} g$. Since $m > t$, we have $B_t \subseteq B_m$ and

$$[b, \overset{(n-3)}{b'}, \overline{b'}, e]_+ \in B_m \cap \operatorname{Ker} g = B_m \cap f(A) = B_t \cap f(A).$$

Now $[b, \overset{(n-3)}{b'}, \overline{b'}, e]_+, b', e \in B_t$ implies $b \in B_t$ and this shows that $B_m \subseteq B_t$. □

Corollary 3.4.

1) *If S is an n-submodule of the R-n-module A, then A is Artinian (Noetherian) iff S and A/S are Artinian (Noetherian).*
2) *Let $A_1, \ldots, A_m$ be R-n-modules with zero. The R-n-module $A_1 \times \cdots \times A_m$ is Artinian (Noetherian) iff $A_1, \ldots, A_m$ are all Artinian (Noetherian).*

Proof. 1) The sequence $S \xrightarrow{i} A \xrightarrow{p} A/S \to 0$, where i is the inclusion and p is the natural homomorphism, satisfies the hypotheses of the preceding proposition.

2) The sequence $A_1 \times \cdots \times A_{n-1} \xrightarrow{f} A_1 \times \cdots \times A_n \xrightarrow{p_n} A_n \to 0$ is exact and the homomorphism f defined by

$$f\big((a_1, \ldots, a_{n-1})\big) = (a_1, \ldots, a_{n-1}, 0)$$

is injective. □

Lemma 3.5. *Let B_1, B, C_1, C be n-submodules of the R-n-module M, with $B_1 \subseteq B \subseteq M$, $C_1 \subseteq C \subseteq M$, $B_1 \cap C_1 \neq \emptyset$. Then*

$$\langle B_1 \cup (B \cap C)\rangle / \langle B_1 \cup (B \cap C_1)\rangle \simeq \langle C_1 \cup (B \cap C)\rangle / \langle C_1 \cup (B_1 \cap C)\rangle.$$

Proof. Identical to the one for the binary case (see [4]); we can apply the isomorphism theorems because $B_1 \cap C_1 \neq \emptyset$. □

Lemma 3.6. (*Schreier*) *Let* $M = S_0 \supseteq S_1 \supseteq \ldots \supseteq S_r = e$ *and* $M = T_0 \supseteq T_1 \supseteq \ldots \supseteq T_s = e$ *be two chains of* n*-submodules of the* R*-*n*-module* M*, where* $e \in \mathcal{N}_0$*. Define* $S_{ij} = \langle S_i \cup (S_{i-1} \cap T_j)\rangle$ *and* $T_{ij} = \langle T_j \cup (T_{j-1} \cap S_i)\rangle$*, for all* $0 \leqslant i \leqslant r$, $0 \leqslant j \leqslant s$*, and we obtain isomorphic refinements of the two chains:*

$$S_{i-1} = S_{i0} \supseteq S_{i1} \supseteq \ldots \supseteq S_{is} = S_i, \quad 0 \leqslant i \leqslant r$$
$$T_{j-1} = T_{0j} \supseteq T_{1j} \supseteq \ldots \supseteq T_{rj} = T_j, \quad 0 \leqslant j \leqslant s$$
$$S_{i,j-1}/S_{ij} \simeq T_{i-1,j}/T_{ij}\,.$$

Proof. Identical to the one for the binary case (see [4]); the preceding lemma is applicable because the zero-idempotent e belongs to each term of the two chains. □

The definition of a composition series of an R-n-module is naturally transferred from R-modules, namely: a *composition series* of an R-n-module M is a finite, strictly decreasing series of n-submodules of M,

$$M = S_0 \supset S_1 \supset \ldots \supset S_m = \{e\}, \quad e \in \mathcal{N}_0 \qquad \text{(c)}$$

which does not admit strictly decreasing refinements. The series (c) is a composition series of M iff each S_i, $i = \{1, \ldots, m\}$ is a maximal n-submodule of S_{i-1}, i.e. iff the factor n-modules S_{i-1}/S_i are simple. One can easily check the validity of the Jordan-Hölder Theorem, with just one additional comment: if

$$M = S_0 \supset S_1 \supset \ldots \supset S_m = \{e\} \qquad (c_1)$$
$$M = T_0 \supset T_1 \supset \ldots \supset T_r = \{f\} \qquad (c_2)$$

are two composition series of M, then in order to use Schreier's Lemma one needs that the series (c_1) and (c_2) have the same last term. For this purpose, we apply to each term of the series (c_2) the automorphism $\varphi_{f,e}$ and we obtain the series:

$$\varphi_{f,e}(M) = M \supset \varphi_{f,e}(T_1) \supset \ldots \supset \varphi_{f,e}(T_r) = \{e\} \qquad (c_3)$$

which is still a composition series. Schreier's Lemma may now be applied. So, if an R-n-module M has a composition series, then all its composition series have the same length, and this will be called *the length of M* (and we say that M has finite length). If M does not have composition series, then we say it has infinite length.

As in the binary case, the following hold:

1) *If S is an n-submodule of M, then* $l(M) = l(S) + l(M/S)$.
2) *If S_1, S_2 are n-submodules of M, then*
$$l(S_1) + l(S_2) = l(\langle S_1 \cup S_2 \rangle) + l(S_1 \cap S_2).$$
3) *If the sequence $A \xrightarrow{f} B \xrightarrow{g} C \to 0$ is exact and the homomorphism f is injective, then* $l(B) = l(A) + l(C)$.

By using a similar argument to the one employed for usual R-modules (see [8]), one proves the following

Theorem 3.7. *An R-n-module M has composition series (i.e. M has finite length) iff M is Artinian and Noetherian.*

Proposition 3.8. *Let $f\colon M \to M$ be an endomorphism of the R-n-module M.*

1) *If M is Artinian, then f is an automorphism iff f is injective.*
2) *If M is Noetherian, then f is an automorphism iff f is surjective.*

Proof. 1) Assume f is injective; then $M \supseteq f(M) \supseteq f^2(M) \supseteq \ldots$, hence there exists m such that $f^m(M) = f^{m+1}(M) = \ldots$. This implies that $\forall y \in M \exists x \in M$ such that $f^m(y) = f^{m+1}(x)$, so $y = f(x)$.

2) Assume f is surjective; then $\mathcal{N}_0 \subseteq f^{-1}(\mathcal{N}_0) \subseteq f^{-2}(\mathcal{N}_0) \subseteq \ldots$, hence there exists m such that $f^{-m}(\mathcal{N}_0) = f^{-(m+1)}(\mathcal{N}_0) = \ldots$. Now take $x \in \operatorname{Ker} f$, that is, $f(x) \in \mathcal{N}_0$. Since f^m is surjective, $\exists x' \in M$ such that $x = f^m(x')$, whence $f^{m+1}(x') = f(x) \in \mathcal{N}_0$, or $x' \in f^{-(m+1)}(\mathcal{N}_0) = f^{-m}(\mathcal{N}_0)$. So $f^m(x') \in \mathcal{N}_0$ and $x \in \mathcal{N}_0$. This proves that $\operatorname{Ker} f = \mathcal{N}_0$ and, since f is surjective, that $f(\mathcal{N}_0) = \mathcal{N}_0$. We may then define the surjective endomorphism

$$f_1\colon \mathcal{N}_0 \to \mathcal{N}_0,\ f_1(x) = f(x),\ \forall x \in \mathcal{N}_0.$$

Being Noetherian, M is finitely generated, which in turn implies that $\mathcal{N}_0$ is finite (see [6], Theorem 3.3) and so f_1 is injective too. This shows (by 1.2) that f is also injective. □

Corollary 3.9. *If $f : M \to M$ is an endomorphism of an R-n-module of finite length, then the following are equivalent:*

1) *f is an automorphism,*
2) *f is injective,*
3) *f is surjective.*

Definition 3.10. Let M be an R-n-module and let $\{M_i\}_{i\in I}$ be a family of n-submodules of M. We say that M is the *(internal) direct sum* of the family $\{M_i\}_{i\in I}$ if

(1) $M = \langle\bigcup\limits_{i\in I} M_i\rangle$

(2) there exists an n-submodule N of $\mathcal{N}_0$ such that for every $j \in I$ we have $M_j \cap \langle\bigcup\limits_{i\neq j} M_i\rangle = N$.

In this case, we say that M is the N-*direct sum* of the family $\{M_i\}_{i\in I}$; in particular, for $N = \emptyset$ or $N = \{e\}$ we call it *0-direct sum* or *1-direct sum*, respectively.

Remark 3.11. 1) Every n-submodule $\emptyset \neq N \subseteq \mathcal{N}_0$ determines an N-decomposition of M, namely: $M = \bigcup\limits_{e\in N} M_e \oplus \mathcal{N}_0$. In particular, for each zero-idempotent $e \in \mathcal{N}_0$ we have a decomposition of M into a 1-direct sum:

$$M = M_e \oplus \mathcal{N}_0 \tag{D}$$

2) For each zero-idempotent $e \in \mathcal{N}_0$ we have a class of decompositions of M into 0-direct sums:

$$M = M_e \oplus \left(\oplus_{f\neq e} T_f\right) \tag{D'}$$

where each T_f is equal either to M_f or to $\{f\}$.

Definition 3.12. An n-module B with zero is called *decomposable* if B can be expressed as a direct sum $B = B_1 \oplus B_2$, with $B_1 \neq \{0\}$ and $B_2 \neq \{0\}$. Otherwise, B is called *indecomposable*.

An n-module M is called *indecomposable* if M_e is indecomposable and $\mathcal{N}_0$ is simple.

Remark 3.13. 1) Simple n-modules are indecomposable.

2) An n-submodule N of $\mathcal{N}_0$ is indecomposable iff it is simple.
3) If the n-module M is indecomposable, then its only decompositions in which M itself does not appear as a summand, are those of the forms (D) and (D').

Definition 3.14. A decomposition of an n-module into a direct sum of n-submodules is called a *canonical decomposition* if

(1) it is obtained from (D) by further decomposition of the two summands,
(2) the direct sum employed is a 1-direct sum,
(3) it does not contain summands which are one-element sets or the empty set.

In a canonical decomposition the summands are either n-modules with zero or n-submodules (n-subgroups) of $\mathcal{N}_0$.

Theorem 3.15. (*Fitting's lemma*) *If M is an R-n-module of finite length and $f\colon M \to M$ is an endomorphism, then there exists an integer $m \geqslant 1$ such that $M = f^m(M) \oplus \operatorname{Ker} f^m$.*

Proof. Similar to the one for the binary case (see [7] or [8]). Since M is Artinian, it follows – as in the proof of the preceding theorem – that there exists $m \geqslant 1$ such that $f^m(M) = f^{m+1}(M) = \ldots$, whence $f^m(M) = f^{2\cdot m}(M)$. Define the map $g\colon f^m(M) \to f^m(M)$, $g(x) = f^m(x)$ and note that g is a surjective endomorphism. Now $f^m(M)$ is Noetherian, being an n-submodule of M, so g is an automorphism. Therefore, we have

$$f^m(M) \cap \operatorname{Ker} f^m = \operatorname{Ker} g = \mathcal{N}_{0f^m(M)} \subseteq \mathcal{N}_0.$$

In addition to that, for any $x \in M$ there exists $y \in M$ such that $f^m(x) = g\big(f^m(y)\big)$ and so

$$\big[f^m(x), \overset{(n-3)}{f^m(f^m(y))}, f^m(f^m(\overline{y})), f^m(e)\big]_+ = f^m(e),$$

$\forall e \in \mathcal{N}_0$. It follows that the element $u = \big[x, \overset{(n-3)}{f^m(y)}, f^m(\overline{y}), e\big]_+$ belongs to $\operatorname{Ker} f^m$ and: $x = [f^m(y), u, \overset{(n-2)}{e}]_+$.

This shows that $M = \big\langle f^m(M) \cup \operatorname{Ker} f^m \big\rangle$. □

Corollary 3.16. *Assume that M is an indecomposable R-n-module* *of finite length.*

1) *If* f *is an endomorphism of* M*, then:*
   a) f *is an automorphism or*
   b) $\operatorname{Ker} f = \mathcal{N}_0$, $\exists e \in \mathcal{N}_0 :\ f(M) = M_e$ *and the map* $g\colon M_e \to M_e,\ g(x) = f(x)$ *is an automorphism or*
   c) f *is nilpotent in the* $(n,2)$*-ring* $\operatorname{End}_R M$.
2) *If* M *is with zero, then any endomorphism of* M *is either nilpotent or an automorphism.*
3) *If* M *is with zero, and* $f_i \in \operatorname{End}_R M$, $i \in \{1, 2, \dots, m\}$, $m \equiv r(\mathrm{mod} n{-}1)$, *while* $f = [f_1, \dots, f_m, \overset{(n-r)}{\theta}]_+$ *is an automorphism, then there exists* $i_0 \in \{1, \dots, m\}$ *such that* f_{i_0} *is an automorphism.*

Proof. 1) It follows from the preceding theorem that there exists $m \geqslant 1$ such that $M = f^m(M) \oplus \operatorname{Ker} f^m$. Since M is indecomposable, we have either $f^m(M) = \mathcal{N}_0$ or $\operatorname{Ker} f^m = \mathcal{N}_0$. In the first case, f^m is a nullary endomorphism and so f is nilpotent; in the second case we have either $f^m(M) = M$ or $f^m(M) = M_e$, for a certain $e \in \mathcal{N}_0$. If $f^m(M) = M$, then $f(M) = M$, so f is a surjective homomorphism and from Corollary 3.9 it follows that f is an automorphism. If $f^m(M) = M_e$, then (as in the proof of the preceding theorem) $M_e = f^m(M) = f^{m+1}(M) = f(M_e)$ and therefore the endomorphism $g\colon M_e \to M_e$ is surjective, so (by Corollary 3.9) it is an automorphism.

Now $\operatorname{Ker} f^m = \mathcal{N}_0$ implies that $\operatorname{Ker} f = \mathcal{N}_0$, while the fact that $\mathcal{N}_0$ is simple implies that $f(\mathcal{N}_0)$ is either a one-element set or the whole of $\mathcal{N}_0$. If $f(\mathcal{N}_0) = \mathcal{N}_0$, then the map $h\colon \mathcal{N}_0 \to \mathcal{N}_0$ is a surjective endomorphism, so an automorphism. But this fact, together with $\operatorname{Ker} f = \mathcal{N}_0$, implies that f is injective, hence f is an automorphism, which contradicts $f^m(M) = M_e$. Therefore there exists $u \in \mathcal{N}_0$ such that $f(\mathcal{N}_0) = \{u\}$; now $f(M_e) = M_e$ implies that $u = e$. Take now $y \in f(M)$ and $x \in M$ cu $y = f(x)$. If $x \in M_e$, then $y = f(x) \in M_e$; if $x \in M_v$, $v \neq e$, then let x' be the uniquely determined element of M_e such that $x = [x', \overset{(n-2)}{e}, v]_+$. Now we have

$$y = f(x) = [f(x'), \overset{(n-2)}{f(e)}, f(v)]_+ = [f(x'), \overset{(n-1)}{e}]_+ = f(x') \in M_e$$

which proves that $f(M) \subseteq M_e$.

2) Direct consequence of 1).

3) The proof is by induction on m.

If $m = 1$, then $f = [f_1, \overset{(n-1)}{\theta}]_+ = f_1$, so f_1 is an automorphism. Let now $m \geqslant 2$ and assume that the statement is true for $m-1$. The equation $f = [f_1, \ldots, f_m, \overset{(n-r)}{\theta}]_+$ implies, by right multiplication with f^{-1}, the following:

$$\mathrm{id}_M = [g_1, \ldots, g_m, \overset{(n-r)}{\theta}]_+ ,$$

where $g_i = f_i \circ f^{-1}$. If g_1 is an automorphism, then f_1 is an automorphism and $i_0 = 1$; otherwise, it follows from 2) that g_1 is nilpotent, i.e. $\exists k \geqslant 1$ such that $g_1^k = \theta$. It follows now

$$[\mathrm{id}_M, \overset{(n-3)}{g_1}, \overline{g_1}, \theta]_+ \circ [\mathrm{id}_M, g_1, \ldots, g_1^{k-1}, \overset{(n-t)}{\theta}]_+$$
$$= \mathrm{id}_M = [\mathrm{id}_M, g_1, \ldots, g_1^{k-1}, \overset{(n-t)}{\theta}]_+ \circ [\mathrm{id}_M, \overset{(n-3)}{g_1}, \overline{g_1}, \theta]_+$$

and so the map

$$[\mathrm{id}_m, \overset{(n-3)}{g_1}, \overline{g_1}, \theta]_+ = [g_2, \ldots, g_m, \overset{(n-r+1)}{\theta}]_+$$

is an automorphism for which we can apply the induction hypothesis. This completes the proof. □

Using arguments identical to those employed in the binary case ([7], [8]), one can prove the following

Theorem 3.17. *If A is an R-n-module with zero, Artinian or Noetherian, then M can be decomposed as a finite direct sum of indecomposable n-submodules.*

Also the Krull–Remack–Schmidt Theorem can be immediately transferred to the case of R-n-modules with zero: Let $B \neq \{0\}$ be an R-n-module with zero which is both Artinian and Noetherian. Then B is a finite direct sum of indecomposable n-submodules. Up to a permutation, the indecomposable components in such a direct sum are uniquely determined up to isomorphism.

Remark 3.18. Let us return now to the general case of R-n-modules (not necessarily with zero): it follows that the problem of decomposing an R-n-module M of finite length into a finite direct sum of indecomposables can be reduced to the decomposition of $\mathcal{N}_{0M}$ (since $M = M_e \oplus \mathcal{N}_{0M}$ and M_e is an n-module with zero). Recall that if M is Noetherian, then the idempotent abelian n-group $\mathcal{N}_{0M}$ is finite and $|\mathcal{N}_{0M}|$ divides $(n-1)^{k-1}$, where k is the cardinal of the generating set. Also recall that, by Remark 3.13, an n-submodule of $\mathcal{N}_0$ is indecomposable if and only if it is simple. Take $e \in \mathcal{N}_{0M}$ and let $G = \operatorname{red}_e \mathcal{N}_{0M}$ be the binary reduce of $\mathcal{N}_{0M}$ with respect to the element e (i.e. $x + y = [x, \overset{(n-2)}{e}, y]_+$); G is a (bi)group of exponent $n-1$. Note that $x_1 + \cdots + x_n = [x_1^n]_+$, which shows that $\mathcal{N}_{0M} = \operatorname{ext}^n G$. Take the decomposition (unique up to isomorphism) of G into a direct sum of indecomposable subgroups of the form $\mathbb{Z}_{p^r}$, with p prime:

$$G = G_1 \oplus \cdots \oplus G_t \tag{d_1}$$

and immediately obtain the following decomposition for $\mathcal{N}_{0M}$:

$$\mathcal{N}_{0M} = \operatorname{ext}^n G = \operatorname{ext}^n G_1 \oplus \cdots \oplus \operatorname{ext}^n G_t \tag{d_2}$$

We still did not solve the problem, since not all these summands are simple: in fact, $\operatorname{ext}^n G_i$ is simple iff G_i is of the form $\mathbb{Z}_p$, p prime. So, it remains to describe the possible decompositions of $\operatorname{ext}^n \mathbb{Z}_{p^r}$, $r > 1$, where $p^r \mid n-1$. Unfortunately, for this case one cannot prove the uniqueness of decomposition, as the following example shows.

Example 3.19. Take $n = 9$ and $A = \operatorname{ext}^9 \mathbb{Z}_8$. The 9-group A has four 9-subgroups of order 2, namely: $A_1 = \{1,5\}, A_2 = \{2,6\}, A_3 = \{3,7\}, A_4 = \{0,4\}$ and the following decompositions into direct sums:

$$\begin{aligned} A =& A_1 \oplus A_2 = A_1 \oplus A_4 = A_3 \oplus A_2 = A_3 \oplus A_4 \\ =& A_i \oplus A_j \oplus A_k = A_1 \oplus A_2 \oplus A_3 \oplus A_4 \end{aligned}$$

where i, j, k are distinct numbers in $\{1,2,3,4\}$. Note that the four 9-subgroups of order 2 are mutually disjoint, which means that any decomposition of A into direct sum of indecomposables is necessarily a 0-direct sum; it is easy to check that in fact this statement is true for any n-group of the form $\operatorname{ext}^n \mathbb{Z}_{p^r}$, with $r > 1$ and $p^r \mid n-1$. Also note that $A_1 \oplus A_3 = \{1,3,5,7\} \simeq \operatorname{ext}^9 \mathbb{Z}_4$, which shows that 0-direct sums with respectively isomorphic summands can give non-isomorphic results.

Summarizing, if M is a Noetherian R-n-module, then one of the following situations occurs:

- $\mathcal{N}_{0M}$ is simple. This is precisely the case when its order is a prime number p (with $p \mid n-1$);
- $\mathcal{N}_{0M}$ is not simple and it has a unique (up to isomorphism) decomposition into a finite 1-direct sum of indecomposable n-submodules. This is precisely the case when every binary reduce has in its decomposition (d_1) only summands of the form $\mathbb{Z}_{p_i}$, with p_i prime numbers.
- $\mathcal{N}_{0M}$ is not simple and it can be decomposed into finite 0-direct sums of indecomposables only. This is precisely the case when every binary reduce has at least one summand of the form $\mathbb{Z}_{p^r}$, p prime and $r > 1$, in the decomposition (d_1).

The above discussion leads us to a weaker version of the Krull–Remack–Schmidt theorem for n-modules, in the special case when $n-1 = p_1 \dots p_k$ (the prime factorization of $n-1$ is multiplicity-free).

Theorem 3.20. *Let $n > 2$ be an integer such that $n-1 = p_1 \dots p_k$ and let M be an R-n-module which is both Artinian and Noetherian. Then M has a finite canonical decomposition into indecomposable n-modules. Up to a permutation, the indecomposable components are uniquely determined up to isomorphism.*

The above theorem allows us to reduce the problem of decomposing an R-n-module into a direct sum of indecomposable n-submodules to the problem of decomposing an R-n-module with zero and an abelian n-group. Both these decompositions can be done by using the binary reduces of the two structures and then their n-ary extensions. To be more precise, if B is an R-n-module with zero, then its *binary reduce* with respect to an element $b \in B$ is the module B with the operations:

$$x + y = [x, \overset{(n-3)}{b}, \overline{b}, y]_+, \qquad r \bullet x = [rx, \overset{(n-3)}{rb}, r\overline{b}, b]_+ ,$$

for our purpose (decomposition), it is useful to consider the binary reduce with respect to the zero element. The *n-ary extension* with respect to an element a of an R-module A is the R-n-module A, with the following operations:

$$[x_1^n]_+ = x_1 + \cdots + x_n - (n-1)a\,, \qquad r \star x = rx - ra + a\,,$$

and a is the zero element in the n-ary extension. Furthermore, one can easily check that for any $a, b \in B$ we have $\mathrm{ext}_b^n(\mathrm{red}_a\, M) \simeq M$; in particular, $\mathrm{ext}_0^n(\mathrm{red}_0\, M) = M$. Note that we can talk about unique decomposition only if it is canonical, as the following example shows.

Example 3.21. Let $(\mathbb{Z}_{30}, +, \cdot)$ be the ring of integers *modulo* 30. We define on the set $M = \mathbb{Z}_{30}$ a structure of $\mathbb{Z}$-7-module by:

$$[x_1^7]_+ = x_1 + \cdots + x_7 \quad \text{and} \quad k \bullet x = (6k+25) \cdot x\,.$$

Then we have

$$\mathcal{N}_M = \mathcal{N}_{0M} = \{0, 5, 10, 15, 20, 25\},\ M_0 = \{0, 6, 12, 18, 24\}$$

and the following canonical decomposition of M:

$$M = \{0, 6, 12, 18, 24\} \oplus \{0, 15\} \oplus \{0, 10, 20\}$$

which is unique up to isomorphism.

However, we can give two different (non–canonical) decompositions of M into 1-direct sums of indecomposable n-submodules, namely:

$$\begin{aligned} M =& \{0, 3, 6, 9, 12, 15, 18, 21, 24, 27\} \oplus \{0, 10, 20\} \\ =& \{0, 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, 26, 28\} \oplus \{0, 15\}\,. \end{aligned}$$

Acknowledgements This paper was written during a visit of the author at Université Paris VII, in 1999. Thanks go to the members of the "Equipe des Groupes Finis" for their hospitality and to the Noesis Foundation for financing this visit.

References

[1] **N. Celakoski**, *On n-modules*, Godisen Zb. Elektro–Mas. Fak. Univ. Skopje **3** (1969), 15 – 26.

[2] **P. M. Cohn**, *Universal algebra*, Second edition, Mathematics and its Applications **6**, D. Reidel Publishing Co., Dordrecht – Boston, Mass. , 1981.

[3] **W. Dörnte**, *Untersuchungen über einen verallgemeinerten Gruppenbegriff*, Math. Z. **29** (1928), $1 - 19$.

[4] **B. Huppert**, *Endliche Gruppen I*, Springer-Verlag, Berlin, 1983.

[5] **L. Iancu**, *Redefining n-modules*, Bul. Şt. Univ. Baia Mare, Ser. B, Mat.–Inf. **14** (1998)

[6] **L. Iancu**, *Free R-n-modules*, Quasigroups and Related Systems **6** (1999), $13 - 22$.

[7] **S. Lang**, *Algebra. Second edition*, Addison–Wesley Publishing Co., Reading, Mass., 1984.

[8] **I. Purdea**, *Tratat de algebră modernă*, Vol.II, (Romanian) (*Treatise on modern algebra. Vol.II*) Ed. Academiei RSR, Bucharest, 1982.

Received March 25, 1999

North University of Baia Mare
Victoriei 7
RO–4800, Baia Mare
Romania
e-mail:liancu@ubm.ro

current address:
Institut Girard Desargues
Bat. 101, Université Lyon 1
43 Bd du 11 Novembre 1918
F-69622 Villeurbanne Cedex
France
e-mail: iancu@desargues.univ-lyon1.fr

Quasigroups and Related Systems **6** (1999), 43 – 59

Some linear conditions and their application to describing group isotopes

Fedir M. Sokhatsky

Abstract

The uniqueness of a canonical decomposition of a group isotope is proved in [1]. Now we characterize components of a canonical decomposition of a group isotope from the main classes of quasigroups.

1. Some known results and notions

A groupoid $(A, \circ)$ is called an *isotope* of a groupoid $(B, \cdot)$, if there are bijections α, β, γ from A to B such that the equality

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

holds for all $x, y \in A$. The triple (α, β, γ) is called an *isotopy* between $(A, \circ)$ and $(B, \cdot)$. Bijections α, β, γ are called *left, right* and *middle components* of this isotopy. A groupoid isotopic to a group $(G, +)$ is called a *group isotope*. $(G, +)$ is called a *decomposition group*. It is easy to see that a group isotope is a quasigroup.

A transformation α of a group $(Q, +)$ is called: *unitary* if $\alpha(0) = 0$; *linear* (*alinear*) if there exist $a, b \in Q$ and an automorphism (antiautomorphism) θ of the group $(Q, +)$ such that $\alpha(x) = a + \theta(x) + b$ for all $x \in Q$; *left* and *right monoregular* if it satisfies the identity

$$\alpha(x + x) = \alpha(x) + x \quad \text{and} \quad \alpha(x + x) = x + \alpha(x),$$

1991 Mathematics Subject Classification: 20N15
Keywords: group, loop, quasigroup

respectively. A linear unitary transformation is an automorphism.

If the left (right) and middle components of an isotopy are linear transformations of a decomposition group, then the isotopy is called *left* (*right*) *linear*. If the left (right) component is alinear but the middle component is linear then the corresponding isotope is called *left* (*rigdt*) *alinear*. A left and right linear (alinear) group isotope is called *linear* (*alinear*). A quasigroup linearly isotopic to a group is called a *linear quasigroup*. If, in addition, the group is abelian then the quasigroup is said to be *abelian*.

The right side of

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

is called a (*middle*) *canonical decomposition* determined by an element $0 \in Q$ of a group isotope $(Q, \cdot)$, if $(Q, +)$ is a group (with 0 as its neutral element) and α, β are unitary permutations of $(Q, +)$. α and β are called *coefficients* of the canonical decomposition, a – the *free member*, $(Q; +)$ – the *canonical decomposition group*.

Left and *right* canonical decompositions are determined by:

$$x \cdot y = a + \alpha x + \beta y, \qquad x \cdot y = \alpha x + \beta y + a,$$

respectively. These three canonical decompositions are uniquely determined by an arbitrary element 0 from the set Q (cf. [1]).

In [1] the following two lemmas are proved.

Lemma 1. *If for permutations α, β, γ, δ, μ of a group $(Q, +)$ the identity $\alpha(\beta(x) + \gamma(y)) = \delta(x) + \mu(y)$ holds, then α is a linear transformation of $(Q, +)$. If in addition $\alpha 0 = 0$, then α is an automorphism of $(Q, +)$.*

Lemma 2. *If* (1) *is a canonical decomposition of a group isotope $(Q, \cdot)$ and α is an automorphism of its decomposition group $(Q, +)$, then in $(Q, \cdot)$ we have*

$$x / y = \alpha^{-1} x - \alpha^{-1} \beta y - \alpha^{-1} a = \alpha^{-1} x + \alpha^{-1} I_a^{-1} I a + \alpha^{-1} I_a^{-1} I \beta y, \tag{2}$$

$$x \oslash y = \alpha^{-1} y - \alpha^{-1} \beta x - \alpha^{-1} a = \alpha^{-1} I_a^{\oplus} I \beta x \oplus \alpha^{-1} I_a^{\oplus} I a \oplus \alpha^{-1} y. \tag{3}$$

In the sequel will be used the following result from [2].

Theorem 3. *Let $(Q,\cdot,\Omega)$ be a quasigroup algebra, where $(Q,\cdot)$ is a group isotope. If in the words υ_1, υ_2, υ_3, υ_4, υ of the signature $\{\cdot\}\cup\Omega$ a variable x (a variable y) appears only in the words υ_1, υ_3 (respectively, υ_2, υ_4) and, in addition, exactly one time in at least one of them, then the group isotope is:*

1) *left linear, if the identity $(\upsilon_1(x)\cdot\upsilon_2(y))\cdot\upsilon=\upsilon_3(x)\cdot\upsilon_4(y)$ holds in $(Q,\cdot,\Omega)$,*
2) *right linear, if the identity $\upsilon\cdot(\upsilon_1(x)\cdot\upsilon_2(y))=\upsilon_3(x)\cdot\upsilon_4(y)$ holds in $(Q,\cdot,\Omega)$,*
3) *left alinear, if the identity $(\upsilon_1(x)\cdot\upsilon_2(y))\cdot\upsilon=\upsilon_4(y)\cdot\upsilon_3(x)$ holds in $(Q,\cdot,\Omega)$,*
4) *right alinear, if the identity $\upsilon\cdot(\upsilon_1(x)\cdot\upsilon_2(y))=\upsilon_4(y)\cdot\upsilon_3(x)$ holds in $(Q,\cdot,\Omega)$.*

It is easy to see that the following lemma is true.

Lemma 4. *If a group isotope $(Q,\cdot)$ has the canonical decomposition* (1), *then*

$$e_x=x\backslash x=\beta^{-1}(-a-\alpha x+x), \tag{4}$$

$$1_x=x/x=\alpha^{-1}(x-\beta x-a), \tag{5}$$

$$R_{e_x}^{-1}(u)=\alpha^{-1}(u-x+\alpha x), \tag{6}$$

$$L_{1_x}^{-1}(u)=\beta^{-1}(\beta x-x+u),$$

where e_x and 1_x are defined by the identities $xe_x=1_xx=x$.

Also the following two results are proved in [2].

Theorem 5. *Let $\{x_0,\dots,x_n\}$ be the set of all variables in the words w, v of the signature $(\cdot,/,\backslash)$ and let 0 be a fixed element of Q. If a quasigroup $(Q,\cdot)$ is abelian or linear and in the words w,v every appearance of every variable is not contained between two appearances of another variable, then the following conditions are equivalent:*

1) *the identity $w=v$ holds in $(Q,\cdot,/,\backslash)$,*
2) *$w(0,...,0,x_i,0,...,0)=v(0,...,0,x_i,0,...,0)$ holds in $(Q,\cdot,/,\backslash)$ for every $i=0,1,\dots,n$,*

3) $w(0,\ldots,0) = v(0,\ldots,0)$ *and for the middle* 0*-canonical decomposition sums of all coefficients of every variable in* w *and* v *are identical.*

Theorem 6. *Let* $(Q,\cdot,\Omega)$ *be a quasigroup algebra, where* $(Q,\cdot)$ *is a group isotope. If the identity* $w_1(x)\cdot w_2(y) = w_3(y)\cdot w_4(x)$ *holds and two pairs of its subwords* (w_1,w_4) *and* (w_2,w_3) *contain all appearances of variables* x *and* y *(respectively) and there exists only one appearance of* x *in* w_1 *or* w_4 *(respectively,* y *in* w_2 *or* w_3*), then* $(Q,\cdot)$ *is isotopic to a commutative group.*

2. Some linear conditions

The aim of this section is description of positions of variables in some identities implying relations between the coefficients of the group isotope in the canonical decomposition.

Lemma 7. *Let* ω *be a word in a quasigroup algebra* $(Q,\cdot,\Omega)$*, where* $(Q,\cdot)$ *is a group isotope. Then the left bracketting*

$$\omega = (\ldots((\omega_n \underset{n}{\circ} \upsilon_{n-1}) \underset{n-1}{\circ} \upsilon_{n-2}) \underset{n-2}{\circ} \ldots) \underset{1}{\circ} \upsilon_0,$$

where $\underset{i}{\circ} \in \{\cdot, /\}$ *and* υ_i *is a subword of the word* ω*, can be represented in the additive form*

$$\alpha^{k_n}\omega_n + \alpha^{k_{n-1}}\rho_{n-1}a + \alpha^{k_{n-1}}\rho_{n-1}\beta\upsilon_{n-1} + \ldots + \alpha^{k_0}\rho_0 a + \alpha^{k_0}\rho_0\beta\upsilon_0,$$

where (1) *denotes the canonical decomposition of* $(Q,\cdot)$*,* k_i *denotes the difference between the numbers of operations* $(\cdot)$ *and* $(/)$ *in the sequence* $(\underset{1}{\circ}, \underset{2}{\circ}, \ldots, \underset{i}{\circ})$ *and*

$$\rho_i \ := \begin{cases} \varepsilon, & \text{if } \ (\underset{i+1}{\circ}) = (\cdot), \\ \alpha^{-1}I_a^{-1}I, & \text{if } \ (\underset{i+1}{\circ}) = (/), \end{cases}$$

for $i = 0, 1, \ldots, n-1$.

Proof. We use the induction by n. For $n = 1$ we have

$$\omega = \alpha\omega_1 + a + \beta\upsilon_0, \qquad \text{if } \ (\underset{1}{\circ}) = (\cdot),$$
$$\omega \overset{(3)}{=} \alpha\omega_1 + \alpha^{-1}I_a^{-1}Ia + \alpha^{-1}I_a^{-1}I\beta\upsilon, \quad \text{if } \ (\underset{1}{\circ}) = (/).$$

These decompositions coincide with the additive form, since $k_0 = 0$, $k_1 = 1 - 0 = 1$, $\rho_0 = \varepsilon$ when $(\underset{1}{\circ}) = (\cdot)$, and $k_1 = 0 - 1 = -1$, $k_0 = 0$, $\rho_0 = \alpha^{-1} I_a^{-1} I$ when $(\underset{1}{\circ}) = (/)$.

Assume, now that the lemma is true for $n-1$. If in the left bracketting of ω we denote $\omega_n \underset{n}{\circ} \upsilon_{n-1}$ by ω_{n-1}, then, by the assumption on $n-1$, we obtain

$$\omega = (\ldots(\omega_{n-1} \underset{n-1}{\circ} \upsilon_{n-2}) \underset{n-3}{\circ} \ldots) \underset{1}{\circ} \upsilon_0$$

$$= \alpha^{k_{n-1}}(\omega_n \underset{n}{\circ} \upsilon_{n-1}) + \alpha^{k_{n-2}}\rho_{n-2}a + \alpha^{k_{n-2}}\rho_{n-2}\beta\upsilon_{n-2} + \ldots$$

$$\ldots + \alpha^{k_0}\rho_0 a + \alpha^{k_0}\rho_0\beta\upsilon_0,$$

which in the case $(\underset{n}{\circ}) = (\cdot)$ gives $\omega_{n-1} = \alpha\omega_n + a + \beta\upsilon_{n-1}$. But $k_n = k_{n-1} + 1$ and $\rho_{n-1} = \varepsilon$, therefore

$$\omega = \alpha^{k_{n-1}}(\alpha\omega_n + a + \beta\upsilon_{n-1}) + \alpha^{k_{n-1}}\rho_{n-1}a + \alpha^{k_{n-2}}\rho_{n-2}\beta\upsilon_{n-2} + \ldots$$

$$\ldots + \alpha^{k_0}\rho_0 a + \alpha^{k_0}\rho_0\omega_0$$

$$= \alpha^{k_{n-1}+1}\omega_n + \alpha^{k_{n-1}}a + \alpha^{k_{n-1}}\beta\upsilon_{n-1} + \alpha^{k_{n-1}}\rho_{n-1}a + \alpha^{k_{n-2}}\rho_{n-2}\beta\upsilon_{n-2} +$$

$$\ldots + \alpha^{k_0}\rho_0 a + \alpha^{k_0}\rho_0\omega_0,$$

which coincides with the additive form of ω.

In the case $(\underset{n}{\circ}) = (/)$ we have $k_n = k_{n-1} - 1$, $\rho_{n-1} = I\alpha^{-1}I_a^{-1}$ and

$$\omega_{n-1} \overset{(2)}{=} \alpha^{-1}\omega_n + \rho_{n-1}a + \rho_{n-1}\beta\upsilon_{n-1}.$$

Therefore

$$\omega = \alpha^{k_{n-1}}(\alpha^{-1}\omega_n + \rho_{n-1}a + \rho_{n-1}\beta\upsilon_{n-1}) + \alpha^{k_{n-2}}\rho_{n-2}a$$

$$+\alpha^{k_{n-2}}\rho_{n-2}\beta\upsilon_{n-2} + \ldots + \alpha^{k_0}\rho_0 a + \alpha^{k_0}\rho_0\omega_0,$$

which also gives the additive form of ω. □

Corollary 8. *A left bracketting* $\omega = (\ldots((\upsilon_n \cdot \upsilon_{n-1}) \cdot \upsilon_{n-2}) \cdot \ldots) \cdot \upsilon_0)$ *of the word* ω *in a left linear group isotope* $(Q, \cdot)$ *can be written in the form*

$$\omega = \alpha^n\upsilon_n + \alpha^{n-1}a + \alpha^{n-1}\beta\upsilon_{n-1} + \alpha^{n-2}a + \alpha^{n-2}\beta\upsilon_{n-2} + \ldots + a + \beta\upsilon_0.$$

Proof. Putting $(\underset{1}{\circ}) = ... = (\underset{n}{\circ}) = (\cdot)$ in Lemma 7 we obtain the above corollary, since in this case $\rho_i = \varepsilon$ for all $i = 0, \dots, n$. □

Theorem 9. *Assume that the identity $\omega = \upsilon$ holds in a quasigroup algebra $(Q, \cdot, /, \backslash, \Omega)$, where $(Q, \cdot)$ is a left linear group isotope, and the first variables in ω and υ are identical and appear in these words only once. If all nodal operations of the overwords of the first variable belong to the set $\{\cdot, /\}$, then the left coefficient α of the canonical decomposition of $(Q, \cdot)$ satisfies the condition $\alpha^{k_1 - k_2 - k_3 + k_4} = \varepsilon$, where k_1, k_3 are the numbers of all nodal operations of the first variable overwords of ω and υ respectively, coinciding with $(\cdot)$, and k_2, k_4 are those coinciding with $(/)$.*

Proof. Let (1) be the canonical decomposition of $(Q, \cdot)$ and let x be the first variable in ω and υ. Applying Lemma 7 to the full left bracketting we see that these words begin with the variable x and that the left and right side of the identity $\omega = \upsilon$ may be written in the form given in Corollary 8. This means that the subword υ_0 contains only one variable x. Since this variable does not appear in other subwords, then replacing of all other variables by elements of Q we obtain

$$\alpha^{k_1 - k_2}(x) + b = \alpha^{k_3 - k_4}(x) + c,$$

where b, c are some fixed elements from Q. Since for $x = 0$ we have $b = c$, therefore $\alpha^{k_1 - k_2} = \alpha^{k_3 - k_4}$, which completes the proof. □

Lemma 10. *Let ω be a word in a quasigroup algebra $(Q, \cdot, \Omega)$, where $(Q, \cdot)$ is a group isotope. Then the right bracketting*

$$\omega = \upsilon_0 \underset{1}{\circ} (\upsilon_1 \underset{2}{\circ} \dots \underset{n-1}{\circ} (\upsilon_{n-1} \underset{n}{\circ} \omega_n) \dots),$$

where $\underset{i}{\circ} \in \{\cdot, \backslash\}$ and υ_i are subwords of the word ω, can be represented in the additive form

$$\omega = \beta^{k_0}\nu_0\upsilon_0 + \beta^{k_0}\nu_0 a + \beta^{k_1}\nu_1\alpha\upsilon_1 + \beta^{k_1}\nu_1 a + ...$$
$$... + \beta^{k_{n-1}}\nu_{n-1}\alpha\upsilon_{n-1} + \beta^{k_{n-1}}\nu_0\beta\upsilon_{n-1} a + \beta^{k_n}\omega_n,$$

where (1) denotes the canonical decomposition of $(Q, \cdot)$, k_i denotes the difference between the numbers of operations $(\cdot)$ and $(\backslash)$ in the *sequence* $(\underset{1}{\circ}, \underset{2}{\circ}, ..., \underset{i}{\circ})$ *and*

$$\nu_i \;:=\; \begin{cases} \varepsilon, & if \quad (\underset{i+1}{\circ}) = (\cdot), \\ \beta^{-1} I_a I, & if \quad (\underset{i+1}{\circ}) = (\backslash), \end{cases}$$

for $i = 0, 1, \ldots, n-1$.

Proof. The proof is analogous to the proof of Lemma 7. □

Corollary 11. *A right bracketting* $\omega = \upsilon_0 \cdot (\upsilon_1 \cdot \ldots \cdot (\upsilon_{n-1} \cdot \upsilon_n) \ldots)$ *of the word* ω *of a right linear group isotope* $(Q, \cdot)$ *can be written in the form*

$$\omega = \alpha\upsilon_0 + a + \beta\alpha\upsilon_1 + \beta a + \beta^2\alpha\upsilon_2 + \beta^2 a + \cdots + \beta^{n-1}a + \beta^n\upsilon_n.$$

Proof. The proof is analogous to the proof of Corollary 8. □

Theorem 12. *Assume that the identity* $\omega = \upsilon$ *hold in a quasigroup algebra* $(Q, \cdot, /, \backslash, \Omega)$*, where* $(Q, \cdot)$ *is a right linear group isotope, and the last variables in* ω *and* υ *are identical and appear in these words only once. If all nodal operations of the overwords of the last variable belong to the set* $\{\cdot, \backslash\}$*, then the right coefficient* β *of the canonical decomposition of* $(Q, \cdot)$ *satisfies the condition* $\beta^{k_1-k_2-k_3+k_4} = \varepsilon$*, where* k_1*,* k_3 *are the numbers of all nodal operations of the last variable overwords of* ω *and* υ *respectively, coinciding with* $(\cdot)$*, and* k_2*,* k_4 *are those coinciding with* $(\backslash)$*.*

Proof. The proof is analogous to the proof of Theorem 9. □

3. Axiomatics of some classes of isotopes

In this section we find criteria for a group isotope to belong to the main classes of quasigroups.

3.1. Moufang, Bol and IP-quasigroups

As it is well-known, a quasigroup $(Q, \cdot)$ is called

left IP-quasigroup, if there exists a transformation λ such that

$$\lambda x \cdot (x \cdot y) = y,$$

right IP-quasigroup, if there exists a transformation ρ such that

$$(x \cdot y) \cdot \rho(y) = x,$$

Moufang quasigroup, if:

$$(xy \cdot z)y = x \cdot y(e_y z \cdot y),$$
$$y(x \cdot yz) = (y \cdot x1_y)y \cdot z,$$

left Bol quasigroup, if:

$$z(x \cdot zy) = R_{e_z}^{-1}(z \cdot xz) \cdot y,$$

right Bol quasigroup, if:

$$(yz \cdot x)z = y \cdot L_{1_z}^{-1}(zx \cdot z).$$

Theorem 13. *For a group isotope $(Q, \cdot)$ the following statements are equivalent:*

1) *$(Q, \cdot)$ is a left IP-quasigroup,*
2) *$(Q, \cdot)$ is a left Bol quasigroup,*
3) *the right coefficient of the canonical decomposition of $(Q, \cdot)$ is involutive automorphism of the decomposition group.*

Proof. 1) $\Longrightarrow$ 3). Assume that the group isotope $(Q; \cdot)$ is a left IP-quasigroup. Then, by the canonical decomposition (1) of $(Q, \cdot)$, the equation defining a left IP-quasigroup may be written in the form

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

where λ is as in the definition of a left IP-quasigroup.

This means that

$$\beta(R_a\alpha(x) + \beta(y)) = IR_a\alpha\lambda(x) + y,$$

where $I(x) = -x$, holds for all $x, y \in Q$. Thus, according to Theorem 1, β is a linear transformation of the group $(Q, +)$. Moreover, β (as a component of the canonical decomposition) is a unitary permutation of $(Q, +)$. Hence, β is an automorphism of $(Q, +)$.

Applying this fact and Theorem 12 to the equality defining a left IP-quasigroup we obtain the relation $\beta^{2-0+0-0} = \varepsilon$, which shows that β is an involutive automorphism of $(Q,+)$.

3) $\Longrightarrow$ 1). Let $(Q,\cdot)$ be an isotope of a group $(Q,+)$, (1) its canonical decomposition and β an involutive automorphism of $(Q,+)$. Putting

$$\lambda = \alpha^{-1}R_a^{-1}I\beta R_a\alpha \tag{7}$$

we obtain a transformation λ of Q such that

$$\begin{aligned}\lambda(x)\cdot(x\cdot y) &= R_a\alpha\lambda(x) + \beta(R_a\alpha(x) + \beta(y))\\ &= R_a\alpha\alpha^{-1}R_a^{-1}I\beta R_a\alpha(x) + \beta R_a\alpha(x) + \beta^2(y)\\ &= -\beta R_a\alpha(x) + \beta R_a\alpha(x) + y = y.\end{aligned}$$

Hence $(Q,\cdot)$ is a left IP-quasigroup.

2) $\Longrightarrow$ 3). Let a group isotope $(Q,\cdot)$ be a left Bol quasigroup. Fixing z in the identity defining a left Bol loop and applying Theorem 3 we obtain the right linearity of $(Q,\cdot)$. Because this identity is balanced with respect to y, then Theorem 12 implies $\beta^{3-0+0-1} = \varepsilon$, where β is a right coefficient of the canonical decomposition of $(Q,\cdot)$. Thus β is an involutive automorphism.

3) $\Longrightarrow$ 2). If β in the canonical decomposition (1) of $(Q,\cdot)$ is an involutive automorphism of $(Q,+)$, then

$$\begin{aligned}R_{e_z}^{-1}(z\cdot xz)\cdot y &\overset{(1)}{=} \alpha R_{e_z}^{-1}(z\cdot xz) + a + \beta y\\ &\overset{(6)}{=} (z\cdot xz) - z + \alpha z + a + \beta y\\ &\overset{(1)}{=} \alpha z + a + \beta(\alpha x + a + \beta z) - z + \alpha z + a + \beta y\\ &= \alpha z + a + \beta\alpha x + \beta a + z - z + \alpha z + a + \beta y\\ &= \alpha z + a + \beta\alpha x + \beta a + \alpha z + a + \beta y.\end{aligned}$$

Similarly

$$\begin{aligned}z(x\cdot zy) &\overset{(1)}{=} \alpha z + a + \beta(\alpha x + a + \beta(\alpha z + a + \beta y))\\ &= \alpha z + a + \beta\alpha x + \beta a + \alpha z + a + \beta y,\end{aligned}$$

which proves that $(Q,\cdot)$ is a left Bol quasigroup. □

Theorem 14. *For a group isotope $(Q,\cdot)$ the following statements are equivalent:*

1) *$(Q,\cdot)$ is a right IP-quasigroup,*
2) *$(Q,\cdot)$ is a right Bol quasigroup,*
3) *the left coefficient of the canonical decomposition of $(Q,\cdot)$ is an involutive automorphism of the decomposition group.*

Proof. The proof is analogous to the proof of Theorem 13. □

Theorem 15. *For a group isotope $(Q,\cdot)$ the following statements are equivalent:*

1) *$(Q,\cdot)$ is an IP-quasigroup,*
2) *$(Q,\cdot)$ is a Moufang quasigroup,*
3) *$(Q,\cdot)$ is a Bol quasigroup,*
4) *all coefficients of the canonical decomposition of $(Q,\cdot)$ are involutive automorphisms of the decomposition group.*

Proof. The equivalence of 1), 3) and 4) follows from Theorems 13 and 14.

2) $\Longleftrightarrow$ 4). Let $(Q,\cdot)$ be a Moufang quasigroup. Putting

$$\upsilon_1 = xy, \quad \upsilon_2 = z, \quad \upsilon = y, \quad \upsilon_3 = x, \quad \upsilon_4 = y(e_y z \cdot y)$$

in the first identity defining this quasigroup and applying Theorem 3 we obtain the right linearity of $(Q,\cdot)$. In the analogous way, the second identity from the definition of a Moufang quasigroup gives the left linearity of $(Q,\cdot)$. Thus $(Q,\cdot)$ is a linear group isotope. But for linear group isotopes this equivalence is proved in [4]. □

A *left* (*right*) symmetri c quasigroup is defined as a quasigroup satisfying the identity $x\cdot(x\cdot y) = y$ (respectively, $(x\cdot y)\cdot y = x$). A quasigroup which is left and right symmetric is called *symmetric* or a *TS-quasigroup.*

Corollary 16. *A group isotope $(Q,\cdot)$ is a left (right) symmetric quasigroup iff the decomposition group $(Q,+)$ is commutative and the right (left) coefficient β of its canonical decomposition is an automorphism of $(Q,+)$ such that $\beta(x) = -x$ for all $x \in Q$.*

Proof. Every left symmetric quasigroup is a left IP-quasigroup, where $\lambda = \varepsilon$. From the proof of Theorem 13 follows $\beta = I$, i.e. $\beta(x) = -x$ for all $x \in Q$. But such defined β is an automorphism only in commutative groups. The converse is obvious.

In the case of a right symmetric quasigroup the proof is analogous. □

3.2. F-quasigroups

Note that a *left* (*right*) F-quasigroup is defined as a quasigroup $(Q, \cdot)$ satisfying the identity

$$x \cdot yz = xy \cdot e_x z, \tag{8}$$

(respectively, $xy \cdot z = x1_z \cdot yz$).

Theorem 17. *A group isotope* $(Q, \cdot)$ *with a canonical decomposition* (1) *is a left F-quasigroup iff* β *is an automorphism of the group* $(Q, +)$, β *commutes with* α *and* α *satisfies the identity*

$$\alpha(x + y) = x + \alpha y - x + \alpha x. \tag{9}$$

Proof. Let $(Q, \cdot)$ be a group isotope satisfying (8). If (1) is a canonical decomposition of $(Q, \cdot)$, then (8) together with Theorem 3 imply that β is an automorphism of $(Q, +)$.

Moreover, (8) for $z = \beta^{-1}(-a)$ and $x = \alpha^{-1}(t - a)$ gives

$$t + \beta\alpha y = \alpha(t + \beta y) + \gamma t, \tag{10}$$

where γ is a some permutation of Q.

This identity $y = 0$ implies $\gamma t = -\alpha t + t$. Hence (10) may be written in the form

$$t + \beta\alpha y = \alpha(t + \beta y) - \alpha t + t,$$

which for $t = 0$ gives $\alpha\beta = \beta\alpha$. This fact together with the transposition of βy and y in (10) implies

$$t + \alpha y = \alpha(t + y) - \alpha t + t,$$

which proves (9).

Conversely, let $(Q,\cdot)$ be a group isotope with the canonical decomposition described in Theorem.

Putting $y=-x$ in (9) we obtain $0=x+\alpha(-x)-x+\alpha(x)$, i.e.

$$x+\alpha(-x)=-\alpha x+x. \tag{11}$$

Hence

$$\begin{aligned}
xy\cdot e_x z &\overset{(1)}{=} \alpha(\alpha x+a+\beta y)+a+\beta(\alpha e_x+a+\beta z)\\
&= \alpha((\alpha x+a)+\beta y)+a+\beta(\alpha e_x)+\beta a+\beta^2 z\\
&\overset{(9)}{=} \alpha x+a+\alpha\beta y-(\alpha x+a)+\alpha(\alpha x+a)+a+\alpha\beta e_x+\beta a+\beta^2 z\\
&\overset{(4)}{=} \alpha x+a+\alpha\beta y-(\alpha x+a)+\alpha(\alpha x+a)+a+\\
&\qquad +\alpha(-(\alpha x+a)+x)+\beta a+\beta^2 z\\
&\overset{(9)}{=} \alpha x+a+\alpha\beta y-(\alpha x+a)+\alpha(\alpha x+a)+a-(\alpha x+a)+\\
&\qquad +\alpha x+\alpha x+a+\alpha(-(\alpha x+a))+\beta a+\beta^2 z\\
&= \alpha x+a+\alpha\beta y-(\alpha x+a)+\alpha(\alpha x+a)+(\alpha x+a+\\
&\qquad +\alpha(-(\alpha x+a)))+\beta a+\beta^2 z\\
&\overset{(11)}{=} \alpha x+a+\alpha\beta y-(\alpha x+a)+\alpha(\alpha x+a)-\alpha(\alpha x+a)+\\
&\qquad +(\alpha x+a)+\beta a+\beta^2 z\\
&= \alpha x+a+\alpha\beta y+\beta a+\beta^2 z\\
&= \alpha x+a+\beta\alpha y+\beta a+\beta^2 z=\alpha x+a+\beta(\alpha y+a+\beta z)\\
&= x\cdot(y\cdot z),
\end{aligned}$$

which proves that $(Q,\cdot)$ is a left F-quasigroup. □

Corollary 18. *If a group isotope is a left F-quasigroup, then it is right linear. It is linear iff the left coefficient of its canonical decomposition commutes with every inner automorphism of the decomposition group.*

Proof. The first part follows from Theorem 17. If a linear group isotope is a left F-quasigroup, then, as it is proved in [4], the left coefficient of its canonical decomposition commutes with every inner automorphism of the decomposition group.

Conversely, if α commutes with every inner automorphism of the group $(Q,+)$, then (9) may be rewritten in the form:

$$\alpha(x+y) = \alpha(x+y-x) + \alpha x,$$

which for $u = x+y-x$ implies $\alpha(u+x) = \alpha u + \alpha x$. Hence α is an automorphism of the group $(Q;+)$. □

Corollary 19. *If a group isotope is a left F-quasigroup, then it is left alinear iff its decomposition group is commutative.*

Proof. Theorem 17 implies (9), which may be rewritten in the form $\alpha y + \alpha x = x + \alpha y - x + \alpha x$, because α is an antiautomorphism of $(Q,+)$. This implies the commutativity of the group $(Q,+)$.

The converse is obvious. □

Theorem 20. *A group isotope $(Q,\cdot)$ with a canonical decomposition (1) is a right F-quasigroup iff α is an automorphism of the group $(Q,+)$, α commutes with β and β satisfies the identity*

$$\beta(y+z) = \beta z - z + \beta y + z.$$

Proof. The proof is analogous to the proof of Theorem 17. □

3.3. Alternative quasigroups

A quasigroup $(Q,\cdot)$ is called *left* (*right*) alternative if it satisfies the identity $x\cdot(x\cdot z) = (x\cdot x)\cdot z$ (respectively, $(x\cdot y)\cdot y = x\cdot(y\cdot y)$).

Theorem 21. *A group isotope $(Q,\cdot)$ with the canonical decomposition (1) is left alternative iff $\beta = \varepsilon$ and $\alpha = R_a^{-1}\theta^{-1}$, where θ is a right monoregular permutation of the group $(Q,+)$.*

Proof. If a group isotope $(Q,\cdot)$ with the canonical decomposition (1) is left alternative, then the identity $x\cdot(x\cdot z) = (x\cdot x)\cdot z$ may be rewritten in the form

$$\alpha x + a + \beta(\alpha x + a + \beta z) = \alpha(\alpha x + a + \beta x) + a + \beta z.$$

Replacing in this identity $a+\beta z$ by z and αx by x we obtain

$$x + a + \beta(x+z) = \alpha(x + a + \beta\alpha^{-1}x) + z,$$

which for $z=0$ gives

$$x+a+\beta x=\alpha(x+a+\beta\alpha^{-1}x). \tag{12}$$

Therefore the previous identity may be written in the form

$$x+a+\beta(x+z)=x+a+\beta x+z.$$

Hence $\beta(x+z)=\beta x+z$, and in the consequence $\beta=\varepsilon$. Thus (12) implies

$$\alpha^{-1}(x+a+x)=x+a+\alpha^{-1}x.$$

Replacing x by $x-a$ we see that $\theta=R_a^{-1}\alpha^{-1}$ is a right monoregular permutation.

Conversely, let the relations $\beta=\varepsilon$ and θ be a right monoregular permutation of the group $(Q;+)$, then

$$\begin{aligned} x\cdot(x\cdot z) &\overset{(1)}{=} \alpha x+a+\beta(\alpha x+a+\beta z)=\alpha x+a+\alpha x+a+z\\ &=(\alpha x+a+\alpha x)+a+z=\alpha(\alpha x+a+x)+a+z\\ &\overset{(1)}{=}(x\cdot x)\cdot z \end{aligned}$$

completes the proof. □

Corollary 22. *A left alternative group isotope is a left loop.*

Proof. Indeed, $\beta=\varepsilon$ implies

$$(\alpha^{-1}(-a))\cdot y\overset{(1)}{=}\alpha(\alpha^{-1}(-a))+a+y=-a+a+y=y$$

for every $y\in Q$. Thus $\alpha^{-1}(-a)$ is a left unit of $(Q,\cdot)$. □

In the similar way as Theorem 21 we can prove

Theorem 23. *A group isotope $(Q,\cdot)$ with the canonical decomposition (1) is a right alternative quasigroup iff $\alpha=\varepsilon$, and $\beta=R_a^{-1}\theta^{-1}$, where θ is a left monoregular permutation of the group $(Q,+)$.*

Corollary 24. *A right alternative group isotope is a right loop.*

3.4. Semimedial quasigroups

A quasigroup $(Q,\cdot)$ is called *left semimedial* if it satisfies the identity

$$xx\cdot yz = xy\cdot xz,$$

and *right semimedial* if it satisfies the identity $xy\cdot zz = xz\cdot yz$. A quasigroup which is left and right semimedial is called *semimedial*. It is a special case of so-called *medial* quasigroups, i.e. quasigroups satisfying the identity $xy\cdot uv = xu\cdot yv$.

Theorem 25. *A group isotope $(Q,\cdot)$ is left semimedial iff there exists a group $(Q,+)$, an element $a\in Q$, a permutation α of Q and an automorphism β of $(Q,+)$ such that*

$$L_{\alpha a}\beta\alpha = \alpha R_a\beta, \tag{13}$$

$$x\cdot y = \alpha x + \beta y + a, \tag{14}$$

$$\alpha(x+y) = \alpha x + \beta x + \alpha y - \beta x \tag{15}$$

for all $x,y\in Q$.

Proof. By Theorem 3, a left semimedial group isotope $(Q,\cdot)$ is right linear and has the decomposition (14), where β is an automorphism of the group $(Q,+)$.

Thus from (14) and $00\cdot yz = 0y\cdot 0z$, where $\beta z = -a$, we obtain $\alpha a + \beta\alpha y = \alpha(\beta y + a)$, which gives (13) and

$$\beta\alpha y = -\alpha a + \alpha(\beta y + a).$$

This together with (14) and $xx\cdot yz = xy\cdot xz$ for $\beta z + a = 0$, $\beta y + a = u$ and $\alpha x = v$ implies

$$\alpha(v + \beta x + a) - \alpha a + \alpha u = \alpha(v+u) + \beta v,$$

which for $u = 0$ gives $\alpha(v + \beta x + a) - \alpha a = \alpha v + \beta v$.

Applying this identity to the previous we obtain (15).

Conversely, if a group isotope $(Q,\cdot)$ has the canonical decomposition (14) such that (13) and (15) are satisfied, then

$$\begin{aligned} xx\cdot yz &\overset{(14)}{=} \alpha(xx)+\beta(yz)+a\\ &\overset{(14)}{=} \alpha(\alpha x+\beta x+a)+\beta(\alpha y+\beta z+a)+a\\ &\overset{(15)}{=} \alpha^2x+\beta\alpha x+\alpha(\beta x+a)-\beta\alpha x+\beta\alpha y+\beta^2z+\beta a+a\\ &\overset{(13)}{=} \alpha^2x+\beta\alpha x+\alpha a+\beta\alpha x-\beta\alpha x+\beta\alpha y+\beta^2z+\beta a+a\\ &= \alpha^2x+\beta\alpha x+\alpha a+\beta\alpha y+\beta^2z+\beta a+a. \end{aligned}$$

and

$$\begin{aligned} xy\cdot xz &\overset{(14)}{=} \alpha(xy)+\beta(xz)+a\\ &\overset{(14)}{=} \alpha(\alpha x+\beta y+a)+\beta(\alpha x+\beta z+a)+a\\ &\overset{(15)}{=} \alpha^2x+\beta\alpha x+\alpha(\beta y+a)-\beta\alpha x+\beta\alpha x+\beta^2z+\beta a+a\\ &\overset{(13)}{=} \alpha^2x+\beta\alpha x+\alpha a+\beta\alpha y+\beta^2z+\beta a+a. \end{aligned}$$

This proves that $(Q,\cdot)$ is left semimedial. □

Corollary 26. *A left semimedial group isotope is right linear. It is left linear iff it is medial.*

Proof. The first part of the statement follows from Theorem 25. By Toyoda-Bruck's Theorem a medial group isotope is linear, and by [4] a semimedial linear group isotope is medial. □

Theorem 27. *A group isotope $(Q,\cdot)$ is right semimedial iff there exists a group $(Q,+)$, an element $a\in Q$, an automorphism α of $(Q,\cdot)$ and a permutation β of Q such that $\beta(x+y)=-\alpha y+\alpha x+\alpha y+\beta y$, $\beta L_a\alpha=R_{\beta a}\alpha\beta$ and $x\cdot y=a+\alpha x+\beta y$ for all $x,y\in Q$.*

Proof. The proof is analogous to the proof of Theorem 25. □

Corollary 28. *A group isotope is medial iff it is semimedial.*

Corollary 29. *A group isotope $(Q,\cdot)$ is commutative iff its decomposition group is commutative and $\alpha=\beta$.*

Corollary 30. *A group isotope $(Q,\cdot 0$ is unipotent iff it has the decomposition $x\cdot y=\alpha x-\alpha y+a$ or $x\cdot y=a+\beta x-\beta y$.*

Corollary 31. *The canonical decomposition group of a commutative unipotent group isotope is a Boolean group.*

References

[1] **F. Sokhatsky**: *On isotopes of groups. I.* (Ukrainian), Ukrain. Mat. Zh. (1995), 1387 – 1398, translation in: Ukrainian Math. J. **47** (1995), 1585 – 1598.

[2] **F. Sokhatsky**: *On isotopes of groups. II.* (Ukrainian), Ukrain. Mat. Zh. (1995), 1692 – 1703, translation in: Ukrainian Math. J. **47** (1995)), 1935 – 1948.

[3] **F. Sokhatsky**: *On isotopes of groups. III.* (Ukrainian), Ukrain. Mat. Zh. (1996), 251 – 260, translation in: Ukrainian Math. J. **48** (1996), 283 – 293.

[4] **O. U. Kirnasovsky**: *Linear isotopes of small order groups*, Quasigroups and Related Systems **2** (1995), 51 – 82.

Vinnitsia State Pedagogical University
Vinnytsia 287100
Ukraine
e-mail: fedir@vinnitsa.com

Received September 10, 1999

Quasigroups and Related Systems **6** (1999), 61 – 70

Invertible elements in associates and semigroups. 2

Fedir M. Sokhatsky and Olena Yurevych

Abstract

This work is a continuation of [12]. Some additional invertibility criteria for elements of associates and n-ary semigroups are found. The corresponding axiomatics for polyagroups and n-ary groups are established.

The study of (i, j)-associative $(n+1)$-ary groupoids is reduced in [8] to the study of so-called associate of the type (s, n), where $s|n$. A bracketting rule and a decomposition of the main operation was described in [10]. Some criteria of invertibility of elements are found in [12]. Here, we give some additional criteria of invertibility and find axiomatics for polyagroups and n-groups.

The following theorem is proved in [10]

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 the bracketting only and the coordinate of every f's occurrence in the words w_1 and w_2 is divisible by r and also there exists a 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).*

By the *coordinate of the i-th occurrence of the symbol f in a word w* is mean a number of all individual variables and constants, appearing

1991 Mathematics Subject Classification: 20N15
Keywords: associate, invertible element

in the word w from the beginning of w to the i-th occurrence of the operation symbol f.

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 the 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 $i = 0, 1, \dots, n$, then it is called *invertible*. Invertible elements in n-semigroups are described by Gluskin in [6] and [7].

The following theorem is proved in [12]

Theorem 2. *An element $a \in Q$ is invertible in an associate (Q, f) of the type (s, n) iff there exists an element $\bar{a} \in Q$ such that*

$$f(\bar{a}, a, \dots a, x) = x, \qquad f(x, a, \dots a, \bar{a}) = x \tag{2}$$

for all $x \in Q$.

1. Criterion of invertibility

Corollary 1. *An element a is invertible in an associate (Q, f) of the type (s, n) iff there exist $\hat{a}$ and $\breve{a}$ such that*

$$f(\hat{a}, a, \dots, a, x) = x, \qquad f(x, a, \dots, a, \breve{a}) = x \tag{3}$$

hold for all $x \in Q$.

Proof. If an element a is r-multiple invertible, then (2) are true according to Theorem 2. Therefore (3) with $\hat{a} = \breve{a} = \bar{a}$ hold.

Conversely, assume that (3) hold. Putting $x = \breve{a}$ in the first equality, and $x = \hat{a}$ in the second, we obtain

$$f(\hat{a}, a, \dots, a, \breve{a}) = \breve{a} \quad \text{and} \quad f(\hat{a}, a, \dots, a, \breve{a}) = \hat{a}.$$

Hence $\hat{a} = \breve{a}$. Thus (2) hold.

The invertibility of a follows from Theorem 2. □

Lemma 1. *If an element a is i-invertible in an associate (Q,f) of the type (s,n), then every i-th skew element to a is also j-th skew for all $j\equiv i \pmod{s}$.*

Proof. Since the i-th shift induced by a is a substitution of the set Q, then

$$a=\lambda_{i,a}^{-1}\lambda_{i,a}(a)\overset{(1)}{=}\lambda_{i,a}^{-1}f(\overset{n+1}{a})\overset{(1)}{=}\lambda_{i,a}^{-1}f(\overset{j}{a},\lambda_{i,a}\lambda_{i,a}^{-1}(a),\overset{n-j}{a})$$

$$\overset{(4)}{=}\lambda_{i,a}^{-1}f(\overset{j}{a},f(\overset{i}{a},\bar a^i,\overset{n-i}{a}),\overset{n-j}{a})\overset{T1}{=}\lambda_{i,a}^{-1}f(\overset{i}{a},f(\overset{j}{a},\bar a^i,\overset{n-j}{a}),\overset{n-i}{a})$$

$$\overset{(1)}{=}\lambda_{i,a}^{-1}\lambda_{i,a}f(\overset{j}{a},\bar a^i,\overset{n-j}{a})=f(\overset{j}{a},\bar a^i,\overset{n-j}{a}).$$

Thus $f(\overset{j}{a},\bar a^i,\overset{n-j}{a})=a$. This means, that $\bar a^i$ is the j-th skew to 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* of the element a, which is denoted by $\bar a^i$ $(\bar a := \bar a^0)$ and is determined by the equality

$$f(\overset{i}{a},\bar a^i,\overset{n-i}{a})=a. \tag{4}$$

The following theorem is valid.

Theorem 3. *In any associate (Q,f) of the type (s,n) for any element a and for any $i=0,1,\dots,n-1$; $k=1,\dots,\frac{n}{s}-1$ the following conditions are equivalent:*

1) *a is invertible;*
2) *a is i- and $(n-i)$-invertible;*
3) *there exist elements $\hat a$ and $\breve a$ from Q such that*

$$f(\overset{i}{a},\hat a,\overset{n-i-1}{a},x)=x \quad \text{and} \quad f(x,\overset{n-i-1}{a},\breve a,\overset{i}{a})=x \tag{5}$$

   hold for all $x\in Q$.
4) *a is ks-invertible.*

Proof. 1) ⇒ 2) by the definition of invertibility.

2) ⇒ 3). Since the element a is i- and $(n-i)$-invertible, the i-th and $(n-i)$-th shifts are substitutions of the set Q.

Let $i\leqslant n-s$. To prove the relation (5), we consider the following equalities:

$$\begin{aligned} x = \lambda_{i,a}^{-1}\lambda_{i,a}(x) &\overset{(1)}{=} \lambda_{i,a}^{-1} f(\overset{i}{a}, x, \overset{n-i}{a}) \\ &\overset{L1}{=} \lambda_{i,a}^{-1} f(\overset{i}{a}, x, \overset{s-1}{a}, f(\overset{n-s-i}{a}, \bar{a}^{(n-i)}, \overset{i+s}{a}), \overset{n-s-i}{a}) \\ &\overset{T1}{=} \lambda_{i,a}^{-1} f(\overset{i}{a}, f(x, \overset{n-i-1}{a}, \bar{a}^{(n-i)}, \overset{i}{a}), \overset{n-i}{a}) \\ &\overset{(1)}{=} \lambda_{i,a}^{-1}\lambda_{i,a} f(x, \overset{n-i-1}{a}, \bar{a}^{(n-i)}, \overset{i}{a}) = f(x, \overset{n-i-1}{a}, \bar{a}^{(n-i)}, \overset{i}{a}). \end{aligned}$$

Hence, the second equality from (5) holds.

To prove the first, observe that

$$\begin{aligned} x = \lambda_{n-i,a}^{-1}\lambda_{n-i,a}(x) &\overset{(1)}{=} \lambda_{n-i,a}^{-1} f(\overset{n-i}{a}, x, \overset{i}{a}) \\ &\overset{L1}{=} \lambda_{n-i,a}^{-1} f(\overset{n-s-i}{a}, f(\overset{i+s}{a}, \bar{a}^{i}, \overset{n-s-i}{a}), \overset{s-1}{a}, x, \overset{i}{a}) \\ &\overset{T1}{=} \lambda_{n-i,a}^{-1} f(\overset{n-i}{a}, f(\overset{i}{a}, \bar{a}^{i}, \overset{n-i-1}{a}, x), \overset{i}{a}) \\ &\overset{(1)}{=} \lambda_{n-i,a}^{-1}\lambda_{n-i,a} f(\overset{i}{a}, \bar{a}^{i}, \overset{n-i-1}{a}, x) = f(\overset{i}{a}, \bar{a}^{i}, \overset{n-i-1}{a}, x). \end{aligned}$$

This proves that for $i \leqslant n-s$ the relation (5) holds.

Let $i > s$. At first, we prove the validity of the relations

$$f(\overset{i-s}{a}, \bar{a}^{i}, \overset{n-i+s-1}{a}, x) = x, \tag{6}$$

$$f(x, \overset{n-i+s-1}{a}, \bar{a}^{(n-i)}, \overset{i-s}{a}) = x. \tag{7}$$

Make a chain of conclusions:

$$\begin{aligned} x = \lambda_{i,a}^{-1}\lambda_{i,a}(x) \overset{(1)}{=} f(\overset{i}{a}, \lambda_{i,a}^{-1}(x), \overset{n-i}{a}) &\overset{(4)}{=} \lambda_{i,a}^{-1} f(\overset{i-s}{a}, f(\overset{i}{a}, \bar{a}^{i}, \overset{n-i}{a}), \overset{s-1}{a}, x, \overset{n-i}{a}) \\ &\overset{T1}{=} \lambda_{i,a}^{-1} f(\overset{i}{a}, f(\overset{i-s}{a}, \bar{a}^{i}, \overset{n-i+s-1}{a}, x), \overset{n-i}{a}) \\ &\overset{(1)}{=} \lambda_{i,a}^{-1}\lambda_{i,a} f(\overset{i-s}{a}, \bar{a}^{i}, \overset{n-i+s-1}{a}, x) = f(\overset{i-s}{a}, \bar{a}^{i}, \overset{n-i+s-1}{a}, x). \end{aligned}$$

This proves (6). To prove (7) note that

$$\begin{aligned} x = \lambda_{n-i,a}^{-1}\lambda_{n-i,a}(x) &\overset{(1)}{=} \lambda_{n-i,a}^{-1} f(\overset{n-i}{a}, x, \overset{i}{a}) \\ &\overset{(4)}{=} \lambda_{n-i,a}^{-1} f(\overset{n-i}{a}, x, \overset{s-1}{a}, f(\overset{n-i}{a}, \bar{a}^{(n-i)}, \overset{i}{a}), \overset{i-s}{a}) \\ &\overset{T1}{=} \lambda_{n-i,a}^{-1} f(\overset{n-i}{a}, f(x, \overset{n-i+s-1}{a}, \bar{a}^{(n-i)}, \overset{i-s}{a}), \overset{i}{a}) \end{aligned}$$

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

Using the obtained relation, we get correctness of the first of equalities (5). Indeed,

$$x \overset{(6)}{=} f(\overset{i-s}{a}, \bar{a}^{i}, \overset{n-i+s-1}{a}, x) \overset{(4)}{=} f(f(\overset{i}{a}, \bar{a}^{i}, \overset{n-i}{a}), \overset{i-s-1}{a}, \bar{a}^{i}, \overset{n-i+s-1}{a}, x)$$
$$\overset{T1}{=} f(\overset{i}{a}, \bar{a}^{i}, \overset{n-i-1}{a}, f(\overset{i-s}{a}, \bar{a}^{i}, \overset{n-i+s-1}{a}, x)) \overset{(6)}{=} f(\overset{i}{a}, \bar{a}^{i}, \overset{n-i-1}{a}, x).$$

In the same way:

$$x \overset{(7)}{=} f(x, \overset{n-i+s-1}{a}, \bar{a}^{(n-i)}, \overset{i-s}{a})$$
$$\overset{(4)}{=} f(x, \overset{n-i+s-1}{a}, \bar{a}^{(n-i)}, \overset{i-s-1}{a}, f(\overset{n-i}{a}, \bar{a}^{(n-i)}, \overset{i}{a}))$$
$$\overset{T1}{=} f(f(x, \overset{n-i+s-1}{a}, \bar{a}^{(n-i)}, \overset{i-s}{a}), \overset{n-i-1}{a}, \bar{a}^{(n-i)}, \overset{i}{a}) \overset{(6)}{=} f(x, \overset{n-i-1}{a}, \bar{a}^{(n-i)}, \overset{i}{a}),$$

which proves the second equality from (5). Thus 2) implies 3).

3) $\Rightarrow$ 4). If $i = 0$, then (5) implies (3), which, by Corollary 1, proves that a is an invertible element. In particular, it is j-invertible for all j.

If $i > 0$, then for

$$\hat{a} := f(\overset{i}{a}, f(\bar{a}^{i}, \overset{n-1}{a}, \bar{a}^{i}), \overset{n-i-1}{a}, \bar{a}^{(n-i)}), \tag{8}$$

$$\breve{a} := f(\bar{a}^{i}, \overset{n-i-1}{a}, f(\bar{a}^{(n-i)}, \overset{n-1}{a}, \bar{a}^{(n-i)}), \overset{i}{a}) \tag{9}$$

we have

$$f(\hat{a}, \overset{n-1}{a}, x) \overset{(8)}{=} f(f(\overset{i}{a}, f(\bar{a}^{i}, \overset{n-1}{a}, \bar{a}^{i}), \overset{n-i-1}{a}, \bar{a}^{(n-i)}), \overset{n-1}{a}, x)$$
$$\overset{T1}{=} f(\overset{i}{a}, f(\bar{a}^{i}, \overset{n-i-1}{a}, f(\overset{i}{a}, \bar{a}^{i}, \overset{n-i-1}{a}, \bar{a}^{(n-i)}), \overset{i}{a}), \overset{n-i-1}{a}, x)$$
$$\overset{(5)}{=} f(\overset{i}{a}, f(\bar{a}^{i}, \overset{n-i-1}{a}, \bar{a}^{(n-i)}, \overset{i}{a}), \overset{n-i-1}{a}, x)$$
$$\overset{(5)}{=} f(\overset{i}{a}, \bar{a}^{i}, \overset{n-i-1}{a}, x) \overset{(5)}{=} x.$$

The second equality from (3) may be proved in the same way. Indeed,

$$f(x, \overset{n-1}{a}, \breve{a}) \overset{(9)}{=} f(x, \overset{n-1}{a}, f(\bar{a}^{i}, \overset{n-i-1}{a}, f(\bar{a}^{(n-i)}, \overset{n-1}{a}, \bar{a}^{(n-i)}), \overset{i}{a}))$$
$$\overset{T1}{=} f(x, \overset{n-i-1}{a}, f(\overset{i}{a}, f(\bar{a}^{i}, \overset{n-i-1}{a}, \bar{a}^{(n-i)}, \overset{i}{a}), \overset{n-i-1}{a}, \bar{a}^{(n-i)}), \overset{i}{a})$$

$$\overset{(5)}{=} f(x, \overset{n-i-1}{a}, f(\overset{i}{a}, \bar{a}^i, \overset{n-i-1}{a}, \bar{a}^{(n-i)}), \overset{i}{a}) \overset{(5)}{=} f(x, \overset{n-i-1}{a}, \bar{a}^{(n-i)}, \overset{i}{a}) \overset{(5)}{=} x.$$

Hence, the relations (3) are valid and therefore, by Corollary 1, the element a is invertible.

4) $\Rightarrow$ 1). Let $j \equiv 0 \pmod{s}$, $0 < j < n$, i.e. $j = ks$, where $k = 1, \ldots, n/s - 1$, and let an element a be j-invertible.

Since the element a is ks-invertible, the ks-th shift is a substitution of the set Q. Observe that for

$$y := \lambda_{ks,a}^{-1}(z), \qquad z := \lambda_{ks,a}(y). \tag{10}$$

the following two equalities hold

$$\lambda_{ks,a}^{-1} f(z, \overset{ks-1}{a}, x, \overset{n-ks}{a}) = f(\lambda_{ks,a}^{-1}(z), \overset{n-1}{a}, x), \tag{11}$$

$$\lambda_{ks,a}^{-1} f(\overset{ks}{a}, x, \overset{n-ks-1}{a}, z) = f(x, \overset{n-1}{a}, \lambda_{ks,a}^{-1}(z)). \tag{12}$$

Indeed,

$$\begin{aligned}
\lambda_{ks,a}^{-1} f(z, \overset{ks-1}{a}, x, \overset{n-ks}{a}) &\overset{(10)}{=} \lambda_{ks,a}^{-1} f(\lambda_{ks,a}(y), \overset{ks-1}{a}, x, \overset{n-ks}{a}) \\
&\overset{(1)}{=} \lambda_{ks,a}^{-1} f(f(\overset{ks}{a}, y, \overset{n-ks}{a}), \overset{ks-1}{a}, x, \overset{n-ks}{a}) \\
&\overset{T1}{=} \lambda_{ks,a}^{-1} f(\overset{ks}{a}, f(y, \overset{n-1}{a}, x), \overset{n-ks}{a}) \\
&\overset{(1)}{=} \lambda_{ks,a}^{-1} \lambda_{ks,a} f(y, \overset{n-1}{a}, x) \overset{(1)}{=} f(y, \overset{n-1}{a}, x) \\
&\overset{(10)}{=} f(\lambda_{ks,a}^{-1}(z), \overset{n-1}{a}, x).
\end{aligned}$$

Similarly

$$\begin{aligned}
\lambda_{ks,a}^{-1} f(\overset{ks}{a}, x, \overset{n-ks-1}{a}, z) &\overset{(1)}{=} \lambda_{ks,a}^{-1} f(\overset{ks}{a}, x, \overset{n-ks-1}{a}, f(\overset{ks}{a}, y, \overset{n-ks}{a})) \\
&\overset{T1}{=} \lambda_{ks,a}^{-1} f(\overset{ks}{a}, f(x, \overset{n-1}{a}, y), \overset{n-ks}{a}) \\
&\overset{(1)}{=} \lambda_{ks,a}^{-1} \lambda_{ks,a} f(x, \overset{n-1}{a}, y) \\
&\overset{(1)}{=} f(x, \overset{n-1}{a}, y) \overset{(10)}{=} f(x, \overset{n-1}{a}, \lambda_{ks,a}^{-1}(z)).
\end{aligned}$$

Now, putting $z := a$ in (11) we obtain

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

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

which together with the definitions of a shift and the definition of a skew element gives

$$x = f(\bar{a}^{ks}, \overset{n-1}{a}, x) \tag{13}$$

for all $x \in Q$. This means, that the first equality from (3) holds. To verify the second one we put $z = a$ in (12). Then

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

which, as in the previous case, implies

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

Thus

$$x = f(x, \overset{n-1}{a}, \bar{a}^{ks}) \tag{14}$$

for all $x \in Q$. Corollary 1 and (13), (14) imply the invertibility of a.

This completes the proof of Theorem 3. □

Note, that for binary semigroups the following assertion is valid.

Lemma 2. *Let $(Q, \cdot)$ be a binary semigroup and shift $\lambda_{0,a}$ ($\lambda_{1,a}$) be a substitution of Q, then the element $e_r := \lambda_{0,a}^{-1}(a)$ ($e_\ell := \lambda_{1,a}^{-1}(a)$) is a right (respectively left) unit, and $a_r^{-1} := \lambda_{0,a}^{-2}(a)$ ($a_\ell^{-1} := \lambda_{1,a}^{-2}(a)$) is a right (respectively left) inverse element of the element a in semigroup $(Q, \cdot)$.*

Proof. Indeed,

$$\lambda_{0,a}(x \cdot e_r) = x \cdot e_r \cdot a = x \cdot \lambda_{0,a}(e_r) = x \cdot \lambda_{0,a}\lambda_{0,a}^{-1}(a) = x \cdot a = \lambda_{0,a}(x).$$

Since $\lambda_{0,a}$ is a substitution of the set Q, then the proved equality

$$\lambda_{0,a}(x \cdot e_r) = \lambda_{0,a}(x)$$

gives $x \cdot e_r = x$ for all $x \in Q$, that is the element e_r is a right unit element in the semigroup $(Q, \cdot)$.

In the same way one can prove that e_ℓ is a left unit element in $(Q,\cdot)$.

To establish that the element a_r^{-1} is a right inverse of a, note that

$$\lambda_{0,a}(a\cdot a_r^{-1}) = a\cdot a_r^{-1}\cdot a = a\cdot\lambda_{0,a}\lambda_{0,a}^{-2}(a) = a\cdot\lambda_{0,a}^{-1}(a) = a\cdot e_r = a.$$

Applying $\lambda_{0,a}^{-1}$ to the equality $\lambda_{0,a}(a\cdot a_r^{-1}) = a$, we get

$$a\cdot a_r^{-1} = \lambda_{o,a}^{-1}(a) = e_r.$$

Hence, the element a is right invertible.

Similarly we can prove that the element a_ℓ^{-1} is a left inverse of a, when the shift $\lambda_{1,a}$ is a substitution of the set Q. □

Corollary 2. *An element a of a binary semigroup is invertible iff it is* 0*-invertible and* 1*-invertible simultaneously.*

An element a of an associate (Q,f) of the type (s,n) is said to be: *right (left) invertible*, if the shift $\lambda_{0,a}$ (respectively $\lambda_{1,a}$) is a substitution of the set Q.

An element a of an $(n+1)$-ary groupoid (Q,f) will be called *inner invertible*, if the shift $\lambda_{i,a}$ is a substitution of the set Q for some $i=1,\dots,n-1$.

Corollary 3. *An element a is invertible in an associate (Q,f) of the type (s,n) iff it is right and left invertible simultaneously.*

The *Proof* follows from the point 2) of Theorem 3 when $i=0$.

Corollary 4. *In any $(n+1)$-ary semigroup (Q,f) for any element a and for any numbers $i=1,\dots,n-1$; $k=1,\dots,\frac{n}{s}-1$ the following assertions are equivalent:*

1) *a is invertible,*
2) *a is inner invertible,*
3) *a is right and left invertible,*
4) *there exist elements $\hat{a}$ and $\breve{a}$ in Q such that for arbitrary $x\in Q$ the following equalities hold:*

$$f(\overset{i}{a},\hat{a},\overset{n-i-1}{a},x) = x, \qquad f(x,\overset{n-i-1}{a},\breve{a},\overset{i}{a}) = x. \tag{15}$$

2. Axiomatics of polyagroups

Definition 1. A groupoid (Q,f) is called a *polyagroup of a type* (s,n) iff it is a quasigroup and an associate of the type (s,n).

It is easy to see that for $s=1$ a polyagroup of a type (s,n) is an $(n+1)$-ary group.

Directly from Theorem 3 and the definition of a polyagroup we obtain:

Theorem 4. *In an associate (Q,f) of the type (s,n) for any $i=0,1,\dots,n-1$ the following conditions are equivalent:*

1) *the associate is a polyagroup,*
2) *every element of the associate is invertible,*
3) *every element of the associate is i- and $(n-i)$-invertible,*
4) *for every element y there exist elements $\hat{y}$ and $\breve{y}$ in Q such that for arbitrary $x\in Q$ the following two equalities hold*

$$f(\overset{i}{y},\hat{y},\overset{n-i-1}{y},x)=x, \qquad f(x,\overset{n-i-1}{y},\breve{y},\overset{i}{y})=x,$$

5) *every element is ks-invertible, for some $k=1,\dots,\frac{n}{s}-1$.*

Since for $s=1$ a polyagroup of a type (s,n) is an $(n+1)$-group (an associate of the type $(1,n)$ is an $(n+1)$-semigroup), then as a simple consequence of the above Theorem, we obtain the following characterizations of $(n+1)$-ary groups, which are proved in [3 – 5].

Corollary 5. *In an $(n+1)$-semigroup (Q,f) for any $i=0,1,\dots,n-1$ the following assertions are equivalent:*

1) *a semigroup is an $(n+1)$-group,*
2) *every element of the semigroup is invertible,*
3) *every element is a right and left invertible,*
4) *every element is inner invertible,*
5) *for every element y there exist elements $\hat{y}$ and $\breve{y}$ in Q such that for arbitrary $x\in Q$ the following two equalities hold*

$$f(\overset{i}{y},\hat{y},\overset{n-i-1}{y},x)=x, \qquad f(x,\overset{n-i-1}{y},\breve{y},\overset{i}{y})=x.$$

References

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

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

[3] **W. A. Dudek**: *Varieties of polyadic groups*, Filomat **9** (1995), 657 – 674.

[4] **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.

[5] **A. M. Gal'mak**: *A new definition of n-ary groups*, (Russian), Voprosy Algebry i Prikl. Mat., Gomel 1995, 31 – 30.

[6] **L. M. Gluskin**: *Positional operatives*, (Russian), Mat. Sbornik **68** (1965), 444 – 472.

[7] **L. M. Gluskin**: *Polyadic semigroups*, (Russian), in "Theory of Semigroups and its Applications", Saratov, 1983, 10 – 19.

[8] **F. M. Sokhatsky**: *About associativity of multiplace operations*, (Russian), Diskretnaya matematyka **4** (1992), 66 – 84.

[9] **F. M. Sokhatsky**: *About classes of polyagroups*, In "Algebraicheskie issledovania", Inst. Mat. NAN Ukrainy, Kyiv 1996, 114 – 131.

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

[11] **F. N. Sokhatsky**: *On polyadic groups*, (Russian), Sovriemiennaya algebra **2(22)** (1997), 79 – 94.

[12] **F. M. Sokhatsky**: *Invertible elements in associates and semigroups. 1*, Quasigroups and Related Systems **5** (1998), 53 – 68.

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

Vinnytsia State Pedagogical University, Vinnytsia, 287100, Ukraine

Quasigroups and Related Systems **6** (1999), 81 – 86

On TS-n-groups

Janez Ušan

Abstract

In this article totally simmetric n-group is described as an n-groupoid (Q, B) in which the following laws hold: $B(x, y, a_1^{n-2}) = B(y, x, a_1^{n-2})$,
$B(a, c_1^{n-2}, B(B(B(z, c_1^{n-2}, z), c_1^{n-2}, b), c_1^{n-2}, B(B(z, c_1^{n-2}, z), c_1^{n-2}, a))) = b$,
$B(x, a_1^{n-2}, y) = B(x, a_1^{n-2}, B(B(y, a_1^{n-2}, y), a_1^{n-2}, y))$ and
$B(B(x, z, b_1^{n-2}), B(y, a_1^{n-2}, z), a_1^{n-2}) = B(x, y, b_1^{n-2})$.

1. Introduction

Definition 1.1. Let (Q, A) be an n-quasigroup and $n \geqslant 2$. Also let α be a permutation in the set $\{1, 2, ..., n+1\}$. Moreover, let

$$A^{\alpha}(x_1^n) = a_{n+1} \iff A(x_{\alpha(1)}, ..., x_{\alpha(n)}) = x_{\alpha(n+1)}$$

for all $x_1^{n+1} \in Q$. We say that (Q, A) is a *totally simmetric n-quasigroup* (briefly: *TS-n-quasigroup*) iff for any permutation α on $\{1, 2, ..., n+1\}$ we have $A^{\alpha} = A$. In the case when $\alpha = (1, n+1)$ instead of A^{α} we write ${}^{-1}A$. Similarly in the case $\alpha = (n, n+1)$ instead of A^{α} we write A^{-1}.

Proposition 1.2. *Let (Q, A) be an n-group, ${}^{-1}$ its inversing operation,* **e** *its $\{1, n\}$-neutral operation and $n \geqslant 2$. Also let*

(a) ${}^{-1}A(x, a_1^{n-2}, y) = z \iff A(z, a_1^{n-2}, y) = x$,

(b) $A^{-1}(x, a_1^{n-2}, y) = z \iff A(x, a_1^{n-2}, z) = y$

1991 Mathematics Subject Classification: 20N15

Keywords: $n-$groupoid, $n-$semigroup, $n-$quasigroup, $n-$group, $\{i, j\}$-neutral operation on $n-$groupoid, inversing operation on $n-$group, TS-$n-$group

for all $x, y, z \in Q$ *and for every* $a_1^{n-2} \in Q$. *Then, for all* $x, y \in Q$ *and for every* $a_1^{n-2} \in Q$ *the following equalities hold*

(1) $\ ^{-1}A(x, a_1^{n-2}, y) = A(x, a_1^{n-2}, (a_1^{n-2}, y)^{-1})$,

(2) $A^{-1}(x, a_1^{n-2}, y) = A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, y)$,

(3) $\mathbf{e}(a_1^{n-2}) = \ ^{-1}A(x, a_1^{n-2}, x)$,

(4) $(a_1^{n-2}, x)^{-1} = \ ^{-1}A(\ ^{-1}A(x, a_1^{n-2}, x), a_1^{n-2}, x)$,

(5) $A(x, a_1^{n-2}, y) = \ ^{-1}A(x, a_1^{n-2}, \ ^{-1}A(\ ^{-1}A(y, a_1^{n-2}, y), a_1^{n-2}, y))$.

Proof. To prove (2) observe that

$$\begin{aligned}
&A^{-1}(x, a_1^{n-2}, y) = z \Longleftrightarrow A(x, a_1^{n-2}, z) = y \\
&\Longleftrightarrow A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, A(x, a_1^{n-2}, z)) = A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, y) \\
&\Longleftrightarrow A(A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, x), a_1^{n-2}, z) = A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, y) \\
&\Longleftrightarrow A(\mathbf{e}(a_1^{n-2}), a_1^{n-2}, z) = A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, y) \\
&\Longleftrightarrow z = A((a_1^{n-2}, x)^{-1}, a_1^{n-2}, y).
\end{aligned}$$

The rest is proved in [7]. □

As a simple consequence of [2], [3] and [4] (see also [6]) we obtain:

Proposition 1.3. *Let* $n \geqslant 2$. *An* n*-group* (Q, A) *is a TS-*n*-group iff there exist a boolean group* $(Q, \cdot)$ *and element* $b \in Q$ *such that*

$$A(x_1^n) = x_1 \cdot \ldots \cdot x_n \cdot b$$

for all $x_1^n \in Q$.

2. Results

From the above we conclude that the following proposition holds.

Proposition 2.1. *Let* (Q, B) *be a TS-*n*-group with* $n \geqslant 2$. *Then*

(*i*) $B(B(x, z, b_1^{n-2}), B(y, a_1^{n-2}, z), a_1^{n-2}) = B(x, y, b_1^{n-2})$,

(*ii*) $B(a, c_1^{n-2}, B(B(B(z, c_1^{n-2}, z), c_1^{n-2}, b), c_1^{n-2}, B(B(z, c_1^{n-2}, z), c_1^{n-2}, a))) = b$,

(*iii*) $B(x, a_1^{n-2}, y) = B(x, a_1^{n-2}, B(B(y, a_1^{n-2}, y), a_1^{n-2}, y))$,

(*iv*) $B(x, y, a_1^{n-2}) = B(y, x, a_1^{n-2})$.

Theorem 2.2. *If the following laws*

$$(i)\quad B(B(x,z,b_1^{n-2}),B(y,a_1^{n-2},z),a_1^{n-2}) = B(x,y,b_1^{n-2}),$$

$$(ii)\quad B(a,c_1^{n-2},B(B(B(z,c_1^{n-2},z),c_1^{n-2},b),c_1^{n-2}, B(B(z,c_1^{n-2},z),c_1^{n-2},a))) = b,$$

$$(iii)\quad B(x,a_1^{n-2},y) = B(x,a_1^{n-2},B(B(y,a_1^{n-2},y),a_1^{n-2},y)),$$

$$(iv)\quad B(x,y,a_1^{n-2}) = B(y,x,a_1^{n-2})$$

hold in an n-groupoid (Q,B), $n \geqslant 2$, then (Q,B) is a TS-n-group.

Proof. For $n \geqslant 2$ the following statements hold.

1° Let (Q,B) be an n-groupoid. If the following two laws

$$B(B(x,z,b_1^{n-2}),B(y,a_1^{n-2},z),a_1^{n-2}) = B(x,y,b_1^{n-2}),$$

$$B(a,c_1^{n-2},B(B(B(z,c_1^{n-2},z),c_1^{n-2},b),c_1^{n-2}, B(B(z,c_1^{n-2},z),c_1^{n-2},a))) = b$$

hold in (Q,B), then there is an n-group (Q,A) such that ${}^{-1}\!A = B$. (see Theorem 2.2 in [7]).

2° There exists the n-ary operation ${}^{-1}B$ in Q such that $(Q, {}^{-1}B)$ is an n-group and ${}^{-1}B = B$.

Indeed, by 1°, we conclude that there is an n-group (Q,A) such that ${}^{-1}\!A = B$. Hence

$${}^{-1}({}^{-1}\!A)(x,a_1^{n-2},y) = z \Leftrightarrow {}^{-1}\!A(z,a_1^{n-2},y) = x \Leftrightarrow A(x,a_1^{n-2},y) = z.$$

Moreover for all $x,y \in Q$ and $a_1^{n-2} \in Q$ we have

$$B(x,a_1^{n-2},y) = B(x,a_1^{n-2},B(B(y,a_1^{n-2},y),a_1^{n-2},y)),$$

and

$${}^{-1}B(x,a_1^{n-2},y) = B(x,a_1^{n-2},B(B(y,a_1^{n-2},y),a_1^{n-2},y)),$$

which proves that ${}^{-1}B = B$.

3° For all $x \in Q$ and for every sequence a_1^{n-2} over Q we have $(a_1^{n-2},x)^{-1} = x$ (see Proposition 1.2 and Remark 1.3 in [7]). Thus $B^{-1} = B$, because by [7] we have

$$B^{-1}(x,a_1^{n-2},y) = B((a_1^{n-2},x)^{-1},a_1^{n-2},y).$$

4° For all $x,y \in Q$ and for every sequence a_1^{n-2} over Q the following equality holds $B(x,a_1^{n-2},y) = B(y,a_1^{n-2},x)$. Indeed,

$$B(x,a_1^{n-2},y)=z \Longleftrightarrow {}^{-1}B(x,a_1^{n-2},y)=z \Longleftrightarrow B(z,a_1^{n-2},y)=x$$
$$\Longleftrightarrow B^{-1}(z,a_1^{n-2},y)=x \Longleftrightarrow B(z,a_1^{n-2},x)=y$$
$$\Longleftrightarrow {}^{-1}B(y,a_1^{n-2},x)=z \Longleftrightarrow B(y,a_1^{n-2},x)=z.$$

5° Let $n\geq 3$ and $\mathbf{e}$ be a $\{1,n\}$-neutral operation of the n-group (Q,B). Then for all $x,y\in Q$ and for every sequence a_1^{n-2} over Q the following equality holds

$$B(\mathbf{e}(a_1^{n-2}),x,a_1^{n-2})=x.$$

To prove it we consider the new operation F defined by

$$F(x,a_1^{n-2}) \stackrel{def}{=} B(x,\mathbf{e}(a_1^{n-2}),a_1^{n-2}).$$

Then

$$B(F(x,a_1^{n-2}),\mathbf{e}(a_1^{n-2}),a_1^{n-2})=B(B(x,\mathbf{e}(a_1^{n-2}),a_1^{n-2}),\mathbf{e}(a_1^{n-2}),a_1^{n-2})$$

and

$$B(F(x,a_1^{n-2}),\mathbf{e}(a_1^{n-2}),a_1^{n-2})=B(x,B(\mathbf{e}(a_1^{n-2}),a_1^{n-2},\mathbf{e}(a_1^{n-2})),a_1^{n-2}).$$

This implies

$$B(F(x,a_1^{n-2}),\mathbf{e}(a_1^{n-2}),a_1^{n-2})=B(x,\mathbf{e}(a_1^{n-2}),a_1^{n-2}).$$

Thus

$$F(x,a_1^{n-2})=x \Longleftrightarrow B(x,\mathbf{e}(a_1^{n-2}),a_1^{n-2})=x.$$

But by (iv) we have

$$B(\mathbf{e}(a_1^{n-2}),x,a_1^{n-2})=B(x,\mathbf{e}(a_1^{n-2}),a_1^{n-2})=x,$$

which completes the proof of 5°.

6° Let $(Q,\{.,\varphi,b\})$ be an arbitrary nHG-algebra associated to the n-group (Q,B) (see [8]). Then, by Proposition 1.6 from [8], there is at least one sequence $a_1^{n-2}\in Q$ such that

$$x\cdot y=B(x,a_1^{n-2},y) \quad \text{and} \quad \varphi(x)=B(\mathbf{e}(a_1^{n-2}),x,a_1^{n-2})$$

for all $x,y\in Q$. Whence, by 4° and 5°, we conclude that

$$x\cdot y=y\cdot x \quad \text{and} \quad \varphi(x)=x.$$

Thus

$$\mathbf{e}(a_1^{n-2})\cdot x=x\cdot\mathbf{e}(a_1^{n-2})=B(x,a_1^{n-2},\mathbf{e}(a_1^{n-2}))=x$$

and

$$(a_1^{n-2},x)^{-1}\cdot x = x\cdot(a_1^{n-2},x)^{-1} = B(x,a_1^{n-2},(a_1^{n-2},x)^{-1}) = \mathbf{e}(a_1^{n-2})$$

by [7]. Hence $x^{-\mathbf{1}} \stackrel{def}{=} (a_1^{n-2},x)^{-1} = x$, which by our Proposition 1.3 completes the proof. □

Remark 2.3. Let $(K,\cdot)$, where $K=\{1,2,3,4\}$, be the Klein's group with the multiplication defined by the following table:

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	1	4	3
3	3	4	1	2
4	4	3	2	1

Then the permutation φ of K defined by

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

is an automorphism of $(K,\cdot)$ and $(K,\{\cdot,\varphi,2\})$ is a 3HG-algebra associated to a 3-group (K,A), where

$$A(x,y,z) = x\cdot\varphi(y)\cdot z\cdot 2.$$

Moreover, $\mathbf{e}(x) = 2\cdot\varphi(x)$, $(a,x)^{-1} = x$, and ${}^{-1}\!A = A = A^{-1}$.

It is not difficult to see that the laws $(i)-(iii)$ hold in this 3-group, but $A(2,4,2) = 4 \neq 3 = A(4,2,2)$.

References

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

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

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

[4] **W. A. Dudek and J. Michalski**: *On a generalization of a theorem of Timm*, Demonstratio Math. **18** (1985), 869 – 883.

[5] **M. Polonijo**: *Abelian totally symmetric n-quasigroups*, Proc. Symp. n-ary Structures, Skopje 1982, 185 – 193.

[6] **J. Ušan**: *On Hosszú-Gluskin algebras corresponding to the same n-group*, Rev. of Research, Fac. of Sci. Univ. of Novi Sad, Math. Ser. **25.1** (1995), 101 – 119.

[7] **J. Ušan**: *$n-$groups as n-groupoids with laws*, Quasigroups and Related Systems **4** (1997), 67 – 76.

[8] **J. Ušan and M. Žižović**: *On ordered n-groups*, Quasigroups and Related Systems **4** (1997), 77 – 87.

Institute of Mathematics
University of Novi Sad
Trg D. Obradovića 4
21000 Novi Sad
Yugoslavia

Received December 29, 1998

Quasigroups and Related Systems **6** (1999), 87 – 98

Fuzzy subquasigroups over a t-norm

Wiesław A. Dudek and Young Bae Jun

Abstract

In this paper, using a t-norm T, we introduce the notion of idempotent T-fuzzy subquasigroups of quasigroups, and investigate some of their properties. Also we describe fuzzy subquasigroups induced by t-norms in the direct product of quasigroups.

1. Introduction

Following the introduction of fuzzy sets by Zadeh [13], the fuzzy set theory developed by Zadeh himself and others have found many applications in the domain of mathematics and elsewhere. For example, in [7] Liu studied fuzzy subrings as well as fuzzy ideals in rings. Properties of some fuzzy ideals in semirings are investigated in [8]. Connections between fuzzy groups and so-called level subgroups are found in [3], [4] and [10]. The similar results for quasigroups are proved in [6].

In this paper, using a t-norm T, we introduce the notion of idempotent T-fuzzy subquasigroups of quasigroups, and investigate some of their properties. Next we use a t-norm to construct T-fuzzy subquasigroups in the finite direct product of quasigroups.

2. Preliminaries

As it is well known, a groupoid $(G,\cdot)$ is called a *quasigroup* if for any $a,b\in G$ each of the equations $ax=b,\ xa=b$ has a unique solution

1991 Mathematics Subject Classification: 20N15, 94D05
Keywords: quasigroup, fuzzy subquasigroup

in G. A quasigroup may be also defined as an algebra $(G,\cdot,\backslash,/)$ with three binary operations $\cdot,\backslash,/$ satisfying the identities

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

(cf. [2] or [9]). We say that such defined quasigroup $(G,\cdot,\backslash,/)$ is an *equasigroup* (i.e. *equationally definable quasigroup*) [9] or a *primitive quasigroup* [2]. Obviously, these two definitions are equivalent because

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

A nonempty subset S of a quasigroup $\mathcal{G}=(G,\cdot,\backslash,/)$ is called a *subquasigroup* if it is closed with respect to these three operations, i.e., if $x*y\in S$ for all $x,y\in S$ and $*\in\{\cdot,\backslash,/\}$.

The class of all equasigroups forms a variety. This means that a homomorphic image of an equasigroup is an equasigroup. Also every subset of an equasigroup closed with respect to these three operations is an equasigroup.

Note that in case when a quasigroup is defined as a set with only one operation, a homomorphic image is not in general a quasigroup. It is *only* a groupoid with division. Similarly a homomorphic preimage of a quasigroup $(G,\cdot)$ is not a quasigroup. Also a subset closed with respect to this multiplication is not a quasigroup (cf. [2]).

For the general development ot the theory of quasigroups the *unipotent quasigroups*, i.e., quasigroups with the identity $xx=yy$, play an important role. These quasigroups are connected with Latin squares which have one fixed element in the diagonal (cf. [5]). Such quasigroups may be defined as quasigroups G with the special element θ satisfying the identity $xx=\theta$. Obviously, θ is uniquely determined and it is an idempotent, but, in general, it is not the (left, right) neutral element.

To avoid repetitions we use the following conventions: *"a quasigroup $\mathcal{G}$"* always denotes an equasigroup $(G,\cdot,\backslash,/)$; G always denotes a nonempty set.

A function $\mu:G\to[0,1]$ is called *a fuzzy set* in a quasigroup $\mathcal{G}$. The set $\mu_\alpha=\{x\in G:\mu(x)\geqslant\alpha\}$, where $\alpha\in[0,1]$ is fixed, is called *a level subset of* μ. $Im(\mu)$ denotes the imege set of μ.

Let μ and ρ be two fuzzy sets defined on G. According to [13] we say that μ is contained in ρ, and denote this fact by $\mu\subseteq\rho$, iff

$\mu(x) \leqslant \rho(x)$ for all $x \in G$. Obviously $\mu = \rho$ iff $\mu(x) = \rho(x)$ for all $x \in G$.

According to [6], a fuzzy set μ in a quasigroup $\mathcal{G} = (G, \cdot, \backslash, /)$ is called a *fuzzy subquasigroup* of $\mathcal{G}$ if

$$\min\{\mu(xy),\, \mu(x \setminus y),\, \mu(x/y)\} \geqslant \min\{\mu(x),\, \mu(y)\}$$

for all $x, y \in G$. It is clear, that this condition may be written as

$$\mu(x * y) \geqslant \min\{\mu(x),\, \mu(y)\}$$

for all $* \in \{\cdot, \backslash, /\}$ and $x, y \in G$.

A fuzzy subquasigroup μ of a quasigroup $\mathcal{G}$ is called *normal* if $\mu(xy) = \mu(yx)$ for all $x, y \in G$. It is not difficult to see that μ is normal iff $\mu(x \setminus y) = \mu(y/x)$ for all $x, y \in G$.

The following two results are proved in [6].

Proposition 2.1. *A fuzzy set μ of a quasigroup $\mathcal{G} = (G, \cdot, \backslash, /)$ is a fuzzy subquasigroup iff for every $\alpha \in [0,1]$, μ_α is either empty or a subquasigroup of G.* □

Proposition 2.2. *If μ is a fuzzy subquasigroup of a unipotent quasigroup $(G, \cdot, \backslash, /, \theta)$, then $\mu(\theta) \geqslant \mu(x)$ for any $x \in G$.* □

3. T-fuzzy subquasigroup

According to [1], by a *t-norm*, we mean a function $T : [0,1] \times [0,1] \to [0,1]$ satisfying the following conditions:

(T_1) $T(\alpha, 1) = \alpha\,,$
(T_2) $T(\alpha, \beta) \leqslant T(\alpha, \gamma)$ whenever $\beta \leqslant \gamma\,,$
(T_3) $T(\alpha, \beta) = T(\beta, \alpha)\,,$
(T_4) $T(\alpha, T(\beta, \gamma)) = T(T(\alpha, \beta), \gamma)$

for all $\alpha, \beta, \gamma \in [0,1]$.

A simple example of a t-norm is a function $T(\alpha, \beta) = \min\{\alpha, \beta\}$. Generally, $T(\alpha, \beta) \leqslant \min\{\alpha, \beta\}$ and $T(\alpha, 0) = 0$ for all $\alpha, \beta \in [0,1]$.

Moreover, $([0,1];T)$ is a commutative semigroup with 0 as the neutral element. In particular it is *medial*, i.e.,

$$T(T(\alpha,\beta),\,T(\gamma,\delta)) = T(T(\alpha,\gamma),\,T(\beta,\delta))$$

holds for all $\alpha,\beta,\gamma,\delta\in[0,1]$.

Let T_1 and T_2 be two t-norms. We say that T_1 dominates T_2 and write $T_1\gg T_2$ if

$$T_1(T_2(\alpha,\beta),\,T_2(\gamma,\delta)) \geqslant T_2(T_1(\alpha,\gamma),\,T_1(\beta,\delta))$$

for all $\alpha,\beta,\gamma,\delta\in[0,1]$ (cf. [1]). Obviously $T\gg T$ for all t-norms.

The set of all idempotents with respect to T, i.e. the set

$$E_T=\{\alpha\in[0,1]\ \mid\ T(\alpha,\alpha)=\alpha\}$$

is a subsemigroup of $([0,1],T)$. If $Im(\mu)\subseteq E_T$ then a fuzzy set μ is called an *idempotent with respect to a t-norm T* (briefly: *T-idempotent*).

Definition 3.1. A fuzzy set μ in G is called a *fuzzy subquasigroup of $\mathcal{G}$ with respect to a t-norm T* (briefly, a *T-fuzzy subquasigroup*) if

$$\mu(x*y)\geqslant T(\mu(x),\,\mu(y))$$

for all $x,y,z\in G$ and $*\in\{\cdot,\backslash,/\}$.

Since $\min\{\alpha,\,\beta\}\geqslant T(\alpha,\,\beta)$ for all $\alpha,\beta\in[0,1]$, every fuzzy subquasigroup is also a T-fuzzy subquasigroup, but not conversely as seen in the following example.

Example 3.2. Let $G=\{0,a,b,c\}$ be the Klein's group with the following Cayley table:

$\cdot$	0	a	b	c
0	0	a	b	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

Define a fuzzy set μ in G by $\mu(0)=0,8$, $\mu(a)=0,7$, $\mu(b)=0,6$, $\mu(c)=0,5$. It is not difficult to see that a function T_m defined by $T_m(\alpha,\beta)=\max\{\alpha+\beta-1,\,0\}$ for all $\alpha,\beta\in[0,1]$ is a t-norm.

By routine calculations, we known that $\mu(x*y)\geqslant T_m(\mu(x),\,\mu(y))$ for all $x,y\in G$, which shows that μ is a T_m-fuzzy subquasigroup of $\mathcal{G}$, which is not T_m-idempotent. It is not a fuzzy subquasigroup since $\mu(c)=\mu(ab)<\min\{\mu(a),\,\mu(b)\}$.

But a fuzzy set ν defined by $\nu(0)=\nu(a)=1$ and $\nu(b)=\nu(c)=0$ is a T_m-idempotent fuzzy subquasigroup of G. It is also a fuzzy subquasigroup. □

Proposition 3.3. *If a fuzzy set μ is idempotent with respect to a t-norm T, then $T(\alpha,\beta)=\min\{\alpha,\beta\}$ for all $\alpha,\beta\in Im(\mu)$.*

Proof. Indeed, if α and β are in $Im(\mu)$, then

$$\min\{\alpha,\beta\}\geqslant T(\alpha,\beta)\geqslant T(\min\{\alpha,\beta\},\,\min\{\alpha,\beta\})=\min\{\alpha,\beta\},$$

which completes the proof. □

Corollary 3.4. *Every T-idempotent fuzzy subquasigroup is also a fuzzy subquasigroup.* □

By application of Proposition 2.1 we obtain

Corollary 3.5. *Every nonempty level set of a T-idempotent fuzzy subquasigroup defined on a quasigroup $\mathcal{G}$ is a subquasigroup of $\mathcal{G}$.* □

Corollary 3.6. *Let T be an idempotent t-norm. Then a fuzzy set defined on a quasigroup $\mathcal{G}$ is a T-fuzzy subquasigroup iff it is a fuzzy subquasigroup.* □

Now we consider the converse of Corollary 3.4.

Theorem 3.7. *Let a fuzzy set μ on a quasigroup $\mathcal{G}$ be idempotent with respect to a t-norm T. If each nonempty level set μ_α is a subquasigroup of $\mathcal{G}$, then μ is a T-idempotent fuzzy subquasigroup.*

Proof. Assume that each nonempty level set μ_α is a subquasigroup of $\mathcal{G}$. Then μ is a fuzzy subquasigroup of $\mathcal{G}$ (by Proposition 2.1), and so

$$\mu(x*y)\geqslant\min\{\mu(x),\,\mu(y)\}=T(\,\mu(x),\mu(y)\,)$$

by Proposition 3.3. Hence μ is a T-idempotent fuzzy subquasigroup of a quasigroup $\mathcal{G}$. □

Theorem 3.8. *Let μ be a T-fuzzy subquasigroup of $\mathcal{G}$, where T is a t-norm and $\alpha \in [0,1]$. Then*

(i) *if $\alpha = 1$, then μ_α is either empty or is a subquasigroup of $\mathcal{G}$,*

(ii) *if $T = \min$, then μ_α is either empty or is a subquasigroup of $\mathcal{G}$.*

Proof. (i) Assume that $\alpha = 1$ and $\mu_\alpha \neq \emptyset$. Then there exist $x, y \in \mu_\alpha$ such that $\mu(x) \geqslant 1$ and $\mu(y) \geqslant 1$. Thus

$$\mu(x * y) \geqslant T(\,\mu(x), \mu(y)\,) \geqslant T(1,1) = 1$$

so that $x * y \in \mu_1$. Hence μ_1 is a subquasigroup of $\mathcal{G}$.

(ii) is a consequence of Proposition 2.1. □

Note that a fuzzy set μ defined in our Example 3.2 is a non-idempotent T_m-fuzzy subquasigroup in which μ_1 is empty and $\mu_{0,6}$ is not a subquasigroup of $\mathcal{G}$. This proves that the analog of Proposition 2.1 for T-fuzzy subquasigroups is not true.

4. Fuzzy sets induced by norms

Let T be a t-norm and let μ and ν be two fuzzy sets in G. Then the *T-product of μ and ν*, denoted by $[\mu \cdot \nu]_T$, is defined as

$$[\mu \cdot \nu]_T(x) = T(\mu(x), \nu(x))$$

for all $x \in G$.

Obviously $[\mu \cdot \nu]_T$ is a fuzzy set in G such that $[\mu \cdot \nu]_T = [\nu \cdot \mu]_T$. Moreover, if μ and ν are normal, then so is $[\mu \cdot \nu]_{T^*}$.

Theorem 4.1. *Let T be a t-norm and let μ and ν be T-fuzzy subquasigroups of $\mathcal{G}$. If a t-norm T^* dominates T, then T^*-product $[\mu \cdot \nu]_{T^*}$ is a T-fuzzy subquasigroup of $\mathcal{G}$.*

Proof. Indeed, for $x, y \in G$ we have

$$\begin{aligned}[\mu \cdot \nu]_{T^*}(x * y) &= T^*(\mu(x * y), \nu(x * y)) \\ &\geqslant T^*(T(\mu(x), \mu(y)),\, T(\nu(x), \nu(y)))\end{aligned}$$

$$\geqslant T(T^*(\mu(x),\nu(x)),\, T^*(\mu(y),\nu(y)))$$
$$= T([\mu\cdot\nu]_{T^*}(x),\, [\mu\cdot\nu]_{T^*}(y))\,,$$

which proves that $[\mu\cdot\nu]_{T^*}$ is a T-fuzzy subquasigroup of $\mathcal{G}$. □

Corollary 4.2 *The T-product of T-fuzzy subquasigroups is a T-fuzzy subquasigroup.* □

Let G and H be nonempty sets and let $f: G \to H$ be an arbitrary mapping. If ν is a fuzzy set in $f(G)$ then $\mu = \nu\circ f$ is the fuzzy set in G, which is called the *preimage of ν under f*.

It is not difficult to see that the following lemma is true.

Lemma 4.3. *Let T be a t-norm and let $\mathcal{G}$ and $\mathcal{H}$ be two quasigroups. If $h:\mathcal{G}\to\mathcal{H}$ is an onto homomorphisms of quasigroups, ν is a fuzzy subquasigroup of $\mathcal{H}$ and μ the preimage of ν under h, then μ is a fuzzy subquasigroup of $\mathcal{G}$. Moreover, μ is normal iff ν is normal. If ν is T-idempotent, then so is μ.* □

Proposition 4.4. *Let T and T^* be t-norms in which T^* dominates T and let $\mathcal{G}$, $\mathcal{H}$ be two quasigroups. If $h:\mathcal{G}\to\mathcal{H}$ be an onto homomorphism of quasigroups, then for any T-fuzzy subquasigroups μ and ν of $\mathcal{H}$, we have*

$$h^{-1}([\mu\cdot\nu]_{T^*}) = [h^{-1}(\mu)\cdot h^{-1}(\nu)]_{T^*}.$$

Proof. By Lemma 4.3 $h^{-1}(\mu)$, $h^{-1}(\nu)$ and $h^{-1}([\mu\cdot\nu]_{T^*})$ are T-fuzzy subquasigroups of $\mathcal{G}$.

Moreover for $x\in G$ we have

$$[h^{-1}([\mu\cdot\nu]_{T^*})](x) = [\mu\cdot\nu]_{T^*}(h(x)) = T^*(\mu(h(x)),\nu(h(x)))$$
$$= T^*([h^{-1}(\mu)](x),\, [h^{-1}(\nu)](x)) = [h^{-1}(\mu)\cdot h^{-1}(\nu)]_{T^*}(x),$$

which completes the proof. □

We say that a fuzzy set μ in G has a *sup property* if, for all subset $S\subseteq G$, there exists $s_0\in S$ such that $\mu(s_0) = \sup\limits_{s\in S}\mu(s)$. In this case for any mapping f defined on G we can define in $f(G)$ the fuzzy set μ^f putting $\mu^f(y) = \sup\limits_{x\in f^{-1}(y)}\mu(x)$ for all $y\in f(G)$ (cf. [12]).

Let $f:\mathcal{G}\to\mathcal{H}$ be a homomorphisms of quasigroups and let T be a continuous t-norm (continuous with respect to the usual topology). Then sets $A_1=f^{-1}(y_1)$ and $A_2=f^{-1}(y_2)$, where $y_1,y_2\in f(G)$ are nonempty subsets of $f(G)$. Similarly, $A_3=f^{-1}(y_1*y_2)$, where $*\in\{\cdot,\backslash,/\}$ is a fixed operation.

Consider the set

$$A_1*A_2=\{a_1*a_2,\ \mid\ a_1\in A_1,\ a_2\in A_2\}.$$

If $x\in A_1*A_2$, then $x=x_1*x_2$ for some $x_1\in A_1$ and $x_2\in A_2$, and so

$$f(x)=f(x_1*x_2)=f(x_1)*f(x_2)=y_1*y_2\,,$$

which implies $x\in f^{-1}(y_1*y_2)=A_3$. Thus $A_1*A_2\subseteq A_3$ for any operation $*\in\{\cdot,\backslash,/\}$.

Therefore

$$\begin{aligned}\mu^f(y_1*y_2)&=\sup_{x\in f^{-1}(y_1*y_2)}\mu(x)\ =\ \sup_{x\in A_3}\mu(x)\\&\geqslant\sup_{x\in A_1*A_2}\mu(x)\ \geqslant\sup_{x_1\in A_1,\,x_2\in A_2}\mu(x_1*x_2)\\&\geqslant\sup_{x_1\in A_1,\,x_2\in A_2}T(\mu(x_1),\,\mu(x_2))\,.\end{aligned}$$

Since t-norm T is (by the assumption) continuous, for every $\varepsilon>0$ there exists $\delta>0$ such that

$$\sup_{x_1\in A_1}\mu(x_1)-t_1\leqslant\delta\quad\text{and}\quad\sup_{x_2\in A_2}\mu(x_2)-t_2\leqslant\delta$$

implies

$$T\left(\sup_{x_1\in A_1}\mu(x_1),\,\sup_{x_2\in A_2}\mu(x_2)\right)-T(t_1,\,t_2)\leqslant\varepsilon\,.$$

This for $t_1=\mu(a_1)$, $t_2=\mu(a_2)$, where $a_1\in A_1$, $a_2\in A_2$, gives

$$T\left(\sup_{x_1\in A_1}\mu(x_1),\,\sup_{x_2\in A_2}\mu(x_2)\right)\leqslant T(\mu(a_1),\,\mu(a_2))+\varepsilon\,.$$

Consequently

$$\begin{aligned}\mu^f(y_1*y_2)&\geqslant\sup_{x_1\in A_1,\,x_2\in A_2}T(\mu(x_1),\,\mu(x_2))\\&\geqslant T\left(\sup_{x_1\in A_1}\mu(x_1),\,\sup_{x_2\in A_2}\mu(x_2)\right)=T(\mu^f(y_1),\,\mu^f(y_2))\,,\end{aligned}$$

which shows that μ^f is a T-fuzzy subquasigroup of $f(\mathcal{G})$.

Thus we have the following

Theorem 4.5. *Let T be a continuous t-norm and let f be a homomorphism on a quasigroup $\mathcal{G}$. If a T-fuzzy subquasigroup μ of $\mathcal{G}$ has the sup property, then μ^f is a T-fuzzy subquasigroup of $f(\mathcal{G})$.* □

Since the function "min" is a continuous t-norm, then, as a simple consequence of the above theorem, we obtain

Corollary 4.6. *If a fuzzy subquasigroup μ of $\mathcal{G}$ has the sup property, then μ^f is a fuzzy subquasigroup of $f(\mathcal{G})$ for every homomorphism f defined on $\mathcal{G}$.* □

5. Direct products of fuzzy subquasigroups

Let T be a fixed t-norm. If μ_1 and μ_2 are two fuzzy sets on G_1 and G_2 (respectively), then μ defined on $G_1 \times G_2$ by the formula

$$\mu(x_1, x_2) = T(\mu_1(x_1), \mu_2(x_2)),$$

is a fuzzy set on $G_1 \times G_2$, which is denoted by $\mu_1 \times \mu_2$.

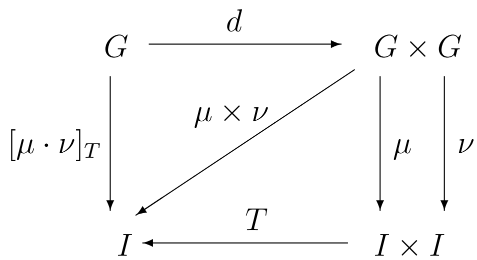
Proposition 5.1. *If μ_1 and μ_2 are T-fuzzy subquasigroup of quasigroups $\mathcal{G}_1$ and $\mathcal{G}_2$ (respectively), then $\mu_1 \times \mu_2$ is a T-fuzzy subquasigroup of the direct product $\mathcal{G}_1 \times \mathcal{G}_2$. Moreover, if μ_1 and μ_2 are T-idempotent, then so is $\mu_1 \times \mu_2$.*

Proof. Let (x_1, x_2), (y_1, y_2) be in $G_1 \times G_2$. Then

$$\begin{aligned}(\mu_1 \times \mu_2)((x_1, x_2) * (y_1, y_2)) &= (\mu_1 \times \mu_2)(x_1 * y_1,\, x_2 * y_2)\\ &= T(\mu_1(x_1 * y_1),\, \mu_2(x_2 * y_2))\\ &\geq T(T(\mu_1(x_1),\, \mu_1(y_1)),\, T(\mu_2(x_2),\, \mu_2(y_2)))\\ &= T(T(\mu_1(x_1),\, \mu_2(x_2)),\, T(\mu_1(y_1),\, \mu_2(y_2)))\\ &= T((\mu_1 \times \mu_2)(x_1, x_2),\, (\mu_1 \times \mu_2)(y_1, y_2)).\end{aligned}$$

Hence $\mu_1 \times \mu_2$ is a T-fuzzy subquasigroup of $\mathcal{G}_1 \times \mathcal{G}_2$. Obviously, if μ_1 and μ_2 are T-idempotent, then so is $\mu_1 \times \mu_2$. □

The relationship between T-fuzzy subquasigroups $\mu\times\nu$ and $[\mu\cdot\nu]$ can be viewed via the following diagram



where $I=[0,1]$ and $d:G\to G\times G$ is defined by $d(x)=(x,x)$.

Applying Lemma 3.2 from [1] it is not difficult to see that $[\mu\cdot\nu]_T$ *is the preimage of* $\mu\times\nu$ *under* d.

Note by the way, that our T-product is different from the product of fuzzy sets studied by Liu [7] and Sessa [11].

Now we generalize this idea to the product of $n\geqslant 2$ T-fuzzy subquasigroups. We first need to generalize the domain of t-norm T to $\prod\limits_{i=1}^{n}[0,1]$ as follows:

Definition 5.2. The function $T_n:\prod\limits_{i=1}^{n}[0,1]\to[0,1]$ is defined by

$$T_n(\alpha_1,\alpha_2,\ldots,\alpha_n)=T(\alpha_i,T_{n-1}(\alpha_1,\ldots,\alpha_{i-1},\alpha_{i+1},\ldots,\alpha_n))$$

for all $1\leqslant i\leqslant n$, where $n\geqslant 2$, $T_2=T$ and $T_1=id$ (identity).

Using the induction on n, we have the following two lemmas.

Lemma 5.3. *For every t-norm* T *and every* $\alpha_i,\beta_i\in[0,1]$, *where* $1\leqslant i\leqslant n$ *and* $n\geqslant 2$, *we have*

$$T_n(T(\alpha_1,\beta_1),T(\alpha_2,\beta_2),\ldots,T(\alpha_n,\beta_n))$$
$$=T(T_n(\alpha_1,\alpha_2,\ldots,\alpha_n),T_n(\beta_1,\beta_2,\ldots,\beta_n)).\ \square$$

Lemma 5.4. *For a t-norm* T *and every* $\alpha_1,\ldots,\alpha_n\in[0,1]$, *where* $n\geqslant 2$, *we have*

$$T_n(\alpha_1,\ldots,\alpha_n)=T(\ldots T(T(T(\alpha_1,\alpha_2),\alpha_3),\alpha_4),\ldots,\alpha_n)$$
$$=T(\alpha_1,T(\alpha_2,T(\alpha_3,\ldots T(\alpha_{n-1},\alpha_n)\ldots))).\ \square$$

Theorem 5.5. *Let T be a t-norm and let $\mathcal{G} = \prod_{i=1}^{n} \mathcal{G}_i$ be the direct product of quasigroups $\{\mathcal{G}_i\}_{i=1}^{n}$. If μ_i is a T-fuzzy subquasigroup of $\mathcal{G}_i$, where $1 \leqslant i \leqslant n$, then $\mu = \prod_{i=1}^{n} \mu_i$ defined by*

$$\mu(x) = (\prod_{i=1}^{n} \mu_i)(x_1, x_2, \ldots, x_n) = T_n(\mu_1(x_1), \mu_2(x_2), \ldots, \mu_n(x_n))$$

for all $x = (x_1, x_2, \ldots, x_n) \in G$, is a T-fuzzy subquasigroup of $\mathcal{G}$. Moreover, if all μ_i are T-idempotent, then so is μ.

Proof. Now let $x = (x_1, x_2, \ldots, x_n)$, $y = (y_1, y_2, \ldots, y_n)$ be any elements of $G = \prod_{i=1}^{n} G_i$. Then by Lemma 5.3 we have

$$\begin{aligned}
\mu(x * y) &= (\prod_{i=1}^{n} \mu_i)((x_1, x_2, \ldots, x_n) * (y_1, y_2, \ldots, y_n)) \\
&= (\prod_{i=1}^{n} \mu_i)((x_1 * y_1,\ x_2 * y_2, \ldots, x_n * y_n)) \\
&= T_n(\mu_1(x_1 * y_1), \mu_2(x_2 * y_2), \ldots, \mu_n(x_n * y_n)) \\
&\geqslant T_n(T(\mu_1(x_1),\ \mu_1(y_1)), T(\mu_2(x_2),\ \mu_2(y_2)), \ldots, T(\mu_n(x_n),\ \mu_n(y_n))) \\
&= T(T_n(\mu_1(x_1),\ \mu_2(x_2), \ldots, \mu_n(x_n)), T_n(\mu_1(y_1),\ \mu_2(y_2), \ldots, \mu_n(y_n))) \\
&= T((\prod_{i=1}^{n} \mu_i)(x_1, x_2, \ldots, x_n),\ (\prod_{i=1}^{n} \mu_i)(y_1, y_2, \ldots, y_n)) \\
&= T(\mu(x),\ \mu(y)).
\end{aligned}$$

Therefore $\mu = \prod_{i=1}^{n} \mu_i$ is a T-fuzzy subquasigroup of $\mathcal{G}$.

Applying Lemma 5.3 it is not difficult to see that μ is T-idempotent if all μ_i are T-idempotent. □

References

[1] **M. T. Abu Osman**: *On some product of fuzzy subgroups*, Fuzzy Sets and Systems **24** (1987), 79 – 86.

[2] **V. D. Belousov**: *Foundations of the theory of quasigroups and loops*, Nauka, Moscow 1967.

[3] **P. Bhattacharya and N. P. Mukherjee**: *Fuzzy relations and fuzzy groups*, Inform. Sci. **36** (1985), 267 – 282.

[4] **P. S. Das**: *Fuzzy groups and level subgroups*, J. Math. Anal. Appl. **84** (1981), 264 – 269.

[5] **J. Dénes and A. D. Keedwell**: *Latin squares an their applications*, New York 1974.

[6] **W. A. Dudek**: *Fuzzy subquasigroups*, Quasigroups and Related Systems **5** (1998), 81 – 98.

[7] **W. J. Liu**: *Fuzzy invariant subgroups and fuzzy ideals*, Fuzzy Sets and Systems **8** (1982), 133 – 139.

[8] **D. S. Malik and J. N. Mordeson**: *Extensions of fuzzy subring and Fuzzy ideals*, Fuzzy Sets and Systems **45** (1992), 245 – 251.

[9] **H. O. Pflugfelder**: *Quasigroups and loops: introduction*, Sigma Series in Pure Math., vol. **7**, Heldermann Verlag, Berlin 1990.

[10] **A. Rosenfeld**: *Fuzzy groups*, J. Math. Anal. Appl. **35** (1971), 512 – 517.

[11] **S. Sessa**: *On fuzzy subgroups and fuzzy ideals under triangular norm*, Fuzzy Sets and Systems **13** (1984), 95 – 100.

[12] **Y. Yu, J. N. Mordeson and S. C. Chen**: *Elements of L-algebras*, Lecture Notes in Fuzzy Math., Creighton Univ. Nebraska 1994.

[13] **L. A. Zadeh**: *Fuzzy sets*, Inform. Control **8** (1965), 338 – 353.

Received December 28, 1999

W. A. Dudek
Institute of Mathematics
Technical University of Wrocław
Wybrzeże Wyspiańskiego 27
50-370 Wrocław
Poland
e-mail: dudek@im.pwr.wroc.pl

Y. B. Jun
Department of Mathematics Education
Gyeongsang National University
Chinju 660-701
Korea
e-mail : ybjun@nongae.gsnu.ac.kr