Quasigroups and Related Systems **22** (2014), 1 − 8

On multiplicative conjugate loops

Shumaila Ambreen and Asif Ali

Abstract. The objective of this paper is twofold. Firstly to define MC-loops and show that every conjugate of subloops of such loops also are subloops Secondly to investigate various properties of MC-loops and its relation with numerous other already existing loops, moreover number of examples and counter examples are provided to make these relations more clearer.

1. Introduction

A loop L is an *inverse property loop* [2] if every $x \in L$ has a unique two-sided inverse, denoted by x^{-1}, and if, for all $x, y \in L$ the loop satisfies

$$x^{-1}(xy) = y = (yx)x^{-1}.$$

A loop L is said to be a *conjugate loop* [1] if it satisfies the following identity $x\left(yx^{-1}\right) = (xy)\,x^{-1}$, for all $x, y \in L$. A loop is *IP-conjugate* [1] if it satisfies inverse property and conjugate property. Smallest non-associative IP-conjugate loop is of order 7.

Following [1], flexible C-loops are conjugate IP-loops. Every diassociative loop is a conjugate IP-loop. Conjugate IP-loop L is commutative iff every element in L is self conjugate.

An IP-conjugate loop L is called a *multiplicative conjugate loop* (MC-loop) iff for all $x, y, g \in L$, we have

$$(xy)^g = x^g y^g.$$

Proposition 1.1. *An IP-conjugate loop L is MC-loop iff $T_g(xy) = T_g(x)T_g(y)$ for $T_g \in INN(L)$.*

Proof. Indeed,

$$\begin{aligned}(xy)^g = x^g y^g &\Leftrightarrow g^{-1}(xy)g = (g^{-1}.xg)(g^{-1}.yg)\\ &\Leftrightarrow (xy)R_gL_{g^{-1}} = (x)R_gL_{g^{-1}}.(y)R_gL_{g^{-1}}\\ &\Leftrightarrow (xy)R_gL_g^{-1} = (x)R_gL_g^{-1}.(y)R_gL_g^{-1} \quad \text{because } L \text{ is an } IP\text{-loop.}\\ &\Leftrightarrow (xy)T_g = (x)T_g.(y)T_g\end{aligned}$$

□

2010 Mathematics Subject Classification: 20N05
Keywords: Multiplicative conjugate loop, conjugate of a subloop, conjuagate loop.

2. Counting of multiplicative conjugate loops

In [8] J. Slaney and A. Ali enumerated IP-loops up to order 13 by using finite domain enumerator FINDER. Using that enumeration and our following GAP code we have counted multiplicative conjugate loops.

```
function(L):=IsMCLoop
local x, y, z;
if not IsConjugateIPLoop(L) then return false;
for x in L do
for y in L do
for z in L do
if z^-1*(x*y)*z <> (z^-1*x*z)*(z^-1*y*z) then return false;
fi;
od;od;od;
return true;
end;
```

Size	IP	*Conjugate* IP	MC
7	2	1	1
8	8	0	0
9	7	0	0
10	47	7	6
11	49	3	3
12	2684	27	17
13	10600	16	10

Number of IP, conjugate IP and MC-loops of order $n = 7, \dots, 13$.

Example 2.1. The smallest non-associative MC-loop has the form.

.	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7
2	2	3	1	6	7	5	4
3	3	1	2	7	6	4	5
4	4	7	6	5	1	2	3
5	5	6	7	1	4	3	2
6	6	4	5	3	2	7	1
7	7	5	4	2	3	1	6

3. Properties of MC-loops

We start with the following obvious lemma.

Lemma 3.1. *In an MC-loop L every $T \in INN(L)$ is pseudo-automorphism with companion* 1. □

Theorem 3.2. *The nucleus of an MC-loop L is a normal subloop.*

Proof. As L is MC-loop so L is also an IP-loop. Moreover let $T : L \to L$ be pseudo-automorphism as described in Lemma 3.1. The restriction of a pseudo-automorphism T from Lemma 3.1 T to the nucleus N of L is an automorphism of N. Hence $aN = Na$ for all $a \in L$ and $N(xy) = (Nx)y$, $(xy)N = x(yN)$ from the definition of a nucleus. □

Theorem 3.3. *A homomorphic image of an MC-loop is an MC-loop.*

Proof. Obvious. □

Proposition 3.4. *If L is an MC-loop, then $[x^y, z^y] = [x, z]^y$ for all $x, y, z \in L$.*

Proof. Indeed,

$$\begin{aligned}[x^y, z^y] &= (x^y)^{-1}(z^y)^{-1} \cdot x^y z^y = (x^{-1})^y (z^{-1})^y \cdot x^y z^y \\ &= (x^{-1}z^{-1})^y \cdot (x^y z^y) = (x^{-1}z^{-1} \cdot xz)^y = [x, z]^y.\end{aligned}$$ □

Theorem 3.5. *Let L be an MC-loop, then $[L, L] = \langle [x, y]; x, y \in L\rangle$ is a weak normal subloop of L.*

Proof. In fact, we have $[L, L]^l = [L^l, L^l] = [L, L]$ for every $l \in L$. □

Theorem 3.6. *If L is an MC-loop and $H \leqslant L$, then $H^x = \{x^{-1}hx : \ \forall h \in H\}$ is a subloop of L.*

Proof. For $x \in L$ and $a, b \in H^x$, there exists $h_1, h_2 \in H$ such that $a = x^{-1}h_1x$ and $b = x^{-1}h_2x$. Thus, $ab = (x^{-1}h_1x)(x^{-1}h_2x) = h_1^x h_2^x = (h_1h_2)^x \in H^x$. Analogously, $a^{-1} = (x^{-1}hx)^{-1} = x^{-1}h^{-1}x = (h^{-1})^x \in H^x$. Thus, $H^x \leqslant L$. □

Theorem 3.7. *In an MC-loop the conjugate of a maximal subloop is also maximal.*

Proof. Let M be a maximal subloop of an MC-loop L. Then M^g is its conjugate subloop. If there is a subloop H such that $M^g \leqslant H \leqslant L$, then $M \leqslant H^{g^{-1}} \leqslant L^{g^{-1}}$. Hence, $M \leqslant H^{g^{-1}} \leqslant L$ which is a contradiction. So, M is maximal. □

Recall that an intersection of all maximal subloops is again a subloop. It is known as the *Frattini subloop*. For a loop L, the Frattini subloop is denoted by $\Phi(L)$.

Theorem 3.8. *If L is an MC-loop, then $\Phi(L)$ is a weak normal in L.*

Proof. Let $\{M_i : i \in I\}$ be the family of all maximal subloops of L and $\Phi(L) = \cap_{i \in I} M_i$. Then $x \in \Phi(L)$ implies $x^g \in \Phi(L)$ for all $g \in L$. Hence, $\Phi(L)$ is weakly normal in L. □

The subloop generated by all the nilpotent normal subloops of L is called the *Fitting subloop* of L and is denoted by $Fit(L)$. Below we prove that in MC-loops it is normal.

Lemma 3.9. *If M and N be normal subloops of an MC-loop L, then the product $MN = \{mn : m \in M, n \in N\}$ is also a normal subloop of L.*

Proof. Let L be an MC-loop and M, N be its two normal subloops. Then for any $m \in M$, $n \in N$ and $l \in L$ we have $(mn)^l = m^l n^l \in MN$. Moreover,

$$(mn \cdot y)z = (m(n_1y))z = m_1(n_1y \cdot z) = m_1(n_2 \cdot yz) = m_2n_2(yz).$$

Similarly, we can prove that $(yz)(MN) = y(z(MN)$. Hence, MN is normal. □

Remark 3.10. It can be shown by induction that the product of a finite family of normal subloops of any MC-loop is its normal subloop.

Theorem 3.11. *If L be an MC-loop, then $Fit(L)$ is normal in L.*

Proof. Let $Fit(L) = \langle N_1, N_2, N_3, \ldots, N_m\rangle$, where all $N_1, N_2, \ldots, N_m$ are nilpotent normal subloops of L. Since, all subloops are normal therefore we can express $Fit(L)$ alternatively as, $Fit(L) = N_1N_2 \cdots N_m$. This completes the proof. □

Theorem 3.12. *In an MC-loop the centralizer of any its non-empty subset is a subloop.*

Proof. The centralizer of X has the form $C_L(X) = \{a \in L : ax = xa \ , \forall\ x \in X\}$.
Let $a, b \in C_L(X)$ and $x \in X$,then

$$(ab)x = x(x^{-1}(ab.x)) = x(ab)^x = x(a^xb^x) = x(ab),$$

which implies $ab \in C_L(X)$. Now, for $b \in C_L(X)$ we have $bx = xb$. Thus, $b^{-1}xb = x$. Hence, $x = b(b^{-1}xb)b^{-1} = bxb^{-1}$, i.e., $b^{-1}x = xb^{-1}$. So, $b^{-1} \in C_L(X)$. □

Corollary 3.13. *The commutant $C(L)$ of an MC-loop L is its subloop.* □

Corollary 3.14. *Let L_1, L_2 be a subloop of a MC-loop L. If $L = L_1 \times L_2$, then $C(L) = C(L_1) \times C(L_2)$.* □

The following fact is obvious.

Proposition 3.15. *For an MC-loop L the map $\delta_x : L \to L$ defined by $(a)\delta_x = x^{-1}ax$ is its automorphism.* □

4. Relation of MC-loops with other loops

In this section we describe connections of MC-loops with other types of loops.
The following fact is well known but we give a short proof of this fact.

Theorem 4.1. *Every commutative IP-loop L is an MC-loop.*

Proof. Let L be an arbitrary commutative IP-loop. Then for all $x, x^{-1}, y \in L$ we have $x^{-1} \cdot yx = x^{-1} \cdot xy = x^{-1}x \cdot y = y$. On the other hand, $x^{-1}y \cdot x = yx^{-1} \cdot x = y \cdot x^{-1}x = y$. Hence, we get $x^{-1} \cdot yx = x^{-1}y \cdot x$. So, L is an IP-conjugate loop.

Moreover, $x^g y^g = (g^{-1}{\cdot}xg)(g^{-1}{\cdot}yg) = (g^{-1}{\cdot}gx)(g^{-1}{\cdot}gy) = (g^{-1}g{\cdot}x)(g^{-1}g{\cdot}y) = xy$ and $(xy)^g = g^{-1}.(xy)g = g^{-1}.g(xy) = (g^{-1}g)(xy) = xy$. So, $(xy)^g = x^g y^g$.

Hence, L is an MC-loop. □

Corollary 4.2. *Every Steiner loop, every commutative C-loop and every commutative Moufang loop are MC-loops but the converse is not true.* □

Example 4.3. The following loop

.	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	4	3	6	5	8	7	12	11	10	9
3	3	6	5	2	1	4	9	10	11	12	7	8
4	4	5	6	1	2	3	10	9	8	7	12	11
5	5	4	1	6	3	2	11	12	7	8	9	10
6	6	3	2	5	4	1	12	11	10	9	8	7
7	7	8	11	10	9	12	1	2	5	4	3	6
8	8	7	12	9	10	11	2	1	4	5	6	3
9	9	12	7	8	11	10	3	4	1	6	5	2
10	10	11	8	7	12	9	4	3	6	1	2	5
11	11	10	9	12	7	8	5	6	3	2	1	4
12	12	9	10	11	8	7	6	5	2	3	4	1

is a noncommutative Moufang loop which is not an MC-loop since $(xy)^g = x^g y^g$ is not true for $x = 2$, $y = 3$ and $g = 7$. □

Example 4.4. This is a non-commutative C-loop which is not an MC-loop.

.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	2	1	5	6	3	4	8	7	10	9	16	14	15	12	13	11
3	3	8	1	7	6	5	4	2	11	13	9	15	10	16	12	14
4	4	6	7	1	8	2	3	5	12	14	15	9	16	10	11	13
5	5	7	2	8	4	3	6	1	13	11	14	16	12	15	10	9
6	6	4	8	2	7	1	5	3	14	12	13	10	11	9	16	15
7	7	5	4	3	2	8	1	6	15	16	12	11	14	13	9	10
8	8	3	6	5	1	7	2	4	16	15	10	13	9	11	14	12
9	9	10	11	12	16	14	15	13	1	2	3	4	8	6	7	5
10	10	9	13	14	15	12	16	11	2	1	8	6	3	4	5	7
11	11	16	9	15	10	13	12	14	3	5	1	7	6	8	4	2
12	12	14	15	9	13	10	11	16	4	6	7	1	5	2	3	8
13	13	15	10	16	9	11	14	12	5	3	6	8	1	7	2	4
14	14	12	16	10	11	9	13	15	6	4	5	2	7	1	8	3
15	15	13	12	11	14	16	9	10	7	8	4	3	2	5	1	6
16	16	11	14	13	12	15	10	9	8	7	2	5	4	3	6	1

It is not an MC-loop because $(2.3)^9 \neq 2^9 3^9$. □

Example 4.5. Consider the following commutative loop.

$\cdot$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	1	4	3	6	5	8	7	10	9
3	3	4	1	2	7	9	5	10	6	8
4	4	3	2	1	10	8	9	6	7	5
5	5	6	7	10	1	2	3	9	8	4
6	6	5	9	8	2	1	10	4	3	7
7	7	8	5	9	3	10	1	2	4	6
8	8	7	10	6	9	4	2	1	5	3
9	9	10	6	7	8	3	4	5	1	2
10	10	9	8	5	4	7	6	3	2	1

It is a commutative MC-loop but not C-loop. □

Since in MC-loops the inverses are unique, we will use unique inverses instead of right or left inverses.

Theorem 4.6. *An MC-loop is a group iff it is conjugacy closed loop (CC loop).*

Proof. If L is a CC-loop, then

$$\begin{aligned} x(yz) &= (x \cdot yz)(x^{-1}x) = ((x \cdot yz)x^{-1})x = (yz)^{x^{-1}} \cdot x = (y^{x^{-1}} \cdot z^{x^{-1}})x \\ &= (y^{x^{-1}} \cdot x)(x^{-1}(z^{x^{-1}} \cdot x)) = (xyx^{-1} \cdot x)(x^{-1}(xzx^{-1} \cdot x)) = (xy)z. \end{aligned}$$

Hence, L is a group. The converse statement is obvious. □

Corollary 4.7. *An MC-loop is a group iff it is an extra loop.*

Proof. Since every extra loop is a conjugacy closed loop so the corollary follows from the last theorem. □

Theorem 4.8. *Every MC-loop is three power associative.*

Proof. Every MC-loop is conjugate IP-loop. Every conjugate IP loop is flexible. Flexible loops are always three power associative. Hence, MC-loop is three power associative. □

Example 4.9. This loop

$\cdot$	1	2	3	4	5
1	1	2	3	4	5
2	2	1	5	3	4
3	3	4	1	5	2
4	4	5	2	1	3
5	5	3	4	2	1

is three power associative but it is not an MC-loop. □

Example 4.10. Consider the following multiplicative conjugate loop.

$\cdot$	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	4	3	6	5	8	7	11	12	9	10
3	3	4	1	2	9	11	10	12	5	7	6	8
4	4	3	2	1	11	9	12	10	6	8	5	7
5	5	6	10	12	1	2	9	11	7	3	8	4
6	6	5	12	10	2	1	11	9	8	4	7	3
7	7	8	9	11	10	12	1	2	3	5	4	6
8	8	7	11	9	12	10	2	1	4	6	3	5
9	9	11	7	8	3	4	5	6	12	1	10	2
10	10	12	5	6	7	8	3	4	1	11	2	9
11	11	9	8	7	4	3	6	5	10	2	12	1
12	12	10	6	5	8	7	4	3	2	9	1	11

It is neither diassociative nor alternative loop. □

The above example shows that "Moufang theorem" is not always applicable in MC-loops. Indeed, in the above loop

$$11(6.12) = (11.6)12.$$

But the subloop $< 11, 6, 12 >$ is a loop which is not associative. From this, we can conclude that in MC-loops three elements associate with each other generata a subloop which is not a group, in general.

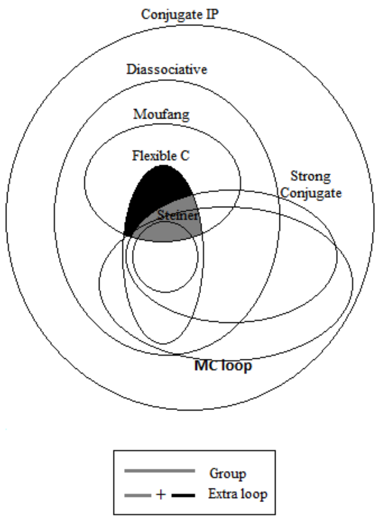
Example 4.11. This loop is a multiplicative conjugate loop but it is not power associative.

$\cdot$	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10
2	2	1	5	6	3	4	9	10	7	8
3	3	5	7	1	9	2	10	4	8	6
4	4	6	1	8	2	10	3	9	5	7
5	5	3	9	2	8	1	6	7	10	4
6	6	4	2	10	1	7	8	5	3	9
7	7	9	10	3	6	8	5	1	4	2
8	8	10	4	9	7	5	1	6	2	3
9	9	7	8	5	10	3	4	2	6	1
10	10	8	6	7	4	9	2	3	1	5

Indeed, the subloop $\langle 3 \rangle = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ is not associative. □

Power associative loops are not MC-loop because Moufang loops are power associative but not MC-loop.

The relationship of MC-loops with other loops is illustrated by the following diagram.



References

[1] **A. Batool, A. Shaheen and A. Ali**, *Conjugate loops: An Introduction*, Intern. Math. Forum **8** (2013), 223 – 228.

[2] **R. H. Bruck**, *Pseudo-automorphism and Moufang loops*, Proc. Amer. Math. Soc. **2** (1951), 66 – 71.

[3] **M. K. Kinyon and K. Kunen**, *The structure of extra loops*, Quasigroups and Related Systems **12** (2004), 39 – 60.

[4] **G. P. Nagay and P. Vojtechovsky**, LOOPS: *Computing with quasigroups and loops in GAP*, version 2.0.0 (2008), http://www.math.du.edu/loops.

[5] **J. D. Philips, P. Vojtechovsky**, *C-loops: An Introduction*, Pupl. Math. (Debrecen) **68** (2006), 115 – 137.

[6] **J. Slaney**, *FINDER, finite domain enumerator: System description*, Lecture Notes Computer Sci. **814** (1994), 798 – 801.

[7] **J. Slaney and A. Ali**, *IP loops of small orders*, (2007), http://users.rsise.anu.edu.au/~jks/IPloops/.

[8] **J. Slaney and A. Ali**, *Generating loops with the inverse property*, Proc. Empirically Successful Automated Reasoning in Math. **378** (2008), 55 – 66.

Received October 05, 2013

S. Ambreen
Quaid-e-Azam University, Pakistan
E-mail: shumaila.ambreen@ymail.com

A. Ali
Department of Mathematics and Natural Sciences, Prince Muhammad Bin Fahd University, POBox: 1664, Al Khobar 31952, Saudi Arabia
E-mail: dr_asif_ali@hotmail.com

Quasigroups and Related Systems **22** (2014), 9 − 18

$\mathsf{H}_v\mathsf{MV}$-algebras, I

Mahmood Bakhshi

Abstract. The aim of this paper is to introduce the concept of $\mathsf{H}_v\mathsf{MV}$-algebras as a common generalization of MV-algebras and hyper MV-algebras. After giving some basic properties and related results, the concepts of $\mathsf{H}_v\mathsf{MV}$-subalgebras, $\mathsf{H}_v\mathsf{MV}$-ideals and weak $\mathsf{H}_v\mathsf{MV}$-ideals are introduced and some of their properties and the connections between them are obtained.

1. Introduction

In 1958, Chang [1], introduced the concept of an MV-algebra as an algebraic proof of completeness theorem for $\aleph_0$-valued Łukasiewicz propositional calculus, see also [2]. Many mathematicians have worked on MV-algebras and obtained significant results. Mundici [6] proved that MV-algebras and abelian ℓ-groups with strong unit are categorically equivalent.

The hyperstructure theory (called also multialgebras) was introduced in 1934 by Marty [5]. Around the 40's, several authors worked on hypergroups, especially in France and in the United States, but also in Italy, Russia and Japan. Recently, Ghorbani et al. [4] applied the hyperstructures to MV-algebras and introduced the concept of hyper MV-algebras. Now hyperstructures have many applications to several sectors of both pure and applied sciences such as: geometry, hypergraphs, binary relations, lattices, fuzzy set and rough sets, automata, cryptography, combinatorics, codes, artificial intelligence and probabilities.

H_v-structures were introduced by Vougiouklis in [7] as a generalization of the well-known algebraic hyperstructures (hypergroup, hyperring, hypermodule and so on). The reader will find in [8] some basic definitions and theorems about H_v-structures. A survey of some basic definitions, results and applications one can find in [3] and [8].

In this paper, in order to obtain a suitable generalization of MV-algebras and hyper MV-algebras which may be equivalent (categorically) to a certain subclass of the class of H_v-groups, the concept of $\mathsf{H}_v\mathsf{MV}$-algebra is introduced and some related results are obtained. In particular, weak $\mathsf{H}_v\mathsf{MV}$-ideals generated by a subset are characterized.

2010 Mathematics Subject Classification: 03B50, 06D35.
Keywords: MV-algebra, $\mathsf{H}_v\mathsf{MV}$-algebra, $\mathsf{H}_v\mathsf{MV}$-ideal.

2. Preliminaries

In this section we present some basic definitions and results.

Definition 2.1. An MV-*algebra* is an algebra $(M; +,^*, 0)$ of type (2,1,0) satisfying the following axioms:
(MV1) $+$ is associative,
(MV2) $+$ is commutative,
(MV3) $x + 0 = x$,
(MV4) $(x^*)^* = x$,
(MV5) $x + 0^* = 0^*$,
(MV6) $(x^* + y)^* + y = (y^* + x)^* + x$.

On any MV-algebra M we can defina a partial ordering $\leqslant$ by putting $x \leqslant y$ if and only if $x^* + y = 0^*$.

Definition 2.2. A *hyper* MV- *algebra* is a nonempty set H endowed with a binary hyperoperation '$\oplus$', a unary operation '*' and a constant '0' satisfying the following conditions: $\forall x, y, z \in M$,
(HMV1) $x \oplus (y \oplus z) = (x \oplus y) \oplus z$,
(HMV2) $x \oplus y = y \oplus x$,
(HMV3) $(x^*)^* = x$,
(HMV4) $(x^* \oplus y)^* \oplus y = (y^* \oplus x)^* \oplus x$,
(HMV5) $0^* \in x \oplus 0^*$,
(HMV6) $0^* \in x \oplus x^*$,
(HMV7) $x \ll y$ and $y \ll x$ imply $x = y$, where $x \ll y$ is defined as $0^* \in x^* \oplus y$.

For $A, B \subseteq H$, $A \ll B$ is defined as $a \ll b$ for some $a \in A$ and $b \in B$.

Proposition 2.3. *In any hyper* MV-*algebra H for all $x, y \in H$ we have*
1. $0 \ll x \ll 0^*$,
2. $x \ll x$,
3. $x \ll y$ *implies that* $y^* \ll x^*$,
4. $x \ll x \oplus y$,
5. $0 \oplus 0 = \{0\}$,
6. $x \in x \oplus 0$.

Definition 2.4. A nonempty subset I of hyper MV-algebra H is called a

- *hyper* MV-*ideal* if

  (I_0) $x \ll y$ and $y \in I$ imply $x \in I$,

  (I_1) $x \oplus y \subseteq I$ for all $x, y \in I$,

- *weak hyper* MV-*ideal* if (I_0) holds and

  (I_2) $x \oplus y \ll I$ for all $x, y \in I$.

Obviously, every hyper MV-ideal is a weak hyper MV-ideal.

3. $\mathsf{H}_v\mathsf{MV}$-algebras

Definition 3.1. An $\mathsf{H}_v\mathsf{MV}$-*algebra* is a nonempty set H endowed with a binary hyperoperation '$\oplus$', a unary operation '*' and a constant '0' satisfying the following conditions:

($\mathsf{H}_v\mathsf{MV}1$) $x \oplus (y \oplus z) \cap (x \oplus y) \oplus z \neq \emptyset$, (weak associativity)
($\mathsf{H}_v\mathsf{MV}2$) $x \oplus y \cap y \oplus x \neq \emptyset$, (weak commutativity)
($\mathsf{H}_v\mathsf{MV}3$) $(x^*)^* = x$,
($\mathsf{H}_v\mathsf{MV}4$) $(x^* \oplus y)^* \oplus y \cap (y^* \oplus x)^* \oplus x \neq \emptyset$,
($\mathsf{H}_v\mathsf{MV}5$) $0^* \in x \oplus 0^* \cap 0^* \oplus x$,
($\mathsf{H}_v\mathsf{MV}6$) $0^* \in x \oplus x^* \cap x^* \oplus x$,
($\mathsf{H}_v\mathsf{MV}7$) $x \in x \oplus 0 \cap 0 \oplus x$,
($\mathsf{H}_v\mathsf{MV}8$) $0^* \in x^* \oplus y \cap y \oplus x^*$ and $0^* \in y^* \oplus x \cap x \oplus y^*$ imply $x = y$.

Remark 3.2. On any $\mathsf{H}_v\mathsf{MV}$-algebra H, we can define a binary relation '$\preceq$' by

$$x \preceq y \;\Leftrightarrow\; 0^* \in x^* \oplus y \cap y \oplus x^*.$$

Hence, the condition ($\mathsf{H}_v\mathsf{MV}8$) can be redefined as follows:

$$x \preceq y \text{ and } y \preceq x \text{ imply } x = y.$$

Let A and B be nonempty subsets of H. By $A \preceq B$ we mean that there exist $a \in A$ and $b \in B$ such that $a \preceq b$. For $A \subseteq H$, we denote the set $\{a^* : a \in A\}$ by A^*, and 0^* by 1.

Obviously, every hyper MV-algebra is an $\mathsf{H}_v\mathsf{MV}$-algebra but the converse is not true. We say $\mathsf{H}_v\mathsf{MV}$-algebra H is *proper* if it is not a hyper MV-algebra.

Example 3.3. Let $H = \{0, a, 1\}$ and the operations $\oplus$ and * be defined as follows:

$\oplus$	0	a	1
0	{0}	{a}	{0,a,1}
a	{0,a}	{1}	{0,1}
1	{0,1}	{0,a,1}	{0,a,1}
$*$	1	a	0

Then $(H; \oplus, ^*, 0)$ is a proper $\mathsf{H}_v\mathsf{MV}$-algebra. □

Example 3.4. Similarly, $H = \{0, a, b, 1\}$ with the operations $\oplus$ and * defined by

$\oplus$	0	a	b	1
0	{0,a}	{0,a,b}	{0,a,b}	{0,a,b,1}
a	{0,a,b,1}	{0,b}	{0,1}	{a,b,1}
b	{a,b}	{0,a,b,1}	{0}	{0,a,b,1}
1	{0,a,1}	{0,a,b,1}	{1}	{0,a,b,1}
$*$	1	b	a	0

is a proper $\mathsf{H}_v\mathsf{MV}$-algebra. □

Proposition 3.5. *In any* $\mathsf{H}_v\mathsf{MV}$*-algebra* H *for* $x, y \in H$ *and* $A, B \subseteq H$ *the following hold:*

1. $x \preceq x$, $A \preceq A$,
2. $0 \preceq x \preceq 1$, $0 \preceq A \preceq 1$,
3. $x \preceq y$ *implies* $y^* \preceq x^*$,
4. $A \preceq B$ *implies* $B^* \preceq A^*$,
5. $A \preceq B$ *implies that* $0^* \in (A^* \oplus B) \cap (B \oplus A^*)$,
6. $(x^*)^* = x$ *and* $(A^*)^* = A$,
7. $0^* \in (A \oplus A^*) \cap (A^* \oplus A)$,
8. $A \cap B \neq \emptyset$ *implies that* $A \preceq B$,
9. $(A \cap B)^* = A^* \cap B^*$,
10. $(A \oplus B) \cap (B \oplus A) \neq \emptyset$,
11. $A \oplus (B \oplus C) \cap (A \oplus B) \oplus C \neq \emptyset$,
12. $(A^* \oplus B)^* \oplus B \cap (B^* \oplus A)^* \oplus A \neq \emptyset$. □

The following example shows that the relation $\preceq$ is not transitive.

Example 3.6. In the $\mathsf{H}_v\mathsf{MV}$-algebra $(H; \oplus, ^*, 0)$, where $H = \{0, a, b, c, 1\}$ and the operations are defined by

$\oplus$	0	a	b	c	1
0	{0}	{0,a}	{0,b}	{0,c}	{0,a,b,c,1}
a	{0,a}	{0,a}	{0,a,b,c,1}	{0,a,b,c,1}	{0,a,b,c,1}
b	{0,b}	{0,a,b,c,1}	{0,a,b,c,1}	{0,a,b,c}	{0,a,b,c,1}
c	{0,c}	{0,a,b,c,1}	{0,a,b,c}	{0,a,b,c,1}	{0,a,b,c,1}
1	{0,a,b,c,1}	{0,a,b,c,1}	{0,a,b,c,1}	{0,a,b,c,1}	{0,a,b,c,1}
$*$	1	b	a	c	0

we have $a \preceq b$ and $b \preceq c$ while $a \not\preceq c$, because $0^* \notin \{0, a, b, c\} = a^* \oplus c$. □

Now let $x \odot y = (x^* \oplus y^*)^*$.

Theorem 3.7. *In any* $\mathsf{H}_v\mathsf{MV}$*-algebra* H *for all* $x, y, z \in H$ *and all nonempty subsets* A *and* B *of* H *we have:*

(1) $x \odot (y \odot z) \cap (x \odot y) \odot z \neq \emptyset$,

(2) $x \odot y \cap y \odot x \neq \emptyset$,

(3) $0 \in x \odot 0 \cap 0 \odot x$,

(4) $0 \in x \odot x^* \cap x^* \odot x$,

(5) $x \in x \odot 1 \cap 1 \odot x$,

(6) $1 \in x \odot y^* \cap y^* \odot x$ *and* $1 \in y \odot x^* \cap x^* \odot y$ *imply* $x = y$,

(7) $(A \oplus B)^* = A^* \odot B^*$,

(8) $(A \odot B)^* = A^* \oplus B^*$,

(9) $x \in x \oplus x$ *if and only if* $x^* \in x^* \odot x^*$,

(10) $x \in x \odot x$ *if and only if* $x^* \in x^* \oplus x^*$.

Proof. It is enough to observe that for $x, y, z \in H$,

$$\begin{aligned} x \odot (y \odot z) &= \bigcup\{x \odot t : t \in (y^* \oplus z^*)^*\} \\ &= \bigcup\{(x^* \oplus t^*)^* : t \in (y^* \oplus z^*)^*\} \\ &= \bigcup\{(x^* \oplus t^*)^* : t^* \in y^* \oplus z^*\} \\ &= \bigcup\{a^* : a \in x^* \oplus t^* : t^* \in y^* \oplus z^*\} \\ &= \bigcup\{a^* : a \in x^* \oplus (y^* \oplus z^*)\} \end{aligned}$$

and similarly

$$(x \odot y) \odot z = \bigcup\{a^* : a \in (x^* \oplus y^*) \oplus z^*\}.$$

This proves (1).

The proofs of $(2) - (6)$ follow from ($\mathsf{H}_v\mathsf{MV2}$) and ($\mathsf{H}_v\mathsf{MV5}$)-($\mathsf{H}_v\mathsf{MV7}$). The proofs of $(7) - (10)$ follow from the definition. □

On H we also define two binary hyperoperations '$\vee$' and '$\wedge$' as

$$x \vee y = (x \odot y^*) \oplus y, \qquad x \wedge y = (x \oplus y^*) \odot y = (x^* \vee y^*)^*.$$

Theorem 3.8. *In any $\mathsf{H}_v\mathsf{MV}$-algebra H, the following hold:*

(1) $(x \wedge y)^* = x^* \vee y^*$, $(x \vee y)^* = x^* \wedge y^*$,

(2) $(x \vee y) \cap (y \vee x) \neq \emptyset$, $(x \wedge y) \cap (y \wedge x) \neq \emptyset$,

(3) $x \in (x \vee x) \cap (x \wedge x)$,

(4) $0 \in (x \wedge 0) \cap (0 \wedge x)$,

(5) $1 \in (x \vee 1) \cap (1 \vee x)$,

(6) $x \in (x \vee 0) \cap (0 \vee x)$,

(7) $x \in (x \wedge 1) \cap (1 \wedge x)$,

(8) $x \preceq y$ *implies* $y \in x \vee y$ *and* $x \in x \wedge y$,

(9) $x \in y \odot x$ *implies* $1 \in y \vee x^*$,

(10) $x \in y \oplus x$ *implies* $0 \in y \wedge x^*$,

(11) *If* $x \in x \oplus x$, *then* $0 \in x \wedge x^*$,

(12) *If* $x \in x \odot x$, *then* $1 \in x \vee x^*$.

Proof. (1). Let $x, y \in H$. Then,

$$x^* \vee y^* = (x^* \odot y) \oplus y^* = (x \oplus y^*)^* \oplus y^* = ((x \oplus y^*) \odot y)^* = (x \wedge y)^*.$$

Similarly, the second equality is proved.

(2). It follows from ($\mathsf{H}_v\mathsf{MV4}$).

(3). From $0 \in x \odot x^*$ it follows that $x \in 0 \oplus x \subseteq (x \odot x^*) \oplus x = x \vee x$. From $0^* \in x \oplus x^*$ it follows that

$$x = (x^*)^* \in (0 \oplus x^*)^* \subseteq ((x \oplus x^*)^* \oplus x^*)^* = (x \oplus x^*) \odot x = x \wedge x.$$

(4). From $1 = 0^* \in x \oplus 0^*$ it follows that $0 \in 1 \odot 0 \subseteq (x \oplus 0^*) \odot 0 = x \wedge 0$. Similarly, from $x^* \in 0 \oplus x^*$ it follows that $0 \in x^* \odot x \subseteq (0 \oplus x^*) \odot x = 0 \wedge x$. Thus, $0 \in (x \wedge 0) \cap (0 \wedge x)$.

(9). If $x \in y \odot x$, then $1 = 0^* \in x \oplus x^* \subseteq (y \odot x) \oplus x^* = y \vee x^*$.

(10). If $x \in y \oplus x$, then $0 \in x \odot x^* \subseteq (y \oplus x) \odot x^* = y \wedge x^*$.

The proofs of the other cases are easy. □

Proposition 3.9. *Let $x \in H$. Then*

(1) $0 \in x \wedge x^*$ *if and only if* $x \oplus x \preceq x$ *if and only if* $x^* \preceq x^* \odot x^*$,

(2) $1 \in x \vee x^*$ *if and only if* $x^* \oplus x^* \preceq x^*$ *if and only if* $x \preceq x \odot x$. □

4. Homomorphisms, subalgebras and $\mathsf{H}_v\mathsf{MV}$-ideals

In this section, homomorphisms, $\mathsf{H}_v\mathsf{MV}$-subalgebras, weak $\mathsf{H}_v\mathsf{MV}$-ideals and $\mathsf{H}_v\mathsf{MV}$-ideals are introduced and some their properties are obtained.

Definition 4.1. Let $(H; \oplus, ^*, 0_H)$ and $(K; \otimes, ^\star, 0_K)$ be $\mathsf{H}_v\mathsf{MV}$-algebras and let $f : H \longrightarrow K$ be a function satisfying the following conditions:

(1) $f(0_H) = 0_K$,

(2) $f(x^*) = f(x)^\star$,

(3) $f(x^*) \preceq f(x)^\star$,

(4) $f(x \oplus y) = f(x) \otimes f(y)$,

(5) $f(x \oplus y) \subseteq f(x) \otimes f(y)$.

f is called a *homomorphism* if it satisfies (1), (2) and (4), and it is called a *weak homomorphism* if it satisfies (1), (3) and (5). Clearly, $f(1) = 1$ if f is a homomorphism. Note that (1) is not a consequence of (2) and (4).

Example 4.2. The set $H = \{0, a, 1\}$ with the operations defined by the table

$\oplus$	0	a	1
0	{0}	{0,a}	{0,1}
a	{0,a}	{0,a,1}	{a,1}
1	{0,1}	{a,1}	{1}
$*$	1	a	0

is an $\mathsf{H}_v\mathsf{MV}$-algebra. The function $f : H \longrightarrow H$ such that $f(0) = 1$, $f(1) = 0$ and $f(a) = a$ satisfies (2) and (4) but not (1). □

Further, for simplicity, we will use the same symbols for operations in H and K.

Theorem 4.3. *Let $f : H \longrightarrow K$ be a homomorphism.*

(1) *f is one-to-one if and only if $kerf = \{0\}$.*

(2) *f is an isomorphism if and only if there exists a homomorphism f^{-1} from K onto H such that $ff^{-1} = 1_K$ and $f^{-1}f = 1_H$.*

Proof. We prove only (1). Assume that f is one-to-one and $x \in kerf$. Then, $f(x) = 0 = f(0)$ whence $x = 0$, i.e., $kerf = \{0\}$. Conversely, assume that $kerf = \{0\}$ and $f(x) = f(y)$, for $x, y \in H$. Then,

$$0^* \in f(x)^* \oplus f(y) \cap f(y) \oplus f(x)^* = f(x^* \oplus y) \cap f(y \oplus x^*)$$

whence $f(s) = 0^* = f(t)$, for some $t \in x^* \oplus y$ and $s \in y \oplus x^*$. Hence, $f(s^*) = f(t^*) = 0$, i.e., $s^*, t^* \in kerf = \{0\}$ and so $0^* = s \in y \oplus x^*$ and $0^* = t \in x^* \oplus y$ whence $x \preceq y$. Similarly, we can show that $y \preceq x$. Thus, $x = y$, i.e., f is one-to-one. □

Proposition 4.4. *A nonempty subset S of H is an $\mathsf{H}_v\mathsf{MV}$-subalgebra of H if and only if $0 \in S$ and $x^* \oplus y \subseteq S$ for all $x, y \in S$.* □

Definition 4.5. A nonempty subset I of H such that $x \preceq y$ and $y \in I$ imply $x \in I$ is called

an $\mathsf{H}_v\mathsf{MV}$-*ideal* if $x \oplus y \subseteq I$, for all $x, y \in I$, and

a *weak* $\mathsf{H}_v\mathsf{MV}$-*ideal* if $x \oplus y \preceq I$, for all $x, y \in I$.

From Proposition 3.5 (8) it follows that every $\mathsf{H}_v\mathsf{MV}$-ideal is a weak $\mathsf{H}_v\mathsf{MV}$-ideal.

Theorem 4.6. *A nonempty subset I of H is a weak $\mathsf{H}_v\mathsf{MV}$-ideal if and only if $x \preceq y$ and $y \in I$ imply $x \in I$ and for all $x, y \in I$ we have $(x \oplus y) \cap I \neq \emptyset$.* □

Theorem 4.7. *If I is an $\mathsf{H}_v\mathsf{MV}$-ideal of an $\mathsf{H}_v\mathsf{MV}$-algebra H in which $x \preceq x \vee y$ holds for all $x, y \in H$, then $0 \in I$, and $a \odot b^* \subseteq I$ together with $b \in I$ imply $a \in I$.*

Proof. If I is an $\mathsf{H}_v\mathsf{MV}$-idealm then obviously, $0 \in I$. Now, let $a \odot b^* \subseteq I$ and $b \in I$. Then, $a \preceq a \vee b = (a \odot b^*) \oplus b \subseteq I$, whence $a \in I$. □

Definition 4.8. A nonempty subset A of H is called $S_\odot$-*reflexive* if $x \odot y \cap A \neq \emptyset$ implies that $x \odot y \subseteq A$. Similarly, A is called $S_\oplus$-reflexive if $x \oplus y \cap A \neq \emptyset$ implies that $x \oplus y \subseteq A$.

Theorem 4.9. *If in an $\mathsf{H}_v\mathsf{MV}$-algebra H for all $x, y \in H$ we have $x \wedge y \preceq x \preceq x \vee y$, then each its $S_\odot$-reflexive and $S_\oplus$-reflexive subset is an $\mathsf{H}_v\mathsf{MV}$-ideal of H.*

Proof. Let $x, y \in H$ be such that $x \preceq y$ and $y \in I$. Then, $0^* \in x^* \oplus y$ and so $0 \in x \odot y^*$, whence $(x \odot y^*) \cap I \neq \emptyset$. Since, I is $S_\odot$-reflexive, $x \odot y^* \subseteq I$ and so $x \in I$. Thus, $x \preceq y$ and $y \in I$ imply $x \in I$. Now, let $x, y \in I$. Then, $(x \oplus y) \odot y^* = x \wedge y^* \preceq x$ and hence, $c \preceq x \in I$, where $c \in x \wedge y^*$. This implies that $c \in I$ and so $(x \oplus y) \odot y^* \cap I \neq \emptyset$. Hence, there exists $a \in x \oplus y$ such that $a \odot y^* \cap I \neq \emptyset$ combining $y \in I$ we get $a \in I$, i.e., $x \oplus y \cap I \neq \emptyset$, whence $x \oplus y \subseteq I$. Thus, I is an $\mathsf{H}_v\mathsf{MV}$-ideal of H. □

Corollary 4.10. *In a hyper* MV*-algebra, every* $S_\odot$*-reflexive and* $S_\oplus$*-reflexive subset* I *that* $x \preceq y$ *and* $y \in I$ *imply* $x \in I$ *is a hyper* MV*-ideal.* □

Theorem 4.11. *Let* $f : H \longrightarrow K$ *be a homomorphism. Then*

(1) $ker f$ *is a weak* $\mathsf{H}_v\mathsf{MV}$*-ideal of* H*.*

(2) *If* I *is an* $\mathsf{H}_v\mathsf{MV}$*-ideal of* K*,* $f^{-1}(I)$ *is an* $\mathsf{H}_v\mathsf{MV}$*-ideal of* H*.*

(3) *Assume that* $x \preceq x \vee y$ *holds for all* $x, y \in H$*. If* f *is onto and* I *is an* $S_\odot$*–reflexive* $\mathsf{H}_v\mathsf{MV}$*-ideal of* H *containing* $ker\, f$*, then* $f(I)$ *is an* $\mathsf{H}_v\mathsf{MV}$*-ideal of* K*.*

Proof. (1). Let $x, y \in H$ be such that $x \preceq y$ and $y \in ker f$. Then, $0^* \in (x^* \oplus y) \cap (y \oplus x^*)$ and $f(y) = 0$. Thus

$$0^* = f(0^*) \in f(x^* \oplus y) \cap f(y \oplus x^*) = f(x)^* \oplus 0 \cap 0 \oplus f(x)^*,$$

which implies that $f(x) \preceq 0$. Hence, $f(x) = 0$, i.e., $x \in ker f$.

Now, let $x, y \in ker f$. Then, $0 \in 0 \oplus 0 = f(x) \oplus f(y) = f(x \oplus y)$ and so $f(t) = 0$, for some $t \in x \oplus y$. This implies that $(x \oplus y) \cap ker f \neq \emptyset$ and so by Theorem 4.6, $ker f$ is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H.

(2) It is easy.

(3) Assume that f is onto and I is an $\mathsf{H}_v\mathsf{MV}$-ideal of H. Let $x \preceq y$ and $y \in f(I)$. Then, $0^* \in x^* \oplus y \cap y \oplus x^*$ and $y = f(b)$, for some $b \in I$. Since, f is onto, there exists $a \in H$ such that $f(a) = x$. Hence,

$$0^* \in f(a^*) \oplus f(b) \cap f(b) \oplus f(a^*) = f(a^* \oplus b) \cap f(b \oplus a^*),$$

whence $f(u) = 0^* = f(v)$, for some $u \in a^* \oplus b$ and $v \in b \oplus a^*$. This implies that $u^*, v^* \in ker f \subseteq I$, i.e., $a \odot b^* \cap I \neq \emptyset$, whence $a \odot b^* \subseteq I$. Since, $b \in I$, so $a \in I$ and hence, $x = f(a) \in f(I)$.

Let now $x, y \in f(I)$. Then, there exist $a, b \in I$ such that $f(a) = x$ and $f(b) = y$. From $a \oplus b \subseteq I$ it follows that $x \oplus y \subseteq f(I)$, proving $f(I)$ is an $\mathsf{H}_v\mathsf{MV}$-ideal of K. □

Definition 4.12. Let A be a nonempty subset of H. The smallest (weak) $\mathsf{H}_v\mathsf{MV}$-ideal of H containing A is called the (weak)$\mathsf{H}_v\mathsf{MV}$-*ideal generated* by A and is denoted by $\langle A \rangle$ (by $\langle A \rangle_w$ respectively).

It is clear that

$$\langle A\rangle \supseteq \{x\in H : x \preceq (\cdots((a_1\oplus a_2)\oplus\cdots)\oplus a_n,\ \text{for some } n\in\mathbb{N}, a_1,\dots,a_n\in A\}.$$

Theorem 4.13. *Assume that $|x\oplus y|<\infty$, for all $x,y\in H$, $\preceq$ is transitive and monotone, and $x\oplus y\in R(H)=\{a\in H : |z\oplus a|=1\ \forall z\in H\}$ for all $x,y\in R(H)$. Then*

$$\langle A\rangle_w = \{x\in H : x\preceq(\cdots((a_1\oplus a_2)\oplus\cdots)\oplus a_n,\ \textit{for some } n\in\mathbb{N}, a_1,\dots,a_n\in A\}$$

for any nonempty subset A of H contained in $R(H)$.

Proof. Assume that

$$B=\{x\in H : x\preceq(\cdots((a_1\oplus a_2)\oplus\cdots)\oplus a_n,\ \text{for some } n\in\mathbb{N}, a_1,\dots,a_n\in A\}.$$

Obviously, $A\subseteq B$. Now, let $x,y\in H$ be such that $x\preceq y$ and $y\in B$. Since, $|x\oplus y|<\infty$, so $y\preceq(\cdots((a_1\oplus a_2)\oplus\cdots)\oplus a_n$ for some $n\in\mathbb{N}$ and $a_1,a_2,\dots,a_n\in A$. This implies that $0^*\in y^*\oplus((\cdots((a_1\oplus a_2)\oplus\cdots)\oplus a_n)$. On the other hand, $x\preceq y$ implies that $y^*\preceq x^*$, whence

$$0^*\in\{0^*\}=y^*\oplus(\cdots((a_1\oplus a_2)\oplus\cdots)\oplus a_n)\preceq x^*\oplus(\cdots((a_1\oplus a_2)\oplus\cdots)\oplus a_n),$$

which gives $0^*\in x^*\oplus(\cdots((a_1\oplus a_2)\oplus\cdots)\oplus a_n)$, i.e., $x\preceq(\cdots((a_1\oplus a_2)\oplus\cdots)\oplus a_n)$. Thus, $x\in B$.

Now, let $x,y\in B$. Then,

$$x\preceq(\cdots(a_1\oplus a_2)\oplus\cdots)\oplus a_n \quad\text{and}\quad y\preceq(\cdots(b_1\oplus b_2)\oplus\cdots)\oplus b_m$$

for some $n,m\in\mathbb{N}$, $a_1,\dots,a_n,b_1,\dots,b_m\in A$. Since, $\preceq$ is monotone,

$$\begin{aligned} x\oplus y &\preceq x\oplus((\cdots(b_1\oplus b_2)\oplus\cdots)\oplus b_m)\\ &\preceq ((\cdots(a_1\oplus a_2)\oplus\cdots)\oplus a_n)\oplus((\cdots(b_1\oplus b_2)\oplus\cdots)\oplus b_m)\end{aligned}$$

and hence there exists $u\in x\oplus y$ such that

$$\begin{aligned} u &\preceq x\oplus((\cdots(a_1\oplus a_2)\oplus\cdots)\oplus a_n)\\ &\preceq ((\cdots(a_1\oplus a_2)\oplus\cdots)\oplus a_n)\oplus((\cdots(b_1\oplus b_2)\oplus\cdots)\oplus b_m)\\ &= (\cdots(((\cdots(a_1\oplus a_2)\oplus\cdots)\oplus a_n)\oplus b_1)\oplus\cdots)\oplus b_m\end{aligned}$$

because $\preceq$ is transitive. The equality holds for $A\cap B\neq\emptyset$, and $|A|=1=|B|$ imply $A=B$. Thus $u\in B$ and so $x\oplus y\preceq B$. Therefore, B is a weak $\mathsf{H}_v\mathsf{MV}$-ideal of H. Obviously, B is the least weak $\mathsf{H}_v\mathsf{MV}$-ideal of H containing A. □

Let $\mathsf{H}_v\mathsf{MVI}$ ($\mathsf{WH}_v\mathsf{MVI}$) denotes the set of all $\mathsf{H}_v\mathsf{MV}$-ideals (weak $\mathsf{H}_v\mathsf{MV}$-ideals) of H. Then, $\mathsf{H}_v\mathsf{MVI}$ ($\mathsf{WH}_v\mathsf{MVI}$) together with the set inclusion, as a partial ordering, is a poset in which for all $A_i\subseteq\mathsf{H}_v\mathsf{MVI}$, $\bigwedge A_i=\bigcap A_i$ and $\bigvee A_i=\langle A_i\rangle$. So, we have

Theorem 4.14. ($\mathsf{H}_v\mathsf{MVI}$,$\subseteq$) *is a complete lattice, and if* $\mathsf{WH}_v\mathsf{MVI}$ *is closed with respect to the intersection,* $\mathsf{H}_v\mathsf{MVI}$ *is a complete sublattice of the complete lattice* ($\mathsf{WH}_v\mathsf{MVI}$,$\subseteq$). □

References

[1] **C. C. Chang**, *Algebraic analysis of many valued logics*, Trans. Amer. Math. Soc. **88** (1958), 467 – 490.

[2] **C. C. Chang**, *A new proof of the completeness of the Lukasiewicz axioms*, Trans. Amer. Math. Soc. **93** (1959), 74 – 80.

[3] **B. Davvaz**, *A brief survey of the theory of H_v-structures*, Proc. 8th International Congress on Algebraic Hyperstructures and Appl., Spanidis Press, (2003), 39 – 70.

[4] **Sh. Ghorbani, A. Hassankhani, E. Eslami**, *Hyper MV-algebras*, Set-Valued Math. Appl. **1** (2008), 205 – 222.

[5] **F. Marty**, *Sur une generalization de la notion de groups*, 8th Congress Math. Scandinaves, Stockhholm, (1934), 45 – 49.

[6] **D. Mundici**, *Interpretation of AFC^*-algebras in Łukasiewicz sentential calsulus*, J. Func. Anal. **65** (1986), 15 – 63.

[7] **T. Vougiouklis**, *The fundamental relation in hyperrings. The general hyperfield*, Proc. of the 4th Int. Congress on Algebraic Hyperstructures and Appl., World Sientific, (1991), 203 – 211.

[8] **T. Vougiouklis**, *Hyperstructures and Their Representations*, Hadronic Press, 1994.

Received December, 19, 2013

Department of Mathematics, Univesity of Bojnord, Bojnord, Iran
E-mail: bakhshi@ub.ac.ir

Quasigroups and Related Systems **22** (2014), 19 − 32

Parastrophically equivalent identities characterizing quasigroups isotopic to abelian groups

Galina B. Belyavskaya

Abstract. We study parastrophic equivalence of identities in primitive quasigroups and parastrophically equivalent balanced and near-balanced identities characterizing quasigroups isotopic to groups (to abelian groups). Some identities in quasigroups with 0-ary operation characterizing quasigroups isotopic to abelian groups are given.

1. Introduction

Quasigroups isotopic to groups, to abelian groups consist important classes of quasigroups. They arise under investigation of different classes and systems of quasigroups and are used in distinct applications. Medial quasigroups, linear quasigroups and T-quasigroups are the most known classes of these quasigroups. Quasigroups isotopic to groups (to abelian groups), their subclasses and identities reducing to them were investigated by many authors. Recall some of the known results.

In [1] and [3] these quasigroups arose under the research of balanced identities, including arbitrary number of variables, and under the study of four quasigroups connected by the law of general associativity. As it was proved, these four quasigroups are isotopic to the same group.

In [3], V. D. Belousov found a balanced identity of five (of four) variables in a primitive quasigroup $(Q, \cdot, \backslash, /)$ that characterizes quasigroups isotopic to groups (to abelian groups).

As M. M. Glukhov informed, he proved that among of the identities characterizing the variety of quasigroups isotopic to abelian groups there not exist balanced identities of three variables and listed six balanced identities of four variables obtained by different authors (see section 5).

In [6], [7] and [9], some identities with permutations of three variables that characterize quasigroups isotopic to groups (to abelian groups) were considered. In

2010 Mathematics Subject Classification: 20N05
Keywords: quasigroup, primitive quasigroup, loop, abelian group, parastrophe, balanced (near-balanced) identity

[7], the type of these identities was defined and some identities with permutations characterizing quasigroups isotopic to abelian groups were given.

In the article we continue this research, consider parastrophic equivalence of identities in primitive quasigroups and parastrophically equivalent balanced and near-balanced identities characterizing quasigroups isotopic to groups (to abelian groups). Some unbalanced identities of Theorem 1.2.1a of [7] are simplified and some identities in quasigroups with 0-ary operation characterizing quasigroups isotopic to abelian groups are given.

2. Preliminaries

Let $(Q,\cdot)$ be a quasigroup. The operation $(\backslash)$, or $(\cdot)^{-1}$ ($(/)$ or ${}^{-1}(\cdot)$):

$$x\backslash y = z \Leftrightarrow xz = y \quad (x/y = z \Leftrightarrow zy = x)$$

is called *the right* (*left*) *inverse operation for the operation* $(\cdot)$, and the quasigroup $(Q,\backslash)$ ($(Q,/)$) is called *the right* (*left*) *inverse quasigroup* for the quasigroup $(Q,\cdot)$. In addition,

$$x\backslash y = L_x^{-1}y, \quad x/y = R_y^{-1}x,$$

where $L_x y = x\cdot y = R_y x$.

If a quasigroup operation is denoted by A, then its right (left) inverse operation is denoted by A^{-1} (respectively, by ${}^{-1}A$).

The primitive quasigroup [4] $(Q,\cdot,\backslash,/)$, e.i., the algebra with three operations satisfying to the following four identities:

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

corresponds to every quasigroup $(Q,\cdot)$.

We also shall use *primitive quasigroups* $(Q,\cdot,\backslash,/,a)$ *with one 0-operation* c_a: $\{\emptyset\}\to a$, where a is some fixed element of the set Q.

It is known that every quasigroup operation A has the following six parastrophic operations (conjugates or parastrophes):

$$A = (\cdot),\ A^{-1} = (\backslash), {}^{-1}A = (/),\ {}^{-1}(A^{-1}) = (\otimes_1),\ ({}^{-1}A)^{-1} = (\otimes_2),\ A^* = (\cdot)^*,$$

where $A^*(x,y) = A(y,x)$ [4], moreover, $x\otimes_1 y = y/x,\ x\otimes_2 y = y\backslash x$.

If a quasigroup $(Q,\cdot)$ is isotopic to a group, then every its parastrophe is also isotopic to the same group (see, for example, [7] and [12]).

3. Equivalent identities in primitive quasigroups

For the first time the concept of conjugate or parastrophic identities (in a quasigroup $(Q,\cdot)$) was introduced by A. Sade in [11]. He also gave a number of rules for simplifying of identities in $(Q,\cdot)$ that involves more than one of parastrophic operations. V.D. Belousov in [2] listed the parastrophic identities in a quasigroup $(Q,\cdot)$ for a number of the well-known identities. Part of these identities was earlier given by S.K. Stein in [13]. In [5], V.D. Belousov considered parastrophic equivalence of the minimal identities in a quasigroup $(Q,\cdot)$ connected with orthogonality. Below we shall consider parastrophic equivalence of identities in primitive quasigroups.

Let a primitive quasigroup $(Q,\cdot,\backslash,/)$ satisfy an identity. Changing the operation $(\cdot)$ for some its parastrophe σ in this identity, we shall obtain an identity, which holds in a primitive quasigroup with another triple of operations. For example, using the change $(\cdot)\to(/)$, we shall get an identity in the quasigroup $(Q,/,\otimes_2,\cdot)$, since in this case $(\backslash)\to(/)^{-1}=(\otimes_2)$, $(/)\to^{-1}(/)=(\cdot)$, $\otimes_1\to(*)$, $(\otimes_2)\to(\backslash)$, $(*)\to(\otimes_1)$ (see Tab. 1 below). But

$$x\otimes_1 y=y/x,\;\; x\otimes_2 y=y\backslash x,\;\; x*y=y\cdot x. \tag{1}$$

After use of these equalities we get another identity in the quasigroup $(Q,\cdot,\backslash,/)$.

Consider the transformations of identities in a primitive quasigroup $(Q,\cdot,\backslash,/)$ that are connected with the change of the operation $(\cdot)$ to its parastrophes. The following Table 1 shows how parastrophes are changed in an identity under the change of the operation $(\cdot)$ for some its parastrophe.

$(\cdot)$	$(\cdot)$	$(\backslash)$	$(/)$	$(\otimes_1)$	$(\otimes_2)$	$(*)$
$(\cdot)$	$(\cdot)$	$(\backslash)$	$(/)$	$(\otimes_1)$	$(\otimes_2)$	$(*)$
$(\backslash)$	$(\backslash)$	$(\cdot)$	$(\otimes_1)$	$(/)$	$(*)$	$(\otimes_2)$
$(/)$	$(/)$	$(\otimes_2)$	$(\cdot)$	$(*)$	$(\backslash)$	$(\otimes_1)$
$(\otimes_1)$	$(\otimes_1)$	$(*)$	$(\backslash)$	$(\otimes_2)$	$(\cdot)$	$(/)$
$(\otimes_2)$	$(\otimes_2)$	$(/)$	$(*)$	$(\cdot)$	$(\otimes_1)$	$(\backslash)$
$(*)$	$(*)$	$(\otimes_1)$	$(\otimes_2)$	$(\backslash)$	$(/)$	$(\cdot)$

Table 1

Indeed, if $(\cdot)\to(\backslash)$, then we have the following change of parastrophes: $(\backslash)\to(\backslash)^{-1}=(\cdot)$, $(/)\to^{-1}(\backslash)=(\otimes_1)$, $(\otimes_1)\to(\backslash)^{\otimes_1}=(/)$, $(\otimes_2)\to(\backslash)^{\otimes_2}=(*)$, $(*)\to(\backslash)^{*}=(\otimes_2)$. Thus we get an identity in the quasigroup $(Q,\backslash,\cdot,\otimes_1)$. This result is reflected in the second row of Table 1. The remaining rows are fulled analogously.

Below we shall consider the parastrophic equivalence of identities in the following sense.

Definition 1. An identity β in a quasigroup $(Q,\cdot,\backslash,/)$ is called *parastrophically equivalent* to an identity α if β can be obtained from α under the change of the operation $(\cdot)$ to one of six its parastrophic operations with the successive passage, if it necessary, to the signature $(\cdot,\backslash,/)$ in the obtained identity by means of the equalities (1).

Note that according to this definition in each identity α we use only the operation $(\cdot)$ even if this operation is absent in this identity (see, for example, the identities 8) and 9) in section 5).

It is easy to prove that the relation of this definition is a relation of equivalence (i. e., symmetric, reflexive and transitive), taking into account that the parastrophic transformations of a quasigroup $(Q, \cdot)$ form the symmetrical group S_3 (see, for example, [8], where the multiplication table of the parastrophic transformations of a quasigroup $(Q, \cdot)$ is given).

Two identities in a quasigroup $(Q, \cdot, \backslash, /)$ is called *mutually symmetric* if one identity is obtained from another one under the passage from the operation $(\cdot)$ to the parastrophe $(*)$. An identity is called *symmetric* if it coincides with the mutually symmetric identity.

Note that if an identity in a quasigroup $(Q, \cdot, \backslash, /)$ characterizes some property of the quasigroup $(Q, \cdot)$, then an identity, which is parastrophically equivalent to this identity, not necessarily characterizes this property of the quasigroup $(Q, \cdot)$, although characterizes it in the corresponding parastrophic quasigroup. However, such situation is sometimes possible.

4. Identities for quasigroups isotopic to groups

Let some identity in a primitive quasigroup $(Q, \cdot, \backslash, /)$ characterize quasigroup $(Q, \cdot)$ isotopic to a group (to an abelian group). Then any identity parastrophically equivalent to this identity also characterizes the property of this quasigroup to be isotopic to this group (to this abelian group).

Indeed, it is known that if a quasigroup $(Q, \cdot)$ is isotopic to a group (to an abelian group) $(Q, +)$, then any its parastrophe is isotopic to this group (see [12] and Lemma 1.1.1 [7]). Write some identity α in a quasigroup $(Q, \cdot, \backslash, /)$ that characterizes the property of quasigroup $(Q, \cdot)$ to be isotopic to a group (to an abelian group) for some parastrophe (Q, σ) of $(Q, \cdot)$ and use the equalities (1). Then we shall get an identity β in the same signature, which is necessary and sufficient for isotopy of the quasigroup (Q, σ) (and of the quasigroup $(Q, \cdot)$, by Lemma 1.1.1 [7]) to the same group (to the same abelian group).

Thus from one identity we can obtain the class of parastrophically equivalent identities in a primitive quasigroup every of which also characterizes the variety of quasigroups isotopic to groups (to abelian groups).

Recall that an identity $w_1 = w_2$ in a quasigroup $(Q, \cdot, \backslash, /)$ is called *balanced* [3], if every variable appears from the left and from the right exactly one time. Let $[w_1] = [w_2] = n$ for an identity $w_1 = w_2$, where $[w]$ is the number of appearances of variables in a word w. Then the number n is called the length of this identity.

Below we shall consider near-balanced identities in the following sense.

Definition 2. An identity $w_1 = w_2$ of length $n + 1$ of $n \geq 2$ variables in a quasigroup $(Q, \cdot, \backslash, /)$ is called *near-balanced* if every of $n - 1$ variables appears exactly one time, but the single variable appears exactly two times on each side of the identity.

From the known balanced identity of Belousov (2) characterizing quasigroups isotopic to groups we can obtain a class of parastrophically equivalent balanced identities (or a parastrophical-equivalent class) characterizing these quasigroups.

Theorem 1. *The following balanced identities of five variables:*

$$((x(y\backslash z))/u)v = x(y\backslash((z/u)v)), \tag{2}$$

$$(u/(x\backslash yz)\backslash v = x\backslash(y((u/z)\backslash v)), \tag{3}$$

$$((x/(z\backslash y))u)/v = x/((zu/v)\backslash y) \tag{4}$$

form a parastrophical-equivalent class of identities characterizing quasigroups isotopic to groups.

Proof. Transform the Belousov identity (2), changing the operation $(\cdot)$ for parastrophes and using equalities (1):

$(\cdot) \to (\backslash)$: $((x\backslash(yz)) \otimes_1 u)\backslash v = x\backslash(y((z \otimes_1 u)\backslash v))$ or (3):

$$(u/(x\backslash yz)\backslash v = x\backslash(y((u/z)\backslash v)).$$

$(\cdot) \to (/)$: $((x/(y \otimes_2 z))u)/v = x/(y \otimes_2 (zu/v))$ or (4):

$$((x/(z\backslash y))u)/v = x/((zu/v)\backslash y).$$

$(\cdot) \to (\otimes_1)$: $((x \otimes_1 (y * z))\backslash u) \otimes_1 v = x \otimes_1 (y * ((z\backslash u) \otimes_1 v))$ or

$$v/((zy/x)\backslash u) = ((v/(z\backslash u))y)/x.$$

But it is the identity (4) after transpositions (x, v), (y, u) of variables.

$(\cdot) \to (\otimes_2)$: $((x \otimes_2 (y/z)) * u) \otimes_2 v = x \otimes_2 (y/((z * u) \otimes_2 v))$ or

$$v\backslash(u((y/z)\backslash x)) = (y/(v\backslash uz))\backslash x.$$

It is the identity (2) after the transpositions (x, v), (y, u).

$(\cdot) \to (*)$: $((x * (y \otimes_1 z)) \otimes_2 u) * v = x * (y \otimes_1 ((z \otimes_2 u) * v))$ or

$$v(u\backslash((z/y)x)) = ((v(u\backslash z))/y)x.$$

It is (2) after the transpositions as above.

Hence, from the identity (2) we obtain a parastrophical-equivalent class of balanced identities of length five. This class contains three identities. Note that the identity (2) is symmetric, the identities (3) and (4) are mutually symmetric (use the transpositions (x, v), (y, u) of variables). □

Theorem 1a. *The following near-balanced identities of four variables:*

$$((x(u\backslash z))/u)v = x(u\backslash((z/u)v)), \tag{2a}$$

$$(u/(x\backslash uz))\backslash v = x\backslash(u((u/z)\backslash v)), \tag{3a}$$

$$((x/(z\backslash u))u)/v = x/((zu/v)\backslash u) \tag{4a}$$

form a parastrophical-equivalent class of identities characterizing the quasigroups isotopic to groups.

Proof. These three identities, each of which characterizes quasigroups isotopic to groups, were given in Corollary 1.1.2 of [7]. The identity $(2a)$ was obtained from the balanced Belousov identity of five variables by F. N. Sokhats'kyi in [12] (the identity (38)). The identity $(3a)$ (the identity $(4a)$) is obtained from $(2a)$ by the change of the operation $(\cdot)$ for the operation $(\backslash)$ (for the operation $(/)$). Indeed, if in $(2a)$ $(\cdot) \to (\backslash)$, then $((x\backslash(uz)) \otimes_1 u)\backslash v = x\backslash(u \cdot ((z \otimes_1 u)\backslash v))$ or

$$(u/(x\backslash(uz))\backslash v = x\backslash(u \cdot ((u/z)\backslash v)). \text{ It is } (3a).$$

If in $(2a)$ $(\cdot) \to (/)$, then $((x/(u \otimes_2 z)) \cdot u)/v = x/(u \otimes_2 ((z \cdot u)/v))$ or $((x/(z\backslash u)) \cdot u)/v = x/((z \cdot u)/v)\backslash u)$. It is $(4a)$.

Consider the identities which can be obtained from $(2a)$ if to change the operation $(\cdot)$ for the operation $(\otimes_1)$ (for $(\otimes_2)$ and for $(*)$ respectively) and to use Table 1 and the equalities (1):

$(\cdot) \to (\otimes_1)$: $((x \otimes_1 (u * z))\backslash u) \otimes_1 v = x \otimes_1 (u * ((z\backslash u) \otimes_1 v))$ or

$$v/((zu/x)\backslash u) = ((v/(z\backslash u))u)/x.$$

But it is $(4a)$ after the change of the positions of variables x, v.

$(\cdot) \to (\otimes_2)$: $((x \otimes_2 (u/z)) * u) \otimes_2 v = x \otimes_2 (u/((z * u) \otimes_2 v))$ or

$$v\backslash(u((u/z)\backslash x)) = (u/(v\backslash uz))\backslash x.$$

It is $(3a)$ if to change the positions of variables x, v.

$(\cdot) \to (*)$: $((x * (u \otimes_1 z)) \otimes_2 u) * v = x * (u \otimes_1 ((z \otimes_2 u) * v))$ or

$$v(u\backslash((z/u)x)) = ((v(u\backslash z))/u)x. \text{ It is } (2a).$$

Note that the identity $(2a)$ is symmetric, and the identities $(3a)$ and $(4a)$ are mutually symmetric. □

5. Quasigroups isotopic to abelian groups

M. M. Gluchov informed the author about some his unpublished results. In particular, he proved that among of the identities characterizing the variety of quasigroups isotopic to abelian groups there not exist balanced identities of three variables and listed the following six balanced identities of length four, every of which characterizes the quasigroups isotopic to abelian groups:

$$\begin{array}{llll} 1) & x\backslash(y(u\backslash v)) = u\backslash(y(x\backslash v)); & 2) & (x/y)(u\backslash v) = (v/y)(u\backslash x); \\ 3) & ((xy)/u)v = ((xv)/u)y; & 4) & xu/(v\backslash y) = vu/(x\backslash y); \\ 5) & x(y\backslash(uv)) = u(y\backslash(xv)); & 6) & ((u/v)x)/y = ((u/y)x)/v. \end{array}$$

The identities 1), 2) were established by V. D. Belousov [3], the identities 3), 4) and 5) were given by A. Drapal [10], A. Tabarov found the identity 6).

Using the change of the quasigroup operation $(\cdot)$ for distinct parastrophic operations in six identities pointed out above, we found yet three balanced identities of length four, every of which characterizes quasigroups isotopic to abelian groups:

$$7) \ (u/v)\backslash yx = (u/x)\backslash yv; \quad 8) \ (y/(v\backslash u))\backslash x = (y/(v\backslash x))\backslash u;$$

$$9)\quad x/((u/v)\backslash y) = u/((x/v)\backslash y).$$

The identity 7) is obtained from 2) under the change $(\cdot) \to (\backslash)$, and when $(\cdot) \to (\otimes_2)$, also from 4) if $(\cdot) \to (\otimes_1)$, and when $(\cdot) \to (*)$.

The identity 8) is obtained from 1) under $(\cdot) \to (/)$, from 3) if $(\cdot) \to (\backslash)$, from 5) when $(\cdot) \to (\otimes_2)$ and from 6) if $(\cdot) \to (\otimes_1)$.

The identity 9) follows from 1) under $(\cdot) \to (\otimes_2)$, from 3) if $(\cdot) \to (\otimes_1)$, from 5) when $(\cdot) \to (/)$ and from 6) if $(\cdot) \to (\backslash)$.

Theorem 2. *All nine balanced identities of length four, pointed out above and characterizing quasigroups isotopic to abelian groups, form two parastrophical-equivalent classes:*

$$\{1), 3), 5), 6), 8), 9)\} \text{ and } \{2), 4), 7)\}.$$

Proof. Transform the identity 1): $x\backslash(y(u\backslash v)) = u\backslash(y(x\backslash v))$ using the passage from the operation $(\cdot)$ to the remaining five its parastrophes, Table 1 and the equalities (1):

$(\cdot) \to (\backslash)$: $x(y\backslash(uv)) = u(y\backslash(xv))$. It is the identity 5).

$(\cdot) \to (/)$: $x \otimes_2 (y/(u \otimes_2 v)) = u \otimes_2 (y/(x \otimes_2 v))$ or $(y/(v\backslash u))\backslash x = (y/(v\backslash x))\backslash u$. It is the identity 8).

$(\cdot) \to (\otimes_1)$: $x * (y \otimes_1 vu) = u * (y \otimes_1 vx)$ or $(vu/y)x = (vx/y)u$. It is 3).

$(\cdot) \to (\otimes_2)$: $x/(y \otimes_2 (u/v)) = u/(y \otimes_2 (x/v))$ or $x/((u/v)\backslash y) = u/((x/v)\backslash y)$. It is 9).

$(\cdot) \to (*)$: $x \otimes_1 ((u \otimes_1 v)y) = u \otimes_1 ((x \otimes_1 v)y)$ or $((v/u)y)/x = ((v/x)y)/u$. It is 6).

Thus for the identity 1) we have six parastrophically equivalent identities: 1), 3), 5), 6), 8) and 9). Moreover, the following pairs of identities are mutually symmetric: 1) and 6); 3) and 5); 8) and 9).

Consider the identity 2): $(x/y)(u\backslash v) = (v/y)(u\backslash x)$.

$(\cdot) \to (\backslash)$: $(x \otimes_1 y)\backslash uv = (v \otimes_1 y)\backslash ux$ or $(y/x)\backslash uv = (y/v)\backslash ux$. It is the identity 7).

$(\cdot) \to (/)$: $xy/(u \otimes_2 v) = vy/(u \otimes_2 x)$ or $xy/(v\backslash u) = vy/(x\backslash u)$. It is 4).

$(\cdot) \to (\otimes_1)$: $(x\backslash y) \otimes_1 vu = (v\backslash y) \otimes_1 xu$ or $vu/(x\backslash y) = xu/(v\backslash y)$. It is the identity 4).

$(\cdot) \to (\otimes_2)$: $yx \otimes_2 (u/v) = yv \otimes_2 (u/x)$ or $(u/v)\backslash yx = (u/x)\backslash yv$. It is the identity 7).

$(\cdot) \to (*)$: $(x \otimes_2 y) * (u \otimes_1 v) = (v \otimes_2 y) * (u \otimes_1 x)$, or $(v/u)(y\backslash x) = (x/u)(y\backslash v)$. It is 2).

Thus we have the class of three parastrophically equivalent identities: 2), 4) and 7). The pair of the identities 4) and 7) is mutually symmetric and the identity 2) is symmetric. $\square$

Corollary 1. *There exist at least two parastrophically equivalent classes of balanced identities of length four characterizing the variety of quasigroups isotopic to abelian groups.* □

6. Identities with a 0-ary operation

In [6], [7] and [9] were considered identities with permutations (or, simply, identities) in a quasigroup $(Q, \cdot)$:

$$\alpha_1(\alpha_2(x \oplus_1 y) \oplus_2 z) = \alpha_3 x \oplus_3 \alpha_4(\alpha_5 y \oplus_4 \alpha_6 z), \tag{5}$$

where x, y, z are variables, α_i, $i = 1, 2, ..., 6$ ($i \in \overline{1,6}$), is a permutation of the set Q, $(\oplus_k)$, $k = 1, 2, 3, 4$, is a parastrophic operation for the quasigroup operation $(\cdot)$. These identities form the special case of the generalized associativity identity [1]. A particular case of this identity (when α_1 is the identity permutation) is the identity with permutations

$$\alpha_2(x \oplus_1 y) \oplus_2 z = \alpha_3 x \oplus_3 \alpha_4(\alpha_5 y \oplus_4 \alpha_6 z). \tag{6}$$

The ordered collection $(\oplus_1, \oplus_2, \oplus_3, \oplus_4)$ of parastrophic operations in an identity (5) is called the *type* of this identity. Note that three variables in (5) (in (6)) are ordered uniformly from the left and from the right.

In [7], it was proved that if a quasigroup $(Q, \cdot)$ satisfies an identity with permutations of the form (5), then the quasigroup $(Q, \cdot)$ is isotopic to a group. A quasigroup $(Q, \cdot)$ is isotopic to a group if and only if it satisfies the following identity with permutations of the type $(\circ, \circ, \circ, \circ)$:

$$R_a^{-1}(x \circ L_a^{-1} y) \circ z = x \circ L_a^{-1}(R_a^{-1} y \circ z)$$

for a fixed element $a \in Q$, where $(\circ)$ is a parastrophe of the operation $(\cdot)$, $R_a x = x \circ a$, $L_a x = a \circ x$ (Theorems 1.1.1 and 1.1.1a of [7]).

For quasigroups isotopic to abelian groups it was proved the following

Theorem 1.2.1. [7] *Let the identity* (6) *of the type* $(\oplus_1, \circ, \circ^*, \oplus_4)$ *with some parastrophes* $(\circ)$, $(\oplus_1), (\oplus_4)$ *and with some permutations* α_i, $i \in \overline{2,6}$, *hold in a quasigroup* $(Q, \cdot)$. *Then the quasigroup* $(Q, \cdot)$ *is isotopic to an abelian group.*

For any type $(\oplus_1, \oplus_2, \oplus_3, \oplus_4)$ *different from* $(\cdot, \cdot, \cdot, \cdot)$ *and* $(*, *, *, *)$, *where* $(\oplus_i) = (\cdot)$ *or* $(\oplus_i) = (\cdot)^*$, $i \in \overline{1,4}$, *there exists an identity of the form* (6) *that characterizes quasigroups* $(Q, \cdot)$ *isotopic to abelian groups.*

Below we show that in each of nine identities of section 5 characterizing quasigroups isotopic to abelian groups one of variables may be fixed. As a result, we obtain some identities of three variables in a quasigroup with a 0-ary operation. Both identities with permutations characterizing quasigroups isotopic to groups and identities with permutations characterizing quasigroups isotopic to abelian groups, can have different types.

Theorem 3. *Each of the following identities in a quasigroup $(Q,\cdot,\backslash,/,a)$ with a 0-operation characterizes quasigroups $(Q,\cdot)$ isotopic to abelian groups:*

$$x\backslash(a(u\backslash v)) = u\backslash(a(x\backslash v)),\ x\backslash(y(u\backslash a)) = u\backslash(y(x\backslash a)); \tag{1a}$$

$$(x/y)(a\backslash v) = (v/y)(a\backslash x),\ (x/a)(u\backslash v) = (v/a)(u\backslash x); \tag{2a}$$

$$((xy)/a)v = ((xv)/a)y,\ ((ay)/u)v = ((av)/u)y; \tag{3a}$$

$$xa/(v\backslash y) = va/(x\backslash y),\ xu/(v\backslash a) = vu/(x\backslash a); \tag{4a}$$

$$x(a\backslash(uv)) = u(a\backslash(xv)),\ x(y\backslash(ua)) = u(y\backslash(xa)); \tag{5a}$$

$$((u/v)a)/y = ((u/y)a)/v,\ ((a/v)x)/y = ((a/y)x)/v; \tag{6a}$$

$$(u/v)\backslash ax = (u/x)\backslash av,\ (a/v)\backslash yx = (a/x)\backslash yv; \tag{7a}$$

$$(y/(a\backslash u))\backslash x = (y/(a\backslash x))\backslash u,\ (a/(v\backslash u))\backslash x = (a/(v\backslash x))\backslash u; \tag{8a}$$

$$x/((u/v)\backslash a) = u/((x/v)\backslash a),\ x/((u/a)\backslash y) = u/((x/a)\backslash y). \tag{9a}$$

Proof. We shall obtain every pair of the identities 1a) – 9a) from the identities 1)– 9) respectively using the sufficient conditions of Theorem 1.2.1 [7] and the equalities (1). In all cases the necessity of the obtained identities follows from the identities 1)– 9) respectively.

1a). The identity $x\backslash(a(u\backslash v)) = u\backslash(a(x\backslash v))$ or $x\backslash L_a(u\backslash v) = u\backslash L_a(x\backslash v)$, where $L_a x = a\cdot x$, is the identity 1) for $y = a$ and can be written as

$$L_a(u\backslash v)\otimes_2 x = u\backslash L_a(v\otimes_2 x),$$

where $(\otimes_2) = (\backslash)^*$. This identity has the form (6) and the type $(\backslash,\otimes_2,\backslash,\otimes_2)$. Therefore, by Theorem 1.2.1 of [7], the quasigroup $(Q,\cdot)$ is isotopic to an abelian group even if in 1) the variable y is fixed.

Putting in 1) $v = a$, we obtain the second identity of 1a):

$$x\backslash(y(u\backslash a)) = u\backslash(y(x\backslash a)),\, x\backslash(y(a\otimes_2 u)) = u\backslash(y(a\otimes_2 x)$$

or $(y\cdot L_a^{\otimes_2}u)\otimes_2 x = u\backslash(y\cdot L_a^{\otimes_2}x)$, where $L_a^{\otimes_2}x = a\otimes_2 x$. Transforming the last identity, we get the identity

$$(u*y)\otimes_2 x = (L_a^{\otimes_2})^{-1}u\backslash(y\cdot L_a^{\otimes_2}x) \text{ of the type } (*,\otimes_2,\backslash,\cdot).$$

Note that the identity obtained from 1) can not be reduced to the required form of Theorem 1.2.1 of [7] if to fix one of the rest two variables.

Thus from the identity 1) in a primitive quasigroup $(Q,\cdot,\backslash,/)$ we obtain two identities in the quasigroup $(Q,\cdot,\backslash,/,a)$ for an element $a\in Q$.

2a). Put $u = a$ in 2): $(x/y)(a\backslash v) = (v/y)(a\backslash x)$, $(x/y)\cdot L_a^{-1}v = (v/y)\cdot L_a^{-1}x$ whence we have the identity

$$(x/y)\cdot v = L_a^{-1}x*(y\otimes_1 L_a v) \text{ of the type } (/,\cdot,*,\otimes_1).$$

If $y = a$ in 2), we obtain the second identity of $2a$): $(x/a)(u\backslash v) = (v/a)(u\backslash x)$, $R_a^{-1}x \cdot (u\backslash v) = R_a^{-1}v \cdot (u\backslash x)$ $R_a x = xa$, and the identity

$$(v \otimes_2 u) * x = R_a^{-1}v \cdot (u\backslash R_a x) \text{ of the type } (\otimes_2, *, \cdot, \backslash).$$

$3a$). For $u = a$ in 3) we have $((xy)/a)v = ((xv)/a)y$, $R_a^{-1}(xy)\cdot v = R_a^{-1}(xv)\cdot y$, and the identity

$$R_a^{-1}(y * x) \cdot v = y * R_a^{-1}(xv) \text{ of the type } (*, \cdot, *, \cdot).$$

Let $x = a$ in 3): $((ay)/u)v = ((av)/u)y$, $(L_a y/u)v = (L_a v/u)y$, Hence, the following identity of the type $(/, \cdot, *, \otimes_1)$ holds

$$(y/u) \cdot v = L_a^{-1}y * (u \otimes_1 L_a v).$$

$4a$). Put in 4) $u = a$: $xa/(v\backslash y) = va/(x\backslash y)$, $R_a x/(v\backslash y) = R_a v/(x\backslash y)$ whence for $(\otimes_1) = (/)^*$ it follows the identity

$$(v\backslash y) \otimes_1 x = R_a v/(y \otimes_2 R_a^{-1}x) \text{ of the type } (\backslash, \otimes_1, /, \otimes_2).$$

If $y = a$, then $xu/(v\backslash a) = vu/(x\backslash a)$, $xu/L_a^{\otimes_2}v = vu/L_a^{\otimes_2}x$ whence we obtain the identity

$$xu/v = L_a^{\otimes_2}x \otimes_1 (u * (L_a^{\otimes_2})^{-1}v) \text{ of the type } (\cdot, /, \otimes_1, *).$$

$5a$). Let $y = a$ in 5): $x(a\backslash(uv)) = u(a\backslash(xv))$, $x \cdot L_a^{-1}(uv) = u \cdot L_a^{-1}(xv)$, and we have the identity

$$L_a^{-1}(uv) * x = u \cdot L_a^{-1}(v * x) \text{ of the type } (\cdot, *, \cdot, *).$$

For $v = a$ in 5) we get $x(y\backslash(ua)) = u(y\backslash(xa))$, $x(y\backslash R_a u) = u \cdot (y\backslash R_a x)$, $(y\backslash R_a u) * x = u(y\backslash R_a x)$, and the identity

$$(u \otimes_2 y) * x = R_a^{-1}u \cdot (y\backslash R_a x) \text{ of the type } (\otimes_2, *, \cdot, \backslash).$$

$6a$). We obtain the identities $((u/v)a)/y = ((u/y)a)/v$, $R_a(u/v)/y = R_a(u/y)/v$ if in 6) $x = a$. From the last identity it follows the identity

$$R_a(v \otimes_1 u)/y = v \otimes_1 R_a(u/y) \text{ of the type } (\otimes_1, /, \otimes_1, /).$$

If $u = a$, then $((a/v)x)/y = ((a/y)x)/v$, $(R_a^{\otimes_1}v \cdot x)/y = (R_a^{\otimes_1}y \cdot x)/v$, where $R_a^{\otimes_1}x = x \otimes_1 a$. Hence, we get the following identity:

$$(R_a^{\otimes_1}v \cdot x)/y = v \otimes_1 (x * R_a^{\otimes_1}y) \text{ of the type } (\cdot, /, \otimes_1, *).$$

$7a$). Put $y = a$ in 7): $(u/v)\backslash ax = (u/x)\backslash av$, $(u/v)\backslash L_a x = (u/x)\backslash L_a v$,

$$(v \otimes_1 u)\backslash x = L_a v \otimes_2 (u/L_a^{-1}x).$$

The type of this identity is $(\otimes_1, \backslash, \otimes_2, /)$.

If $u = a$, we get $(a/v)\backslash yx = (a/x)\backslash yv$, $(v \otimes_1 a)\backslash(yx) = (x \otimes_1 a)\backslash(yv)$, $yx \otimes_2 R_a^{\otimes_1} v = R_a^{\otimes_1} x\backslash yv$, and the identity

$$(x * y) \otimes_2 v = R_a^{\otimes_1} x\backslash(y \cdot (R_a^{\otimes_1})^{-1} v) \text{ of the type } (*, \otimes_2, \backslash, \cdot).$$

8a). Let $v = a$ in 8): $(y/(a\backslash u))\backslash x = (y/(a\backslash x))\backslash u$, $(y/L_a^{-1}u)\backslash x = (y/L_a^{-1}x)\backslash u$ whence we obtain the identity

$$(u \otimes_1 y)\backslash x = L_a u \otimes_2 (y/L_a^{-1}x) \text{ of the type } (\otimes_1, \backslash, \otimes_2, /).$$

Put $y = a$: $(a/(v\backslash u))\backslash x = (a/(v\backslash x))\backslash u$, $(a/(u \otimes_2 v)\backslash x = u \otimes_2 (a/(v\backslash x))$. Let $L_a^{(/)} x = a/x$, then from the last identity we have the identity

$$L_a^{(/)}(u \otimes_2 v)\backslash x = u \otimes_2 L_a^{(/)}(v\backslash x) \text{ of the type } (\otimes_2, \backslash, \otimes_2, \backslash).$$

9a). Putting $y = a$ in 9), we get $x/((u/v)\backslash a) = u/((x/v)\backslash a)$, $(a \otimes_2 (u/v)) \otimes_1 x = u/(a \otimes_2 (x/v))$, and the following identity:

$$L_a^{\otimes_2}(u/v) \otimes_1 x = u/L_a^{\otimes_2}(v \otimes_1 x) \text{ of the type } (/, \otimes_1, /, \otimes_1).$$

If $v = a$, $x/((u/a)\backslash y) = u/((x/a)\backslash y)$, $((u/a)\backslash y) \otimes_1 x = u/((y \otimes_2 (x/a))$. Let $R_a^{(/)} x = x/a$, then we have the identity

$$(R_a^{(/)} u\backslash y) \otimes_1 x = u/(y \otimes_2 R_a^{(/)} x) \text{ of the type } (\backslash, \otimes_1, /, \otimes_2). \qquad \square$$

7. Near-balanced identities for quasigroups

In [7], the identities with permutations of different types were considered. As a corollary, in a quasigroup $(Q, \cdot, \backslash, /)$ the following identities characterizing quasigroups isotopic to abelian groups were obtained (Theorem 1.2.1a, the identities (1.2.9) – (1.2.15) of [7]):

$$((x \cdot y)/u) \cdot (u\backslash z) = x \cdot u\backslash((z/u) \cdot y), \tag{7}$$

$$(((y/u) \cdot (u\backslash x))/u) \cdot (u\backslash z) = (x/u) \cdot (u\backslash((z/u) \cdot (u\backslash y))), \tag{8}$$

$$z \cdot (u\backslash((y/u) \cdot x)) = ((z \cdot x)/u) \cdot (u\backslash y), \tag{9}$$

$$((y \cdot x)/u) \cdot z = ((y \cdot z)/u) \cdot x, \tag{10}$$

$$z \cdot u\backslash((y/u) \cdot (u\backslash x)) = (x/u) \cdot u\backslash(z \cdot (u\backslash y)), \tag{11}$$

$$((x/u) \cdot y)/u \cdot (u\backslash z) = ((z/u) \cdot y)/u \cdot (u\backslash x), \tag{12}$$

$$((x/u) \cdot y)/u \cdot (u\backslash z) = ((z/u) \cdot (u\backslash x))/u \cdot y \tag{13}$$

Consider these identities more carefully. First note that the identities (7) and (9) coincide although they correspond to different types of identities with permutations (unfortunately, that was not noticed in [7]).

The identity (10) is the balanced identity 3) of the Glukhov list, the rest identities of four variables are unbalanced. Show that identities (11), (12) and (13) can be simplified and reduced to the known balanced identities.

Proposition 1. *The identity* (10) *is the identity* 3)*, the identity* (11) *is reduced to the identity* 5)*, the identities* (12) *and* (13) *are reduced to* 3)*.*

Proof. (10) is the balanced identity 3) of the Glukhov list. The identity (11) means that $z\cdot L_u^{-1}(R_u^{-1}y\cdot L_u^{-1}x) = R_u^{-1}x\cdot L_u^{-1}(z\cdot L_u^{-1}y)$ or $z\cdot L_u^{-1}(\alpha_u y\cdot x) = \alpha_u x\cdot L_u^{-1}(z\cdot y)$, where $\alpha_u = R_u^{-1}L_u$. From where for $z = u$ it follows that $\alpha_u y\cdot x = \alpha_u x\cdot y$. Therefore, $z\cdot L_u^{-1}(\alpha_u x\cdot y) = \alpha_u x\cdot L_u^{-1}(z\cdot y)$ or $z\cdot(u\backslash xy) = x\cdot(u\backslash zy)$. It is the balanced identity 5) of the Glukhov list.

(12) is $R_u^{-1}(R_u^{-1}x\cdot y)\cdot L_u^{-1}z = R_u^{-1}(R_u^{-1}z\cdot y)\cdot L_u^{-1}x$ or $R_u^{-1}(\alpha_u x\cdot y)\cdot z = R_u^{-1}(\alpha_u z\cdot y)\cdot x$, from where for $y = u$ we get $\alpha_u x\cdot z = \alpha_u z\cdot x$. Hence, $R_u^{-1}(yx)\cdot z = R_u^{-1}(y\cdot z)\cdot x$ or $(yx/u)\cdot z = (yz/u)\cdot x$. It is the identity 3).

(13) is $R_u^{-1}(R_u^{-1}x\cdot y)\cdot L_u^{-1}z = R_u^{-1}(R_u^{-1}z\cdot L_u^{-1}x)\cdot y$ or $R_u^{-1}(R_u^{-1}L_u x\cdot y)\cdot z = R_u^{-1}(R_u^{-1}L_u z\cdot x)\cdot y$.

If $y = u$, we have the equality $\alpha_u x\cdot z = \alpha_u z\cdot x$ and the identity 3) of Glukhov's list: $((xy)/u)\cdot z = ((xz)/u)\cdot y$. □

Theorem 4. *The following near-balanced identities of length five in a quasigroup* $(Q,\cdot,\backslash,/)$*:*

$$(xy/u)\cdot(u\backslash z) = x\cdot(u\backslash((z/u)\cdot y)), \tag{14}$$

$$(u/(x\backslash y))\backslash(uz) = x\backslash(u\cdot((u/z)\backslash y)), \tag{15}$$

$$((x/y)\cdot u)/(z\backslash u) = x/((zu/y)\backslash u), \tag{16}$$

$$zu/((y/x)\backslash u) = ((y/(z\backslash u))\cdot u)/x, \tag{17}$$

$$(u/z)\backslash(u\cdot(y\backslash x)) = (u/(y\backslash uz))\backslash x, \tag{18}$$

$$(z/u)\cdot(u\backslash yx) = ((y\cdot(u\backslash z))/u)\cdot x \tag{19}$$

form a parastrophical-equivalent class of identities characterizing quasigroups isotopic to abelian groups.

Proof. The identity (14) is (7) and, by Theorem 1.2.1a [7], characterizes quasigroups isotopic to abelian groups. At first we shall give the short proof from [7] of this fact.

Let a quasigroup $(Q,\cdot)$ be isotopic to an abelian group. Then, by Albert's theorem (see [4]), we conclude that the loop $(Q,+)$: $x+y = R_a^{-1}x\cdot L_a^{-1}y$, which is principally isotopic to this quasigroup, is an abelian group for any element $a\in Q$.

Hence, the identity $(x+y)+z = x+(z+y)$ is fulfilled. Pass in this identity to the operation $(\cdot)$:

$$R_a^{-1}(R_a^{-1}x \cdot L_a^{-1}y) \cdot L_a^{-1}z = R_a^{-1}x \cdot L_a^{-1}(R_a^{-1}z \cdot L_a^{-1}y). \tag{20}$$

From this identity with permutations after the respective change of variables we have the following identity:

$$R_a^{-1}(x \cdot y) \cdot L_a^{-1}z = x \cdot L_a^{-1}(R_a^{-1}z \cdot y). \tag{21}$$

This identity is true for any element $a \in Q$. Thus we have the identity (7).

Conversely, if the identity (7) holds, then the identity (21) and the identity $R_a^{-1}(x \cdot y) \cdot z = x \cdot L_a^{-1}(y * R_a^{-1}L_a z)$ hold. But the last identity is an identity of the form (5) and, by Theorem 1.1.1 [7], the quasigroup $(Q,\cdot)$ is isotopic to a group. After the inverse transformation of the last identity we obtain the identity (20), which means that in the group $(Q,+)$: $x+y = R_a^{-1}x \cdot L_a^{-1}y$ the identity $(x+y)+z = x+(z+y)$ holds. From where it follows that $(Q,+)$ is an abelian group (put $x=0$, where 0 is the unit of the group).

The rest identities of the theorem we shall obtain from the identity (14) passing on in this identity from the operation $(\cdot)$ to the parastrophes $(\backslash)$, $(/)$, $(\otimes_1)$, $(\otimes_2)$ and $(*)$ respectively and using Tale 1 and the equalities (1).

For example, in (14) change the operation $(\cdot)$ for the parastrophe $(\backslash)$:

$$((x\backslash y) \otimes_1 u)\backslash(uz) = x\backslash(u \cdot ((z \otimes_1 u)\backslash y)) \text{ or } (u/(x\backslash y))\backslash(uz) = x\backslash(u \cdot ((u/z)\backslash y)).$$

It is the identity (15).

The remaining identities are checked analogously.

Note that each of the pairs of identities (19) and (14), (15) and (17), (18) and (16) is mutually symmetric. □

Proposition 2. *The identity* (8) *is reduced to the identity* (19).

Proof. Writing the identity (8):

$$(((y/u) \cdot (u\backslash x))/u) \cdot (u\backslash z) = (x/u) \cdot (u\backslash((z/u)) \cdot (u\backslash y))$$

with the help of translations, we obtain the identities

$$R_u^{-1}(R_u^{-1}y \cdot L_u^{-1}x) \cdot L_u^{-1}z = R_u^{-1}x \cdot L_u^{-1}(R_u^{-1}z \cdot L_u^{-1}y),$$
$$R_u^{-1}(R_u^{-1}L_u y \cdot x) \cdot z = R_u^{-1}L_u x \cdot L_u^{-1}(R_u^{-1}L_u z \cdot y).$$

Let $R_u^{-1}L_u = \alpha_u$, $z = u$, then $\alpha_u y \cdot x = \alpha_u x \cdot y$ and $R_u^{-1}(y \cdot L_u^{-1}x) \cdot z = R_u^{-1}x \cdot L_u^{-1}(y \cdot z)$ or $((y \cdot (u\backslash x))/u) \cdot z = (x/u) \cdot (u\backslash yz)$. But it is the identity (19) if to interchange the positions of the variables x and z. □

References

[1] **V. D. Belousov**, *Globally associative systems of quasigroups*, (Russian), Mat. Sb. **55(97)** (1961), 221 – 236.

[2] **V. D. Belousov**, *Systems of quasigroups with generalized identities*, (Russian), Usp. Mat. Nauk **20** (1965), 75 – 146.

[3] **V. D. Belousov**, *Balanced identities in quasigroups*, (Russian), Mat. Sb. **70(112)** (1966), 55 – 97.

[4] **V. D. Belousov**, *Foundations of quasigroups and loops theory*, (Russian), Moscow, Nauka, 1967.

[5] **V. D. Belousov**, *Parastrophic-orthogonal quasigroups*, Quasigroups and Related Systems **13** (2005), 25 – 72.

[6] **G. B. Belyavskaya**, *Identities with permutations associated with quasigroups isotopic to groups*, Bul. Acad. Ştiinţe Repub. Moldova, ser. Matematica **2(53)** (2007), 19 – 24.

[7] **G. B. Belyavskaya**, *Quasigroups: Identities with permutations, linearity and nuclei*, (Russian), LAP, Germany, 2013.

[8] **G. B. Belyavskaya, T. V. Popovich**, *Conjugate sets of loops and quasigroups: DC-quasigroups*, Bul. Acad. Ştiinţe Repub. Moldova, ser. Matematica **1(68)** (2012), 21 – 32.

[9] **G. B. Belyavskaya, A. Kh. Tabarov**, *Identities with permutations leading to linearity of a quasigroup*, Discrete Math. Appl. **19** (2009), 172 – 190.

[10] **A. Drapal**, *On multiplication groups of relatively free quasigroups isotopic to abelian groups*, Czechoslovak Math. J. **55(130)** (2005), 61 – 87.

[11] **A. Sade**, *Quasigroupes parastrophiques. Expressions et identites*, Math. Nachr. **20** (1959), 73 – 106.

[12] **F. N. Sokhats'kyi**, *On isotopes of groups. II*, (Ukrainian), Ukrainskyi Mat. Zh. **47** (1995), 1692 – 1703.

[13] **S. K. Stein**, *On the foundations of quasigroups*, Trans. Amer. Math. Soc. **85** (1957), 228 – 256.

Received October 25, 2013

Institute of Mathematics and Computer Science, Academy of Sciences of Moldova,
str. Academiei 5, MD-2028 Chişinău , Moldova
E-mail: gbel1@rambler.ru

Quasigroups and Related Systems **22** (2014), 33 − 50

Filter theory on hyper residuated lattices

Rajabali Borzooei, Mahmud Bakhshi and Omid Zahiri

Abstract. We apply the hyper structures to residuated lattices and introduce the notion of hyper residuated lattice which is a generalization of the residuated lattice and verified some related results. Finally, we state and prove some theorems about filters and deductive systems.

1. Introduction

Residuated lattices, introduced by Ward and Dilworth [12], are a common structure among algebras associated with logical systems. In this definition to any bounded lattice $(\mathcal{L}, \vee, \wedge, 0, 1)$, a multiplication '$*$' and an operation '$\rightarrow$' are equpped such that $(\mathcal{L}, *, 1)$ is a commutative monoid and the pair $(*, \rightarrow)$ is an adjoint pair, i.e.,

$$x * y \leqslant z \text{ if and only if } x \leqslant y \rightarrow z, \ \forall x, y, z \in \mathcal{L}.$$

The main examples of residuated lattices are MV-algebras introduced by Chang [4] and BL-algebras introduced by Hájek [9]. The hyperstructure theory was introduced by Marty [10], at the 8th Congress of Scandinavian Mathematicians. In his definition, a function $f : A \times A \longrightarrow P^*(A)$, of the set $A \times A$ into the set of all non-empty subsets of A, is called a *binary hyperoperation*, and the pair (A, f) is called a *hypergroupoid*. If f is associative, A is called a *semihypergroup*, and it is said to be *commutative* if f is commutative. Also, an element $1 \in A$ is called the *unit* or the *neutral element* if $a \in f(1, a)$, for all $a \in A$. Since then many researchers have worked on this area. R. A. Borzooei et al. introduced and studied hyper K-algebras [2] and S. Ghorbani et al. [8], applied the hyperstructures to MV-algebras and introduced the concept of hyper MV-algebra, which is a generalization of MV-algebra. In [11], Mittas et al. applied the hyperstructures to lattices and introduced the concepts of a hyperlattice and supperlattice: A *superlattice* is a partially ordered set $(S; \leqslant)$ endowed with two binary hyperoperations $\vee$ and $\wedge$ satisfying the following properties: for all $a, b, c \in S$,

(SL1) $a \in (a \vee a) \cap (a \wedge a)$,
(SL2) $a \vee b = b \vee a, \quad a \wedge b = b \wedge a$,
(SL3) $(a \vee b) \vee c = a \vee (b \vee c), \quad (a \wedge b) \wedge c = a \wedge (b \wedge c)$,
(SL4) $a \in ((a \vee b) \wedge a) \cap ((a \wedge b) \vee a)$,

2010 Mathematics Subject Classification: 03G10, 06B99, 06B75.
Keywords: hyper residuated lattice, (weak) filter, (weak) deductive system.

(SL5) $a \leqslant b$ implies $b \in a \vee b$ and $a \in a \wedge b$,

(SL6) if $a \in a \wedge b$ or $b \in a \vee b$ then $a \leqslant b$.

Hyperstructures have many applications to several sectors of both pure and applied sciences. A short review of the theory of hyperstructures appear in [5]. In [6] a wealth of applications can be found, too. There are applications to the following subjects: geometry, hypergraphs, binary relations, lattices, fuzzy set and rough sets, automata, cryptography, combinatorics, codes, artificial intelligence and probabilities.

It is well know, the class of MV-algebras, BL-algebras, and Heyting algebras are proper subclass of the class of residuated lattices. In this paper, as an application of hyperstructures to residuated lattices, we introduce the notion of a hyper residuated lattice. We define the concepts of (weak) filter and (weak) deductive system, and verify their properties, as mentioned in the abstract. In fact, we want to construct a hyper structure, which is more general than hyper MV-algebra and hyper K-algebra.

2. Hyper residuated lattices

Throughout this paper, L will denote a hyper residuated lattice, unless otherwise stated.

Let $(X, \leqslant)$ be a partially ordered set and A, B be two subsets of X. Then we write

- $A \ll B$, if there exist $a \in A$ and $b \in B$ such that $a \leqslant b$.
- $A \leqslant B$ if for any $a \in A$, there exists $b \in B$ such that $a \leqslant b$.

Definition 2.1. [13] By a *hyper residuated lattice* we mean a non-empty set L endowed with four binary hyperoperations $\vee$, $\wedge$, $\odot$, $\rightarrow$ and two constants 0 and 1 satisfying the following conditions:

(HRL1) $(L, \leq, \vee, \wedge, 0, 1)$ is a bounded superlattice,

(HRL2) $(L, \odot, 1)$ is a commutative semihypergroup with 1 as the identity,

(HRL3) $a \odot c \ll b$ if and only if $c \ll a \rightarrow b$.

L is called *nontrivial* if $0 \neq 1$. An element $a \in L$ is called *scalar* if $|a \odot x| = 1$, for all $x \in L$.

Example 2.2. (i) Let $S = [0, 1]$. Then S with the natural ordering is a partially ordered set. Define the hyperoperations $\vee$, $\wedge$, $\odot$, and $\rightarrow$ on S as follows:

$$a \odot b = a \wedge b = \min\{a, b\}, \qquad b \vee a = a \vee b = \begin{cases} S, & a = b, \\ S - \{a\}, & a < b, \\ S - \{b\}, & b < a \end{cases}$$

$$a \to b = \begin{cases} 1, & a \leqslant b, \\ b, & a > b. \end{cases}$$

Then, it is easy to check that $(S, \vee, \wedge, \odot, \to, 0, 1)$ satisfies the properties (HRL1) $-$(HRL3) and so is a hyper residuated lattice.

(ii) Let $L = [0, 1]$ and $\odot$, $\vee$ be the hyperoperations in (i). Define two hyperoperations $\wedge$ and $\to$ on L as follows:

$$a \wedge b = \{x \in L | x \leqslant a, x \leqslant b\}, \qquad a \to b = \begin{cases} \{1\}, & a \leqslant b, \\ [b, 1], & a > b. \end{cases}$$

It is not difficult to check that $(L, \vee, \wedge, \odot, \to, 0, 1)$ is a hyper residuated lattice.

(iii) Let $(L = \{0, a, b, 1\}, \leq)$ be a chain such that $0 < a < b < 1$. Define the hyperoperations $\vee$ and $\wedge$ on L as given in the tables 1 and 2:

Table 1

$\vee$	0	a	b	1
0	{0,a,b,1}	{a,b,1}	{b,1}	{1}
a	{a,b,1}	{a,1,b}	{b,1}	{1}
b	{b,1}	{b,1}	{b,1}	{1}
1	{1,0}	{1}	{1}	{1}

Table 2

$\wedge$	0	a	b	1
0	{0}	{0}	{0}	{0}
a	{0}	{0,a}	{0,a}	{0,a}
b	{0}	{0,a}	{0,b,a}	{0,b,a}
1	{0}	{0,a}	{0,b,a}	{0,a,b,1}

Then $(L, \vee, \wedge, 0, 1)$ is a bounded hypper lattice. Let $x \odot y = \wedge$ and define the hyperoperations $\to$ and $\rightsquigarrow$ on L as given in the tables 3 and 4.

Table 3

$\to$	0	a	b	1
0	{1}	{1}	{1}	{1}
a	{a,b,1}	{1,a}	{1}	{1}
b	{a,1}	{a}	{b,1}	{1}
1	{0,1}	{a}	{1,b}	{1}

Table 4

$\rightsquigarrow$	0	a	b	1
0	{1}	{1,b}	{1,b}	{1,b}
a	{a,b,1}	{1}	{1}	{1}
b	{a,b,1}	{a}	{1,b}	{1,b}
1	{0,a,1}	{1,a}	{1}	{1}

Routine calculations show that $(L, \vee, \wedge, \odot, \to, 0, 1)$ and $(L, \vee, \wedge, \odot, \rightsquigarrow, 0, 1)$ are hyper residuated lattices. $\square$

Proposition 2.3. *In any hyper residuated lattice L, for all $x, y, z \in L$ and $A, B, C \subseteq L$, the following hold:*

(1) $1 \ll A$ *implies* $1 \in A$*, for all non-empty subsets A of L,*

(2) $x \leqslant y$ *implies* $1 \in x \to y$*, and if* 1 *is a scalar, the converse hold,*

(3) $1 \in x \to x$*,* $1 \in x \to 1$*,* $1 \in 0 \to x$*, if* 1 *is a scalar,* $x \in 1 \to x$*,*

(4) $A \ll B \to C$ *if and only if* $A \odot B \ll C$ *if and only if* $B \ll A \to C$*,*

(5) $0 \in x \odot 0$*,* $x \ll \neg\neg x$*, where* $\neg x = x \to 0$*,*

(6) $x \odot (x \to y) \ll y$*,* $x \odot (x \to y) \ll x$*,*

(7) $x \ll y \to (x \odot y)$,

(8) $x \odot y \ll x$, $x \odot y \ll y$. *Particularly,* $0 \in x \odot 0$,

(9) $A \odot B \ll A$, $A \odot B \ll B$,

(10) $A \ll x \ll B$ *implies* $A \ll B$. *Moreover, if* $A \cap B \neq \emptyset$, *then* $A \ll B$ *and* $B \ll A$.

(11) $x \leqslant y$ *implies* $x \odot z \ll y \odot z$,

(12) $x \leqslant y$ *implies* $z \to x \ll z \to y$,

(13) $x \leqslant y$ *and* $x \leqslant z$ *imply* $x \ll y \wedge z$,

(14) $y \leqslant x$ *and* $z \leqslant x$ *imply* $y \vee z \ll x$,

(15) $x \to y \subseteq \{u \,|\, u \odot x \ll y\}$,

(16) $x \leqslant y$ *implies* $y \to z \ll x \to z$,

(17) *If* y' *is a scalar of* L, *then* $(x \to y') \odot (y' \to z) \ll x \to z$,

(18) $x \to (y \to z) \ll (x \odot y) \to z$,

(19) $(x \odot y) \to z \ll x \to (y \to z)$.

Proof. The proofs of (3) – (7), (9), (11), (14), (15) and (19) are straightforward.

(1). If $A \subseteq L$ is such that $1 \ll A$, then $1 \ll a$, for some $a \in A$ whence $1 = a \in A$.

(2). Assume that $a \leqslant b$. From $a \in a \odot 1$ it follows that $a \odot 1 \ll b$ whence $1 \ll a \to b$. Thus, $1 \in a \to b$, by (1). Conversely, if 1 is a scalar, $1 \in a \to b$ implies that $\{a\} = a \odot 1 \ll b$, i.e., $a \leqslant b$.

(8). Since, $y \leqslant 1 \in x \to x$, so $x \odot y \ll x$. Similarly, it follows that $x \odot y \ll y$.

(10). Assume $A \ll x$ and $x \ll B$. Then $a \ll x$ and $x \ll b$, for some $a \in A$ and $b \in B$, whence $a \leqslant b$, i.e., $A \ll B$. The proof of other part is easy.

(12). Let $x \leqslant y$. Since, $z \odot (z \to x) \ll x$, by (6), $z \odot (z \to x) \ll y$ and so $z \to x \ll z \to y$.

(13). From $x \leqslant a$ and $x \leqslant b$ it follows that $x \in x \wedge a$ and $x \in x \wedge b$ whence $x \in x \wedge b \subseteq (x \wedge a) \wedge b = x \wedge (a \wedge b)$. Hence, there exists $u \in a \wedge b$ such that $x \in x \wedge u$ and so $x \leqslant u$ means that $x \ll a \wedge b$.

(16). Let $x \leqslant y$ and $z \in L$. By (15), we have

$$\begin{aligned} y \to z &\subseteq \{u \in L \,|\, y \odot u \ll z\} = \{u \in L \,|\, y \ll u \to z\} \subseteq \{u \in L \,|\, x \ll u \to z\} \\ &= \{u \in L \,|\, u \ll x \to z\}, \end{aligned}$$

whence $y \to z \ll x \to z$.

(17). Let y' be a scalar element of L, $u \in x \to y'$ and $v \in y' \to z$. Then $u \ll x \to y'$ and so $u \odot x \ll y'$. By a similar way, $v \odot y' \ll z$. Hence there exists

$a \in u \odot x$ such that $a \leqslant y'$ and so by (11), $a \odot v \ll y' \odot v$. Hence $v \odot (u \odot x) \ll v \odot y'$. Since $v \odot y' \ll z$ and $|v \odot y'| = 1$, then we get that $(v \odot u) \odot x = v \odot (u \odot x) \ll z$. Hence there exists $b \in u \odot v$ such that $x \odot b \ll z$ and so $b \ll x \to z$. Since $b \in u \odot v \subseteq (x \to y') \odot (y' \to z)$, then $(x \to y') \odot (y' \to z) \ll x \to z$.

(18). Let $u \in x \to (y \to z)$. Then there exists $a \in y \to z$ such that $u \in x \to a$. Then we get that

$$\begin{aligned} u \ll x \to a &\Rightarrow u \odot x \ll a \\ &\Rightarrow u \odot x \ll y \to z, \\ &\Rightarrow (u \odot x) \odot y \ll z, \qquad \text{by (4)}, \\ &\Rightarrow u \odot (x \odot y) \ll z, \\ &\Rightarrow u \ll (x \odot y) \to z, \qquad \text{by (4)}. \end{aligned}$$

Hence, $x \to (y \to z) \ll (x \odot y) \to z$. □

The next theorem shows that if there exists a hyper residuated lattice of order n, then there exists a hyper residuated lattice of order $n+1$.

Theorem 2.4. *Each hyper residuated lattice of order n can be extend to a hyper residuated lattice of order $n+1$, for any $n \in \mathbb{N}$.*

Proof. Let L be a hyper residuated lattice of order n, for $n \in \mathbb{N}$ and $e \notin L$. Set $\overline{L} = L \cup \{e\}$ and define a relation $\leqslant'$ on $\overline{L}$ by

$$\begin{aligned} z &\leqslant' y \quad \Leftrightarrow z \leqslant y, \text{ for all } z, y \in L, \\ x &\leqslant' e \quad \text{for all } x \in L'. \end{aligned}$$

Then $(\overline{L}, \leqslant')$ is a poset and 0 and e are the minimum and the maximum elements of $\overline{L}$, respectively. We define the binary hyperoperations $\vee', \wedge', \odot'$ and $\to'$ on $\overline{L}$ by

$$a \vee' b = \begin{cases} a \vee b & \text{if } a, b \in L, \\ \{e\} & \text{if } a = e \text{ or } b = e. \end{cases} \qquad a \to' b = \begin{cases} (a \to b) \cup \{e\} & \text{if } a, b \in L, 1 \in a \to b, \\ a \to b & \text{if } a, b \in L, 1 \notin a \to b, \\ \{e\} & \text{if } b = e, \\ \{b\} & \text{if } a = e. \end{cases}$$

$$a \odot' b = \begin{cases} a \odot b & \text{if } a, b \in L, \\ \{a\} & \text{if } a \in L \text{ and } b = e, \\ \{b\} & \text{if } b \in L \text{ and } a = e, \\ \{e\} & \text{if } a = b = e. \end{cases} \qquad a \wedge' b = \begin{cases} a \wedge b & \text{if } a, b \in L, \\ \{b\} & \text{if } b \in L \text{ and } a = e, \\ \{a\} & \text{if } a \in L \text{ and } b = e, \\ \{e\} & \text{if } a = b = e. \end{cases}$$

Routine calculation shows that (HRL1) and (HRL2) hold. We shall prove (HRL3). Let $x, y, z \in \overline{L}$.

(1). Let $x, y, z \in L$ and $1 \notin y \to z$. Then by definitions of $\odot'$ and $\leqslant'$, we get

$$x \odot' y \ll' z \Leftrightarrow x \odot y \ll z \Leftrightarrow x \ll y \to z \Leftrightarrow x \ll' y \to' z.$$

(2). Let $x, y, z \in L$ and $1 \in y \to z$. If $x \odot' y \ll' z$, then by definition of $\to'$, $e \in y \to' z$ and so $x \ll' y \to' z$. Now, let $x \ll' y \to' z$. Since $1 \in y \to z$, then $x \ll y \to z$ and so $x \odot y \ll z$. Hence $x \odot' y = x \odot y \ll' z$.

(3). Let $x, y \in L$ and $z = e$. Since $y \to' z = \{e\}$ and $u \ll' e$, for all $u \in L'$, then $x \odot' y \ll' z$ implies $x \ll' y \to' z$. Now, let $x \ll' y \to' z$. Since $z = e$, then clearly, $x \odot' y \ll' z$.

(4). Let $x, z \in L$ and $y = e$. Then $x \odot' y = \{x\}$ and $y \to' z = \{z\}$. Therefore, $x \odot' y \ll' z$ if and only if $x \ll' y \to' z$.

(5). Let $y, z \in L$ and $x = e$. Then $x \odot' y = \{y\}$. If $x \odot' y = \{y\} \ll' z$, then $y \ll' z$. Since $y, z \in L$ we get $y \ll z$ and so $1 \in y \to z$. Hence $e \in y \to' z$ and so $x \ll' y \to' z$. Now, let $x \ll' y \to' z$. Then by definition of $\leq'$, we have $e \in y \to' z$ and so $1 \in y \to z$ or $z = e$. Since $y \in L$, then $y \neq e$ and so $1 \in y \to z$. Therefore, $x \odot' y \ll' z$.

(6). Let $x = y = e$ and $z \in L$. Then $x \odot' y = \{e\}$ and $y \to' z = \{z\}$. Hence $x \odot' y = \{e\} \ll' z$ and $x \ll' y \to' z = \{z\}$ are impossible.

(7). Let $x = z = e$ and $y \in L$. Then $x \odot' y = \{y\}$ and $y \to' z = \{e\}$. Therefore, $x \odot' y \ll' z$ if and only if $x \ll' y \to' z$.

An analogous result holds for $y = z = e$.

(8). For $x = y = z = e$, it is obvious.

Therefore, $(\overline{L}, \vee', \wedge', \odot', \to', 0, e)$ is a hyper residuated lattice of order $n+1$. $\square$

Corollary 2.5. *For any $n \geqslant 4$ and $n \in \mathbb{N}$, there exists at least one hyper residuated lattice of order n.*

Proof. By Example 2.2 and Theorem 2.4, the proof is clear. $\square$

3. (Weak) Filters and deductive systems

In this section, we introduce the concepts of (weak) filters and (weak) deductive systems in hyper residuated lattices and we give some related results. Then we introduced special kinds of weak deductive systems in hyper residuated lattices and verify the relation between them.

Definition 3.1. [13] Let F be a non-empty subset of L satisfying

(F) $x \leqslant y$ and $x \in F$ imply $y \in F$.

then F is called a

- *filter* if $x \odot y \subseteq F$, for all $x, y \in F$,
- *weak filter* if $F \ll x \odot y$, for all $x, y \in F$.

A filter F of L is said to be *proper* if $F \neq L$ and this is equivalent to that $0 \notin F$

Remark 3.2. Clearly, any filter is a weak filter. Moreover, $1 \in F$, for any (weak) filter F of L.

Example 3.3. In any hyper residuated lattice L, $\{1\}$ is a weak filter and L is a filter of L. Of course, in Example 2.2(i), $\{1\}$ is a filter and in Example 2.2(iii), $\{a, b, 1\}$ and $\{b, 1\}$ are weak filters of L. But, $\{1, b\}$ is not a filter. □

The next theorem gives an equivalent condition for weak filters.

Theorem 3.4. A non-empty subset F of L is a weak filter if and only if it satisfies (F) and $(x \odot y) \cap F \neq \emptyset$, for all $x, y \in F$.

Proof. Straightforward. □

Definition 3.5. Let D be a non-empty subset of L. D is called a

- *deductive system* if for all $x, y \in L$,

  (DS) $1 \in D$,

  (HDS) $x \in D$ and $x \to y \subseteq D$ imply $y \in D$,

- *weak deductive system* if (DS) holds and for all $x, y \in L$,

  (WHDS) $x \in D$ and $D \ll x \to y$ imply $y \in D$.

A deductive system D is said to be proper if $D \neq L$.

Example 3.6. In Example 2.2(ii), for any $a \in (0, 1]$, $D = [a, 1]$ is a deductive system of L, which is not a weak deductive system of L, since $[a, 1] \ll a \to y$, for any $y \leqslant a$ and $y \notin [a, 1]$). Moreover, in Example 2.2(i), for any $a \in S$, $D = [a, 1]$ is a weak deductive system of S. □

Proposition 3.7. *Let L be a hyper residuated lattice. Then*

(i) *every weak deductive system satisfies (F);*

(ii) *if D is a non-empty subset of L satisfying (F), then D is a weak deductive system of L if and only if $(x \to y) \cap D \neq \emptyset$ and $x \in D$ imply $y \in D$.*

Proof. (i). Let F be a weak hyper deductive system of L, $x \leqslant y$ and $x \in F$, for $x, y \in L$. Then by Proposition 2.3(2), $1 \in x \to y$, and so $F \ll x \to y$. Now, from (WHDS) it follows that $y \in F$. Thus, (F) holds.

(ii). ($\Rightarrow$) It follows from Proposition 2.3,(10).

($\Leftarrow$) Let D be a non-empty subset of L satisfying the given conditions. Obviously, $1 \in D$. Now, let $x \in D$ and $D \ll x \to y$. Then there exist $d \in D$ and $u \in x \to y$ such that $d \leqslant u$ and so by (F), $u \in D$. Hence $D \cap (x \to y) \neq \emptyset$ and so $y \in D$. Therefore, D is a weak hyper deductive system of L. □

Now, we give the connection between (weak) filters and (weak) deductive systems.

Theorem 3.8. *Let L be a hyper residuated lattice. Then*

(i) *every weak deductive system is a weak filter,*

(ii) *every filter is a deductive system.*

Proof. (i). Let F be a weak deductive system of L. Then by Proposition 3.7(i), (F) holds. Now, let $x, y \in F$. By Proposition 2.3(7), $y \ll x \to (x \odot y)$ and so $y \leqslant u$, for some $u \in x \to (x \odot y)$. Hence $u \in F$. But $u \in x \to (x \odot y)$ implies that $u \in x \to v$, for some $v \in x \odot y$, and hence $F \ll x \to v$. Since, $x \in F$, so $v \in F$ and hence, $F \ll x \odot y$.

(ii). Assume that F is a filter of L. Since, F is non-empty, then there exists $x \in L$ such that $x \in F$. From $x \ll 1$ and (F), it follows that $1 \in F$. Thus, (DS) holds. Now, let $x \in F$ and $x \to y \subseteq F$, for $x, y \in L$. Then, $x \odot (x \to y) = \cup_{u \in x \to y} x \odot u \subseteq F$. On the other hand, from Proposition 2.3(6), we know that $x \odot (x \to y) \ll y$. Hence, there exists $v \in x \odot (x \to y)$ such that $v \leqslant y$, and since $v \in F$, so $y \in F$. $\square$

Example 3.9. Consider the residuated lattice L given in the Example 2.2(iii). It is not difficult to check that $F = \{b, 1\}$ is a weak filter of L but it is not a weak deductive system. Because $F \ll \{a, b\} = b \rightsquigarrow 0$, $b \in F$ while $0 \notin F$. $\square$

Definition 3.10. A non-empty subset A of L is said to be

- $S_{\odot}$-*reflexive* if $(x \odot y) \cap A \neq \emptyset$ implies $x \odot y \subseteq A$, for all $x, y \in L$,
- $S_{\to}$-*reflexive* if $(x \to y) \cap A \neq \emptyset$ implies $x \to y \subseteq A$, for all $x, y \in L$.

Clearly, any $S_{\odot}$-reflexive weak filter of L is a filter.

Example 3.11. (i) Let $(L, \vee, \wedge, \odot, \to, 0, 1)$ be the hyper residuated lattice in Example 2.2(iii). Then $A = \{0\}$ is a $S_{\to}$-reflexive subset of $(L, \vee, \wedge, \odot, \to, 0, 1)$.

(ii) Let $(L; \leq, \vee, \wedge, 0, 1)$ be the bounded super lattice defined in Example 2.2(iii). Consider the following tables:

Table 5

$\odot$	0	a	b	1
0	{0}	{0}	{0}	{0}
a	{0}	{a,0}	{a}	{a}
b	{0}	{a}	{b}	{b}
1	{0}	{a}	{b}	{1}

Table 6

$\to$	0	a	b	1
0	{1}	{1}	{1}	{1}
a	{0,a}	{1}	{1}	{1}
b	{0}	{0,a}	{1}	{1}
1	{0}	{a}	{b}	{1}

It is not difficult to check that $(L, \vee, \wedge, \odot, \to, 0, 1)$ is a hyper residuated lattice. Let $F_1 = \{1\}, F_2 = \{1, b\}$. Then F_1 and F_2 are $S_{\odot}$-reflexive (weak) filters of L and F_1 is a $S_{\to}$-reflexive deductive system of L. $\square$

Theorem 3.12. *Every $S_{\odot}$-reflexive weak filter is a weak deductive system.*

Proof. Let F be an $S_{\odot}$-reflexive weak filter of L. Obviously $1 \in F$. Now, let $x, y \in L$ be such that $x \in F$ and $F \ll x \to y$. Then there exist $a \in F$ and $b \in x \to y$ such that $a \leqslant b$. Hence $b \in F$ and so by Theorem 3.4, $(x \odot b) \cap F \neq \emptyset$. Since F is $S_{\odot}$-reflexive, we get $x \odot b \subseteq F$. From $b \in x \to y$ it follows that $b \odot x \ll y$ and so $u \leqslant y$, for some $u \in b \odot x$. Since $x \odot b \subseteq F$, then $u \in F$ whence $y \in F$. Therefore, F is a weak deductive system of L. $\square$

Theorem 3.13. *Every $S_{\to}$-reflexive deductive system is a filter.*

Proof. Let D be a $S_{\to}$-reflexive deductive system, $x \in D$ and $x \leqslant y$, for some $y \in L$. By Proposition 2.3(2), $1 \in x \to y$ and so $(x \to y) \cap D \neq \emptyset$. Since D is a $S_{\to}$-reflexive, we get $x \to y \subseteq D$ whence $y \in D$. Hence D satisfies (F). Now, let $x, y \in D$. If $u \in x \odot y$, then $x \odot y \ll u$ and so $x \ll y \to u$. From $x \in D$ it follows that $D \ll y \to u$ and so $D \cap (y \to u) \neq \emptyset$. Since D is $S_{\to}$-reflexive, then $y \to u \subseteq D$ whence $u \in D$. Hence, $x \odot y \subseteq D$ means that D is a filter of L. □

Proposition 3.14. *Let $\{F_i \mid i \in I\}$ be a family of non-empty subsets of L.*

(i) *If F_i is a filter (deductive system, weak deductive system), for all $i \in I$, then $\cap F_i$ is a filter (deductive system, weak deductive system) of L.*

(ii) *Assume that $\{F_i \mid i \in I\}$ be a chain. If F_i is a filter (weak filter, weak deductive system), for all $i \in I$, then $\cup F_i$ is a filter (weak filter, weak deductive system) of L.*

Proof. We only prove the case of weak deductive systems. The proof of the other cases is easy.

(i). Assume that F_i is a weak deductive system of L, for all $i \in I$. Clearly, $1 \in \cap F_i$. Let $x \in \cap F_i$ and $\cap F_i \ll x \to y$, for some $y \in L$. Then $x \in F_i$ and $F_i \ll x \to y$, for all $i \in I$. Hence $y \in F_i$, for all $i \in I$ and so $y \in \cap F_i$. Therefore, $\cap F_i$ is a weak deductive system of L.

(ii). Let $\{F_i \mid i \in I\}$ be a chain of weak deductive systems of L. Clearly, $1 \in \cup F_i$. Let $x \in \cup F_i$ and $\cup F_i \ll x \to y$, for some $y \in L$. Then, there exist $j, k \in I$ such that $x \in F_j$ and $F_k \ll x \to y$. Since F_i's forms a chain, so we can assume that $F_j \subseteq F_k$. Thus, $F_k \ll x \to y$ and $x \in F_k$ imply that $y \in F_k \subseteq \cup F_i$ proving $\cup F_i$ is a weak deductive system of L. □

The next example shows that Proposition 3.14(ii) may not be true for deductive systems, in general.

Example 3.15. Let $L = \{x_i \mid i \in \mathbb{N}\} \cup \{0, 1\}$ be a lattice, whose Hasse diagram is below (see Figure 1).

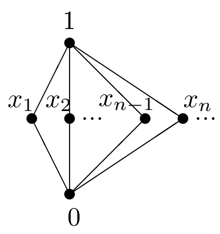


Figure 1: The Hasse diagram of L

Define binary hyperoperations $\vee, \wedge, \odot$ and $\rightarrow$ on L as follows:

$$a \vee b = \{c \in L \mid a \leqslant c \text{ and } b \leqslant c\}, \qquad a \wedge b = \{c \in L \mid c \leqslant a \text{ and } c \leq b\}$$

$a \odot b = a \wedge b$ and

$$a \rightarrow b = \begin{cases} \{1\} & \text{if } a \leqslant b, \\ \{x_i \mid i \in \mathbb{N}\} & \text{if } a = 1,\ b \in L - \{1\}. \\ \{x_j \mid j \in \mathbb{N}, j \leqslant i\} \cup \{1\} & \text{if } a, b \in \{x_i \mid i \in \mathbb{N}\},\ a = x_i,\ a \neq b, \\ \{x_j \mid j \in \mathbb{N}, j \leqslant i\} \cup \{1\} & \text{if } a \in \{x_i \mid i \in \mathbb{N}\},\ b = 0 \end{cases}$$

for all $a, b \in L$. Routine calculations show that $(L, \vee, \wedge, \odot, \rightarrow, 0, 1)$ is a hyper residuated lattice. Let $D_i = \{1, x_1, \ldots, x_i\}$, for all $i \in \mathbb{N}$. It is easy to verify that D_i is a deductive system of L and $D_i \subseteq D_{i+1}$, for all $i \in \mathbb{N}$. But, $1 \in \cup_{i \in I} D_i$, $1 \rightarrow 0 = \{x_i \mid i \in \mathbb{N}\} \subseteq \cup_{i \in I} D_i$ and $0 \notin \cup_{i \in I} D_i$. Therefore, $\cup_{i \in I} D_i$ is not a deductive system of L. $\square$

Definition 3.16. Let F be a proper (weak) filter of L. Then F is said to be *maximal* if $F \subseteq J \subseteq L$, implies $F = J$ or $J = L$, for all (weak) filters J of L.

Maximal (weak) deductive systems are defined analogously.

Example 3.17. Let $(L, \vee, \wedge, \odot, \rightarrow, 0, 1)$ be the hyper residuated lattice defined in the Example 3.11. Then $F = \{1, b\}$ is a maximal filter and $\{1, a, b\}$ is a maximal weak filter of L. $\square$

Theorem 3.18. *In a hyper residuated lattice*

(i) *every proper* (*weak*) *filter of* L *is contained in a maximal* (*weak*) *filter of* L,

(ii) *every proper weak deductive system of* L *is contained in a maximal weak deductive system of* L.

Proof. (i). Let F be a proper (weak) filter of L and S be the collection of all proper (weak) filters of L containing F. Then $F \in S$ and $(S, \subseteq)$ is a poset. Let $\{F_i \mid i \in I\}$ be a chain in S. Then by Proposition 3.14(ii), $\cup F_i$ is a (weak) filter of L containing F. If $0 \in \cup F_i$, then there exists $i \in I$ such that $0 \in F_i$, which is impossible. Hence $\cup F_i$ is a proper (weak) filter of L containing F and so $\cup F_i \in S$. Hence any chain of elements of S has an upper bound in S. By Zorn's lemma, S has a maximal element such as M. We show that M is a maximal (weak) filter of L. Let $M \subseteq J \subseteq L$, for some (weak) filter J of L. If $J \neq L$, then $J \in S$. Since M is a maximal element of S we get $M = J$. Therefore, M is a maximal (weak) filter of L.

(ii). Similar to (i). $\square$

From the fact that $\{1\}$ is a weak filter of any hyper residuated lattice, we conclude that

Corollary 3.19. *Every nontrivial hyper residuated lattice has a maximal weak hyper filter.*

4. (Positive) Implicative weak deductive systems

Definition 4.1. Let $(L, \vee, \wedge, \odot, \rightarrow, 0, 1)$ be a hyper residuated lattice and D be a non-empty subset of L containing 1. Then D is called

- *an implicative weak deductive system* or simply $IWDS$ if for all $x, y, z \in L$

  $x \rightarrow (y \rightarrow z) \cap D \neq \emptyset$ and $x \rightarrow y \cap D \neq \emptyset$ imply $x \rightarrow z \cap D \neq \emptyset$,

- *a positive implicative weak deductive system* or simply $PIWDS$ if

  $x \rightarrow ((y \rightarrow z) \rightarrow y)) \cap D \neq \emptyset$ and $x \in D$ imply $y \in D$, for all $x, y, z \in L$.

Note: Clearly, if L is a residuated lattice, then the concept of implicative (positive implicative) filters are coincide by the concept of implicative (positive implicative) weak deductive systems.

Example 4.2. Let $L = \{a, b, c, 0, 1\}$ be a partially ordered set whose Hasse diagram depicted in Figure 2.

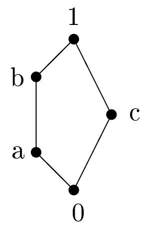


Figure 2: The Hasse diagram of L

Let $x \wedge y = \{u \in L \,|\, u \leqslant x, u \leqslant y\}$ and $x \vee y = \{u \in L \,|\, x \leqslant u, y \leqslant u\}$, for all $x, y \in L$. Now, consider the following tables:

Table 7

$\rightarrow$	0	a	b	c	1
0	{1}	{1}	{1}	{1}	{1}
a	{c}	{1}	{1}	{c}	{1}
b	{c}	{a,b,c}	{1}	{c}	{1}
c	{a,b}	{a,b}	{b,a}	{1}	{1}
1	{0}	{a}	{b,a}	{c}	{1}

Table 8

$\odot$	0	a	b	c	1
0	{0}	{0}	{0}	{0}	{0}
a	{0}	{a}	{a}	{0}	{a}
b	{0}	{a}	{b,a}	{0}	{a,b}
c	{0}	{0}	{0}	{c}	{c}
1	{0}	{a}	{b,a}	{c}	{1}

It is easy to show that $(L, \vee, \wedge, \odot, \rightarrow, 0, 1)$ is a hyper residuated lattice. Moreover, easy calculations show that

(i) $\{1, a\}$, and $\{1, a, b\}$ are implicative weak deductive systems.

(ii) $\{1, a\}$ is not a positive implicative weak deductive systems (since $1 \in 1 \rightarrow (\{a, c\} \rightarrow b) \subseteq 1 \rightarrow ((b \rightarrow a) \rightarrow b)$ and $b \notin \{1, a\}$).

(iii) $\{1, a, b\}$ is a positive implicative weak deductive system. $\square$

Lemma 4.3. *Let $(L, \vee, \wedge, \odot, \rightarrow, 0, 1)$ be a hyper residuated lattice. Then L satisfies the following conditions: for all $a, b, c \in L$,*

(i) $a \rightarrow (b \rightarrow c) \leqslant b \rightarrow (a \rightarrow c)$,

(ii) $x \leqslant y$ *implies* $z \rightarrow x \leqslant z \rightarrow y$,

(iii) $a \rightarrow b \leqslant (b \rightarrow c) \rightarrow (a \rightarrow c)$.

Proof. (i). Let u be an arbitrary element of $a \rightarrow (b \rightarrow c)$. Then $u \ll (a \rightarrow (b \rightarrow c))$ and so $u \ll a \rightarrow x$, for some $x \in b \rightarrow c$. Hence $u \odot a \ll x$ and so $y \ll x$, for some $y \in u \odot a$. Since $x \in b \rightarrow c$, then we get $y \ll b \rightarrow c$ and so $y \odot b \ll c$. Hence $(u \odot b) \odot a = (u \odot a) \odot b \ll c$ and by Proposition 2.3(4), we get $u \odot b \ll a \rightarrow c$. Therefore, by Proposition 2.3(4), $u \ll b \rightarrow (a \rightarrow c)$ and so $a \rightarrow (b \rightarrow c) \leqslant b \rightarrow (a \rightarrow c)$.

(ii). Let $u \in z \rightarrow x$. Then $u \ll z \rightarrow x$, so $u \odot z \ll x$. Since $x \leqslant y$, then we get $u \odot z \ll y$ and so $u \ll z \rightarrow y$. Therefore, $z \rightarrow x \leqslant z \rightarrow y$.

(iii). We know that $(b \rightarrow c) \rightarrow (a \rightarrow c) \subseteq \cup\{u \rightarrow v | u \in b \rightarrow c, \text{ and } v \in a \rightarrow c\}$. Let $u \in b \rightarrow c$. Then $u \ll b \rightarrow c$. Thus $u \odot b \ll c$. Hence $b \ll u \rightarrow c$ and so there exists $t \in u \rightarrow c$ such that $b \leqslant t$. Now, by (i) and (ii), we get $a \rightarrow b \leqslant a \rightarrow t \subseteq (a \rightarrow (u \rightarrow c)) \leqslant u \rightarrow (a \rightarrow c)$. Since $u \in b \rightarrow c$, we conclude that $a \rightarrow b \leqslant (b \rightarrow c) \rightarrow (a \rightarrow c)$. □

Note that, in the proof of Lemma 4.3(iii) we proved that $a \rightarrow b \leqslant u \rightarrow (a \rightarrow x)$, for all $u \in b \rightarrow x$.

From now on, in this section, $(L, \vee, \wedge, \odot, \rightarrow, 0, 1)$ or simply L will denote a hyper residuated lattice satisfies $1 \odot x = \{x\}$, for all $x \in L$, unless otherwise stated.

Proposition 4.4. *Let D be a non-empty subset of L. Then*

(i) *for all $x \in L$, $x \in 1 \rightarrow x$ and x is a maximum element of $1 \rightarrow x$,*

(ii) *if D is a $PIWDS$ of L, then D is a weak deductive system,*

(iii) *if D is an $IWDS$ of L is an upset, then D is a weak deductive system.*

Proof. (i). Let $x \in L$. For any $u \in 1 \rightarrow x$, we have $u \ll 1 \rightarrow x$ and so $\{u\} = 1 \odot u \ll x$. Since $x \in 1 \odot x$, then we get $1 \odot x \ll x$. It follows that $x \ll 1 \rightarrow x$. Hence there exists $u \in 1 \rightarrow x$ such that $x \leqslant u$. So, $x \leqslant u \leqslant x$. Therefore, $x \in 1 \rightarrow x$.

(ii). Assume that D is a $PIWDS$ of L. Clearly, (DS) holds. Let $(x \rightarrow y) \cap D \neq \emptyset$ and $x \in D$. Then by Proposition 2.3(3), we have $x \rightarrow (1 \rightarrow y) \subseteq x \rightarrow ((y \rightarrow 1) \rightarrow y)$. Now, by (i) we get $x \rightarrow y \subseteq x \rightarrow (1 \rightarrow y)$ and so $(x \rightarrow ((y \rightarrow 1) \rightarrow y)) \cap D \neq \emptyset$. Since $x \in D$ and D is a positive implicative weak deductive system of L, we conclude that $y \in D$. Therefore, D is a weak deductive system of L.

(iii). Assume that D is an $IWDS$ of L. Clearly, (DS) holds. Let $(x \rightarrow y) \cap D \neq \emptyset$ and $x \in D$. Then by (i), $(1 \rightarrow (x \rightarrow y)) \cap D \neq \emptyset$ and $(1 \rightarrow x) \cap D \neq \emptyset$. Since D

is an implicative weak deductive system of L, then $(1 \to y) \cap D \neq \emptyset$. Since by (i) y is a maximum element of $1 \to y$ and D is an upset, then we get $y \in D$. $\square$

Theorem 4.5. *Let D be a non-empty subset of L. Then*

(i) *D is a $PIWDS$ of L if and only if D is a weak deductive system such that $((x \to y) \to x) \cap D \neq \emptyset$ implies $x \in D$, for all $x, y \in L$,*

(ii) *D is an $IWDS$ of L if and only if $D_x = \{u \in L \mid (x \to u) \cap D \neq \emptyset\}$ is a weak deductive system of L, for all $x \in L$.*

Proof. (i). Let D be a $PIWDS$. Then by Proposition 4.4(ii), D is a weak deductive system. Now, let and $((x \to y) \to x) \cap D \neq \emptyset$. Then there exists $u \in ((x \to y) \to x) \cap D$. By Proposition 4.4(i), $u \in 1 \to u \subseteq (1 \to ((x \to y) \to x)) \cap D$. Since $1 \in D$ and D is a $PIWDS$, then we get $x \in D$. Conversely, let D be a weak deductive system such that $((x \to y) \to x) \cap D \neq \emptyset$ implies $x \in D$, for all $x, y \in L$. Let $(x \to ((y \to z) \to y)) \cap D \neq \emptyset$ and $x \in D$. Since D is a weak deductive system and $x \in D$, then $((y \to z) \to y) \cap D \neq \emptyset$ and so $y \in D$. Therefore, D is a $PIWSD$.

(ii). Let D be an $IWDS$ of L and $x \in L$. By Proposition 2.3(3), $1 \in D_x$. Now, let $(a \to b) \cap D_x \neq \emptyset$ and $a \in D_x$, for some $a, b \in L$. Then $(x \to a) \cap D \neq \emptyset$ and $(x \to (a \to b)) \cap D \neq \emptyset$. Since D is an $IWDS$, we get $(x \to b) \cap D \neq \emptyset$ and so $b \in D_x$. Hence D_x is a weak deductive system. Conversely, let $D_x = \{u \in L | (x \to u) \cap D \neq \emptyset\}$ is a weak deductive system of L, for all $x \in L$. If $(x \to (y \to z)) \cap D \neq \emptyset$ and $(x \to y) \cap D \neq \emptyset$, for some $x, y, z \in L$, then $y \in D_x$ and $(y \to z) \cap D_x \neq \emptyset$. Since D_x is a weak deductive system of L, then we conclude that $z \in D_x$ and so $(x \to z) \cap D \neq \emptyset$. Therefore, D is an $IWDS$ of L. $\square$

Example 4.6. Let $P = \{1, 0, a, b\}$, $P' = \{1, 0, a, c\}$ and $\leqslant$ be the partially relation was defined in Example 4.2. Then $(P, \leqslant)$ and $(P', \leqslant)$ are two partially ordered sets. Consider the following tables.

Table 9

$\to$	0	a	b	1
0	{1}	{1}	{1}	{1}
a	{0}	{1,a}	{1}	{1}
b	{0}	{a}	{1,b}	{1}
1	{0}	{a}	{b,a}	{1}

Table 10

$\rightsquigarrow$	0	a	c	1
0	{1}	{1}	{1}	{1}
a	{c}	{1,c}	{c}	{1}
c	{a}	{a}	{1,a}	{1}
1	{0}	{a}	{c}	{1}

Easy calculations show that $(P, \vee, \wedge, \odot, \to 0, 1)$ and $(P', \vee, \wedge, \odot, \rightsquigarrow, 0, 1)$ are two hyper residuated lattices, where $\vee$, $\odot$ and $\wedge$ are the same as in L (Example 4.2) except restricted to P and P', respectively.

(i) Consider the hyper residuated lattice $(P, \vee, \wedge, \odot, \to 0, 1)$. If $D = \{1\}$, then $D_1 = \{1\}$, $D_a = \{1, a, b\}$, $D_b = \{1, b\}$ and $D_0 = P$. Since D_0, D_a, D_b and D_1 are weak deductive systems of $(P, \vee, \wedge, \odot, \to 0, 1)$, then by Theorem 4.5(ii), $\{1\}$ is an $IWDS$ of $(P, \vee, \wedge, \odot, \to 0, 1)$. Moreover, $a \notin \{1\}$ and $((a \to a) \to a) \cap \{1\} \neq \emptyset$. Hence by Theorem 4.5(i), $\{1\}$ is not $PIWDS$ of $(P, \vee, \wedge, \odot, \to 0, 1)$.

(ii) $\{1, a, b\}$ is a $PIWDS$ of P.

(iii) $\{1\}$ is a $PIWDS$ of $(P', \vee, \wedge, \odot, \rightsquigarrow, 0, 1)$. $\square$

Open Problem: *Is there a PIWDS which is not IWDS?*

Example 4.7. Let $(S, \vee, \wedge, \odot, \rightarrow, 0, 1)$ be the hyper residuated lattice in Example 2.2(ii). It is easy to show that $[a, 1]$ is a weak deductive system of S, for any $a \in [0, 1)$. Let $D = [a, 1]$. Then by definition of $\rightarrow$ we get

$$D_x = \begin{cases} [\text{x,1}] & \text{if } x \leqslant a, \\ D & \text{if } a \leqslant x \end{cases}$$

Hence D_x is a weak deductive system of S and so by Theorem 4.5(ii), D is an $IWDS$ of S. Now, let $D = (0, 1]$. Since $(0 \rightarrow y) \rightarrow 0 = 1 \rightarrow 0 = \{0\}$, for all $y \in [0, 1]$, then we get D is a $PIWDS$ of L. We show that $(0, 1]$ is the only proper $PIWDS$ of S. Let F be a $PIWDS$ of S. Then by Proposition 4.4 and Theorem 3.8, F is an upset. So $F = (a, 1]$ or $F = [a, 1]$, for some $a \in S - \{0\}$. Let $e, f \in (0, a)$ such that $f < e$. Then $(e \rightarrow f) \rightarrow e = f \rightarrow e = \{1\}$ and $((e \rightarrow f) \rightarrow e) \cap F \neq \emptyset$. Since $e \in S - F$, then by Theorem 4.5(i), D is not $PIWDS$ of S. □

Theorem 4.8. *Let D be a weak deductive system of L. Then the following are equivalent:*

(i) *D is an $IWDS$ of L,*

(ii) *$(y \rightarrow (y \rightarrow x)) \cap D \neq \emptyset$ implies $(y \rightarrow x) \cap D \neq \emptyset$, for all $x, y \in L$,*

(iii) *$(z \rightarrow (y \rightarrow (y \rightarrow x))) \cap D \neq \emptyset$ and $z \in D$ imply $(y \rightarrow x) \cap D \neq \emptyset$, for all $x, y \in L$,*

(iv) *$(x \rightarrow u) \cap D \neq \emptyset$ for any $x \in L$ and any $u \in x \odot x$.*

Proof. (i)$\Rightarrow$ (ii). Let D be an $IWDS$ of L and $(y \rightarrow (y \rightarrow x)) \cap D \neq \emptyset$. By Proposition 2.3(3), $(y \rightarrow y) \cap D \neq \emptyset$. Since D is an $IWDS$ of L, then $(y \rightarrow x) \cap D \neq \emptyset$.

(ii)$\Rightarrow$ (iii). Let (ii) holds, $(z \rightarrow (y \rightarrow (y \rightarrow x))) \cap D \neq \emptyset$ and $z \in D$. Since D is a weak deductive system, then $(y \rightarrow (y \rightarrow x)) \cap D \neq \emptyset$ and so $y \rightarrow x \in D$.

(iii)$\Rightarrow$ (i). Let (iii) holds, $(x \rightarrow (y \rightarrow z)) \cap D \neq \emptyset$ and $(x \rightarrow y) \cap D \neq \emptyset$. Since $x \rightarrow (y \rightarrow z) \leqslant y \rightarrow (x \rightarrow z)$ (by Lemma 4.3) and D is an upset (by Theorem 3.8), then we get there exists $u \in (y \rightarrow (x \rightarrow z)) \cap D$. Now,

$$\begin{aligned} u \ll y \rightarrow (x \rightarrow z) &\Rightarrow u \odot y \ll x \rightarrow z, \text{ by Proposition 2.3(4)} \\ &\Rightarrow y \ll u \rightarrow (x \rightarrow z), \text{ by Proposition 2.3(4)} \\ &\Rightarrow y \leqslant a, \text{ for some } a \in u \rightarrow (x \rightarrow z) \\ &\Rightarrow x \rightarrow y \leqslant x \rightarrow a, \text{ by Lemma 4.3(ii)} \\ &\Rightarrow x \rightarrow y \leqslant x \rightarrow (u \rightarrow (x \rightarrow z)) \\ &\Rightarrow (x \rightarrow (u \rightarrow (x \rightarrow z))) \cap D \neq \emptyset, \text{ since } x \rightarrow y \cap D \neq \emptyset \\ &\Rightarrow (u \rightarrow (x \rightarrow (x \rightarrow z))) \cap D \neq \emptyset, \text{ by Lemma 4.3(i).} \end{aligned}$$

Since $u \in D$, then by (iii), we conclude that $(x \to z) \cap D \neq \emptyset$. Therefore, D is an $IWDS$ of L.

(ii) $\Rightarrow$ (iv). Suppose that $x \in L$ and $u \in x \odot x$. Then $x \odot x \ll u$ and so $x \ll x \to u$. Hence by Proposition 2.3(3), $1 \in (x \to (x \to u)) \cap D$ and $1 \in (x \to x) \cap D$. Since D is an $IWDS$ of L, then $(x \to u) \cap D \neq \emptyset$.

(iv) $\Rightarrow$ (ii). Let $(y \to (y \to x)) \cap D \neq \emptyset$, for some $x, y \in L$. Then there exists $u \in (y \to (y \to x)) \cap D$. By Proposition 2.3(3), $1 \in u \to (y \to (y \to x))$ and so by Lemma 4.3(i), $1 \in y \to (y \to (u \to x))$. It follows that $1 \ll y \to (y \to t)$, for some $t \in u \to x$ and so $\{y\} = 1 \odot y \ll y \to t$. Hence $y \odot y \ll t$, whence $a \leqslant t$, for some $a \in y \odot y$. Since $y \to a \leqslant y \to t$, then by Lemma 4.3, we obtain $\emptyset \neq D \cap (y \to t) \subseteq y \to (u \to x) \leqslant u \to (y \to x)$. Since D is a weak deductive system of L by Theorem 3.8, $u \to (y \to x) \cap D \neq \emptyset$. Now, $u \in D$ implies $(y \to x) \cap D \neq \emptyset$. Therefore, D is an $IWDS$ of L. □

Theorem 4.9. *Let F and G be two weak deductive system of L such that $F \subseteq G$. If F is an $IWDS$ of L, then G is an $IWDS$ of L, too.*

Proof. It follows from Theorem 4.8. □

Corollary 4.10. *Any weak deductive systems of L is an $IWDS$ of L if and only if $\{1\}$ is an $IWDS$ of L, or equivalently, if and only if $x \leqslant u$, for any $u \in x \odot x$.*

Proof. (i). Let $(x \to y) \cap \{1\} \neq \emptyset$ and $x \in \{1\}$. Then $1 \ll 1 \to y$ and so $1 \odot 1 \ll y$. Since $1 \odot u = \{u\}$, for all $u \in L$, we get $1 \ll y$ and so $y = 1$. Hence $\{1\}$ is a weak deductive system of L, Now, by using of Theorem 4.9, we get $\{1\}$ is an $IWDS$ if and only if any weak deductive system of L is an $IWDS$ of L.

(ii). By Proposition 2.3(2), we have $x \leqslant y$ if and only if $1 \in x \to y$. Suppose that $\{1\}$ is an $IWDS$ of L. Then by Theorem 4.8, $1 \in x \to u$, for any $u \in x \odot x$ and so $x \leqslant u$, for any $u \in x^2$. Conversely, suppose that $x \leqslant u$, for all $u \in x^2$ and $(a \to (a \to b)) \cap \{1\} \neq \emptyset$, for some $a, b \in L$. Then $1 \in a \to (a \to b)$ and so by Proposition 2.3(4), $\{a\} = 1 \odot a \ll a \to b$. Hence $a \odot a \ll b$. By assumption we get $a \leqslant b$ and so $1 \in a \to b$. Therefore, $(a \to b) \cap \{1\} \neq \emptyset$ and so $\{1\}$ is an $IWDS$ of L. □

We note that, if $\{1\}$ is an $IWDS$ of L, then Corollary 4.10 and Proposition 2.3(8), imply $x \in x \odot x$, for all $x \in L$.

Theorem 4.11. *Let D be a weak deductive system of L. Then D is a maximal and implicative weak deductive system of L if and only if $x \to y \cap D \neq \emptyset$ and $y \to x \cap D \neq \emptyset$, for all $x, y \in L - D$.*

Proof. Suppose that D is a maximal and implicative weak deductive system and $x, y \in L - D$. By Proposition 2.3(3) and (8), we get that $x \in D_x$, $y \in D_y$, $D \subseteq D_x \subseteq L$ and $D \subseteq D_y \subseteq L$. Moreover, Theorem 4.5(ii) implies D_x and D_y are weak deductive systems of L. Hence by assumption $D_x = L = D_y$ and so $y \in D_x$, $x \in D_y$. Therefore, $x \to y \cap D \neq \emptyset$ and $y \to x \cap D \neq \emptyset$. Conversely, let D be a weak deductive system such that $x \to y \cap D \neq \emptyset$ and $y \to x \cap D \neq \emptyset$, for all $x, y \in L - D$. If there exists $a \in L$ such that D_a is not weak deductive systems of L, then there are $x, y \in L$ such that $x \to y \cap D_a \neq \emptyset$, $x \in D_a$ and $y \notin D_a$. Hence $a \to x \cap D \neq \emptyset$ and $a \to u \cap D \neq \emptyset$, for some $u \in x \to y$. But $a \to y \cap D = \emptyset$. From Proposition 2.3(8) and Theorem 3.8, we get that $y \notin D$. Hence by assumption $a \in D$. Since $a \to x \cap D \neq \emptyset$ and $a \to x \cap D \neq \emptyset$, then we get $x \in D$ and $u \in D$. It follows that $x \to y \cap D \neq \emptyset$. That is $y \in D$, which is contradiction. Hence D_a is a weak deductive system of L, for any $a \in L$. By Theorem 4.5(ii), D is an implicative deductive system. Now, we show that, D_a is the least weak deductive system of L containing $D \cup \{a\}$, for any $a \in L - D$. Let $a \in L - D$ and D' be a weak deductive system of L containing $D \cup \{a\}$ and u be an arbitrary element of D_a. Then $a \to u \cap D \neq \emptyset$ and so $a \to u \cap D' \neq \emptyset$. Since $a \in D'$, then $u \in D'$. Hence $D_a \subseteq D'$. That is D_a is the least weak deductive system of L containing $D \cup \{a\}$. Assume that $D \subsetneq E \subseteq L$, for some weak deductive system E of L. Then there exists $a \in E - D$. It follows that $D_a \subseteq E$. Since $a \in L - D$, by assumption of Proposition 2.3(8) and Theorem 3.8, we get $D_a = L$ and so $E = L$. Therefore, D is a maximal weak deductive system of L. □

5. Relation between hyper MV-algebras and hyper residuated lattices

Definition 5.1. [8] A *hyper MV-algebra* is a non-empty set M endowed with a binary hyper operation $\oplus$, a unary operation $*$ and a constant 0 satisfying the following conditions: for all $x, y, z \in M$

($hMV1$) $x \oplus (y \oplus z) = (x \oplus y) \oplus z$,
($hMV2$) $x \oplus y = y \oplus x$,
($hMV3$) $(x^*)^* = x$,
($hMV4$) $(x^* \oplus y)^* \oplus y = (y^* \oplus x)^* \oplus x$,
($hMV5$) $0^* \in x \oplus 0^*$,
($hMV6$) $0^* \in x \oplus x^*$,
($hMV7$) if $x \ll y$ and $y \ll x$, then $x = y$,

where $x \ll y$ is defined by $0^* \in x^* \oplus y$.

For every $A, B \subseteq M$, we define $A \ll B$ if and only if there exist $a \in A$ and $b \in B$ such that $a \ll b$ and $A \oplus B = \cup\{a \oplus b \mid a \in A, b \in B\}$. Also, we define $0^* = 1$ and $A^* = \{a^* \mid a \in A\}$.

Lemma 5.2. *Let* $(L, \vee, \wedge, \odot, \to, 0, 1)$ *be a hyper residuated lattice and* $\neg\neg x = \{x\}$, *for all* $x \in L$. *Then* $|\neg x| = 1$, *for all* $x \in L$.

Proof. Let $x \in L$ and $a, b \in \neg x$. Then $\neg a \subseteq \neg\neg x = \{x\}$ and so $\neg a = \{x\}$. Similarly, $\neg b = \{x\}$. It follows that $\neg a = \neg b$ and so $\{a\} = \neg\neg a = \neg\neg b = \{b\}$. Hence $a = b$. Therefore, $|\neg x| = 1$. □

Theorem 5.3. *Let* $(L, \vee, \wedge, \odot, \rightarrow, 0, 1)$ *be a hyper residuated lattice satisfying the following conditions:*

(i) $\neg\neg x = \{x\}$, *for all* $x \in L$,

(ii) $\neg(x \odot \neg y) \odot \neg y = \neg(y \odot \neg x) \odot \neg x)$, *for all* $x, y \in L$.

Let $x + y = \neg(\neg x \odot \neg y)$. *Then* $(M, +, \neg, 0)$ *is a hyper MV-algebra (since* $|\neg x| = 1$, *we use* $\neg x$ *to denote the only element of* $\neg x$).

Proof. Let $x, y, z \in L$.

(1). Since $(L, \odot, 1)$ is a commutative semihypergroup, then we have

$$(x + y) = \neg(\neg x \odot \neg y) = \neg(\neg y \odot \neg x) = (y + x).$$

$$\begin{aligned}(2).\quad (x + y) + z = \cup\{a + z | a \in x + y\} &= \cup\{\neg(\neg a \odot \neg z) \mid a \in x + y\} \\ &= \cup\{\neg(\neg a \odot \neg z) \mid a \in \neg(\neg x \odot \neg y)\} \\ &= \cup\{\neg(\neg\neg b \odot \neg z) \mid b \in (\neg x \odot \neg y)\} \\ &= \cup\{\neg(b \odot \neg z) \mid b \in (\neg x \odot \neg y)\} \\ &= \neg((\neg x \odot \neg y) \odot \neg z)\end{aligned}$$

By the similar way, we can show that $\neg((\neg x \odot \neg y) \odot \neg z) = x + (y + z)$. Therefore, $x + (y + z) = (x + y) + z$.

(3). By Proposition 2.3(5), we get $x + 1 = x + \neg 0 = \neg(\neg x \odot \neg\neg 0) \supseteq \neg 0 = 1$.

(4). By Proposition 2.3(6), $(x \odot \neg x \ll 0$, so $0 \in x \odot \neg x$. Hence

$$(x + \neg x) = \neg(\neg x \odot \neg\neg x) = \neg(\neg x \odot x) \supseteq \neg 0 = 1.$$

(5). Let $1 \in (\neg x + y) \cap (x + \neg y)$. Then $1 \in \neg(\neg\neg x \odot \neg y) \cap \neg(\neg x \odot \neg\neg y)$ and so $0 \in (x \odot \neg y) \cap (\neg x \odot y)$. It follows that $x \odot \neg y \ll 0$ and $\neg x \odot y \ll 0$. Hence $x \ll \neg\neg y$ and $y \ll \neg\neg x$ and so $x = y$.

$$\begin{aligned}(6).\quad \neg(\neg x + y) + y = (\neg\neg(x \odot \neg y)) + y &= (x \odot \neg y) + y \\ &= \neg(\neg(x \odot \neg y) \odot \neg y) \\ &= \neg(\neg(y \odot \neg x) \odot \neg x), \text{ by assumption} \\ &= \neg(\neg y + x) + x.\end{aligned}$$

From (i) and (1) – (6), it follows that, $(M, +, \neg, 0)$ is a hyper MV-algebra. □

Example 5.4. Let $(P', \vee, \wedge, \odot, \rightsquigarrow, 0, 1)$ be a hyper residuated lattice in Example 4.6. Then P' satisfies the conditions of Theorem 5.3. □

Open problem: *Under what conditions we can obtain a hyper residuated lattice from a hyper MV-algebra?*

6. Conclusions and future works

In this paper, we introduce the concept of hyper residuated lattice which is a generalization of the concept of residuated lattice, and we give some properties and related results. The category of hyper residuated lattices, quotient structure, filter theory, lattice structures of filters and hyper residuated lattices could be topics for future researchs.

References

[1] **M. Bakhshi, R. A. Borzooei**, *Lattice structure on fuzzy congruence relations of a hypergroupoid*, Information Sci. **177** (2007), 3305 – 3313.

[2] **R. A. Boorzooei, A. Hasankhani, M. M. Zahedi, Y.B. Jun**, *On hyper K-algebra*, J. Math. Japonica **1** (2000), 113 – 121.

[3] **T. S. Blyth**, *Lattices and ordered algebraic structures*, Springer-Verlag, (2005).

[4] **C. C. Chang**, *Algebraic analysis of many valued logics*, Trans. Am. Math. Soc. **88** (1958), 467 – 490.

[5] **P. Corsini**, *Prolegomena of hypergroups*, Aviani Editore, (1993).

[6] **P. Corsini, V. Leoreanu**, *Applications of hyperstructure theory*, Kluwer Academic Publ., Dordrecht, (2003).

[7] **B. A. Davey, H. A. Priestley**, *Introduction to lattices and order*, Cambridge Univ. Press, United Kingdown, (2002).

[8] **Sh. Ghorbani, A. Hasankhani, E. Eslami**, *Hyper MV-algebras*, Set-Valued Math. Appl. **1** (2008), 205 – 222.

[9] **P. Hájek**, *Metamathematics of fuzzy logic*, Kluwer Academic Publ., Dordrecht, (1998).

[10] **F. Marty**, *Sur une généralization de la notion de groups*, 8th Congress Math. Scandinaves, Stockholm, (1934), 45 – 49.

[11] **J. Mittas, M. Konstantinidou**, *Sur une nouvelle génération de la notion de treillis. Les supertreillis et certaines de leurs propriétés générales*, Ann. Sci. Univ. Blaise Pascal (Clermont II), Sér. Math. Fasc. **25** (1989), 61 – 83.

[12] **M. Ward, R. P. Dilworth**, *Residuated lattices*, Trans. Amer. Math. Soc. **45** (1939), 335 – 354.

[13] **O. Zahiri, R. A. Borzooei, M. Bakhshi**, (*Quotient*) *hyper residuated lattices*, Quasigroups and Related Systems, **20** (2012), 125 – 138.

Received October 10, 2013

R. Borzooei, O. Zahiri
Department of Mathematics, Shahid Beheshti University, Tehran, Iran
E-mails: borzooei@sbu.ac.ir, om.zahiri@gmail.com

M. Bakhshi
Department of Mathematics, Bojnord University, Bojnord, Iran
E-mail: bakhshi@ub.ac.ir

On sheaf spaces of partially ordered quasigroups

Ján Brajerčík and Milan Demko

Abstract. The conditions under which a partially ordered quasigroup can be represented as sections of a sheaf space of partially ordered quasigroups are investigated.

1. Introduction

There are known some characterizations of representable lattice ordered groups, i.e., lattice ordered groups, shortly l-groups, which are l-isomorphic to a subdirect product of totally ordered groups; see, e.g., [2]. One of these characterizations is based on the theory of sheaf spaces of l-groups. The central theorem used for this purpose gives the conditions (using ideals of l-groups) under which an l-group can be represented as sections of a sheaf space of l-groups (see [2, Theorem 49.4]). In this paper we generalize this result for partially ordered quasigroups.

2. Preliminaries

A *quasigroup* is an algebra $(Q, \cdot, \backslash, /)$ with three binary operations $\cdot, \backslash, /$ satisfying the following identities

$$y\backslash(y \cdot x) = x; \qquad (x \cdot y)/y = x; \qquad y \cdot (y\backslash x) = x; \qquad (x/y) \cdot y = x. \tag{1}$$

It is easy to see that

$$x/(y\backslash x) = y; \qquad (x/y)\backslash x = y \tag{2}$$

follow from (1). Further, the identities (1) imply that, given $a, b \in Q$, the equations $b \cdot x = a$ and $y \cdot b = a$ have unique solutions $x = b\backslash a$ and $y = a/b$, respectively. Conversely, if G is a groupoid such that the equations $b \cdot x = a$ and $y \cdot b = a$ have unique solutions x, $y \in G$, then G is a quasigroup, where $b\backslash a$ and a/b are defined as the solution of the equation $b \cdot x = a$ or $x \cdot b = a$, respectively. Clearly, every group is a quasigroup with $x/y = x \cdot y^{-1}$ and $y\backslash x = y^{-1} \cdot x$. General information concerning the properties of quasigroups can be found, e.g., in [1], [5].

A quasigroup $(Q, \cdot, \backslash, /)$ with a binary relation $\leqslant$ is called a *partially ordered quasigroup* (*po-quasigroup*) if

2010 Mathematics Subject Classification: 06F99, 20N05, 54B40.
Keywords: sheaf space, partially ordered quasigroup.
The second author acknowledges the support of the Slovak VEGA Grant No. 1/0063/14.

(i) $(Q, \leqslant)$ is a partially ordered set,

(ii) for all $x, y, a \in Q$, $x \leqslant y$ implies

$$ax \leqslant ay,\ xa \leqslant ya,\ x/a \leqslant y/a,\ a\backslash x \leqslant a\backslash y,\ a/y \leqslant a/x,\ y\backslash a \leqslant x\backslash a.$$

For a po-quasigroup we will use the notation $\mathcal{Q} = (Q, \cdot, \backslash, /, \leqslant)$. Clearly, every partially ordered group is a po-quasigroup.

A partially ordered quasigroup $\mathcal{Q}$ is called a *lattice ordered quasigroup* (shortly *l-quasigroup*), if $\leqslant$ is a lattice order. Analogously to the case of the lattice ordered groups it can be proved that for l-quasigroups the following identities, determining the relationship between the quasigroup operations and the lattice operations $\vee$, $\wedge$, hold

(L1) $a(b \vee c) = ab \vee ac$; $(b \vee c)a = ba \vee ca$,
$a(b \wedge c) = ab \wedge ac$; $(b \wedge c)a = ba \wedge ca$.

(L2) $(b \vee c)/a = (b/a) \vee (c/a)$; $a\backslash(b \vee c) = (a\backslash b) \vee (a\backslash c)$,
$(b \wedge c)/a = (b/a) \wedge (c/a)$; $a\backslash(b \wedge c) = (a\backslash b) \wedge (a\backslash c)$.

(L3) $a/(b \vee c) = (a/b) \wedge (a/c)$; $(b \vee c)\backslash a = (b\backslash a) \wedge (c\backslash a)$,
$a/(b \wedge c) = (a/b) \vee (a/c)$; $(b \wedge c)\backslash a = (b\backslash a) \vee (c\backslash a)$.

Here we prove only the first identity from (L3); the proofs of remaining identities are analogous. Since $b, c \leqslant b \vee c$, we have $a/(b \vee c) \leqslant a/b, a/c$, and therefore $a/(b \vee c) \leqslant (a/b) \wedge (a/c)$. On the other hand, $(a/b) \wedge (a/c) \leqslant a/b, a/c$. Using (2) we obtain $c, b \leqslant ((a/b) \wedge (a/c))\backslash a$, which implies $b \vee c \leqslant ((a/b) \wedge (a/c))\backslash a$. Hence $(a/b) \wedge (a/c) \leqslant a/(b \vee c)$. Therefore we can conclude that $a/(b \vee c) = (a/b) \wedge (a/c)$.

Let $\mathcal{Q}$ and $\mathcal{H}$ be the partially ordered quasigroups. We say that a mapping $\Phi : Q \to H$ is an *o-embedding* of $\mathcal{Q}$ into $\mathcal{H}$ if Φ is a quasigroup homomorphism and

$$\Phi(x) \leqslant \Phi(y) \Longleftrightarrow x \leqslant y.$$

In that case we say that $\mathcal{Q}$ is o-embedded into $\mathcal{H}$.

Let $\mathcal{Q} = (Q, \cdot, \backslash, /, \leqslant)$ be a partially ordered quasigroup. Let θ be a congruence relation on $(Q, \cdot, \backslash, /)$. The congruence class of θ containing $a \in Q$ will be denoted by $[a]\theta$, i.e., $[a]\theta = \{x \in Q |\, x\theta a\}$. Clearly, every congruence class $[a]\theta$ is a partially ordered set under the relation induced by $\leqslant$. We say that θ is a *convex congruence relation* on $\mathcal{Q}$ if θ is a congruence relation on $(Q, \cdot, \backslash, /)$ and there exists $a \in Q$ such that the congruence class $[a]\theta$ is a convex subset of $\mathcal{Q}$. We say that θ is a *directed congruence relation* on $\mathcal{Q}$ if θ is a congruence relation on $(Q, \cdot, \backslash, /)$ and there exists $a \in Q$ such that the congruence class $[a]\theta$ is a directed subset of $\mathcal{Q}$ (i.e., for each $x, y \in [a]\theta$ there exist $u, v \in [a]\theta$ such that $u \leqslant x, y$ and $x, y \leqslant v$).

Let $\mathcal{Q}$ be a po-quasigroup and let θ be a convex congruence relation on $\mathcal{Q}$. Let us put

$$[x]\theta \leqslant [y]\theta \text{ if and only if there exist } x_0 \in [x]\theta, y_0 \in [y]\theta \text{ such that } x_0 \leqslant y_0. \quad (3)$$

A quotient-quasigroup $(Q, \cdot, \backslash, /)/\theta$ with the relation defined by (3) is a partially ordered quasigroup; it will be denoted by $\mathcal{Q}/\theta$ (see [3, Theorem 2.6]). If $\mathcal{Q}$ is an l-quasigroup and θ is a convex directed congruence relation on $\mathcal{Q}$, then $\mathcal{Q}/\theta$ is an l-quasigroup with the lattice operations $\vee$ and $\wedge$ defined by (see [3])

$$[x]\theta \vee [y]\theta = [x \vee y]\theta; \;\; [x]\theta \wedge [y]\theta = [x \wedge y]\theta.$$

3. Sheaf spaces of po-quasigroups

Let E and X be topological spaces. A continuous mapping $\sigma : E \to X$ is called a *local homeomorphism*, if each point $s \in E$ has a neighborhood V such that $\sigma(V)$ is an open set in X and the restricted mapping $\sigma|_V : V \to \sigma(V)$ is a homeomorphism. If $x \in X$ is a point, the set $E_x = \sigma^{-1}(x)$ is called the *fibre* over x. Let U be an open set in X. A continuous mapping $f : U \to E$ such that $f(x) \in \sigma^{-1}(x)$ for all $x \in U$ is called a *continuous local section* of σ *over* U. If σ is surjective and $U = X$, f is called a *continuous global section*. The basic facts on sections of a local homeomorphism can be find, e.g., in [4]. For the sake of convenience, we summarize here some results which will be frequently used.

Proposition 3.1. (cf. [4, Lemma 1])

(*i*) *A local homeomorphism is an open mapping.*

(*ii*) *The restriction of a local homeomorphism to a topological subspace is a local homeomorphism.*

Proposition 3.2. (cf. [4, Lemma 2]) *Let $\sigma : E \to X$ be a local homeomorphism.*

(*i*) *To each point $s \in E$ there exist a neighborhood U of $x = \sigma(s)$ and a continuous section $f : U \to E$ such that $f(x) = s$.*

(*ii*) *Let f be a continuous section of E over an open subset U of X. To each point $x \in U$ and each neighborhood V of $f(x)$ such that $\sigma(V)$ is open and $\sigma|_V$ is a homeomorphism, there exists a neighborhood U_0 of x such that $f(U_0) \subseteq V$ and $f|_{U_0} = (\sigma|_V)^{-1}|_{U_0}$.*

(*iii*) *If U, V are open sets in X, and $f : U \to E$, $g : V \to E$ are continuous sections, then the set $\{x \in U \cap V \mid f(x) = g(x)\}$ is open.*

(*iv*) *Every continuous section of E defined on an open set is an open mapping.*

Proposition 3.3. (cf. [4, Lemma 3]) *Let $\sigma : E \to X$ be a local homeomorphism.*

(*i*) *The open sets $V \subseteq E$ such that $\sigma|_V : V \to \sigma(V)$ is a homeomorphism form a basis of the topology of E.*

(*ii*) *The topology of E coincides with the final topology associated with the set of all continuous sections of E.*

Let $\sigma : E \to X$ be a local homeomorphism. For any $U \subseteq X$ we denote

$$E_U = \bigcup_{x \in U} E_x.$$

Immediately from the definition of a local homeomorphism we obtain

Lemma 3.4. *If $U \subseteq X$ is open in X, then E_U is an open set in E.*

By $E\Delta E$ we denote the set $\bigcup_{x\in X}(E_x \times E_x)$ with the induced topology from $E \times E$.

Definition 3.5. Let E and X be topological spaces and let $\sigma : E \to X$ be a surjective local homeomorphism. We say that a triplet (E, X, σ) is a *sheaf space of po-quasigroups* if

(i) each fibre E_x is a po-quasigroup,

(ii) the mappings $(s,t) \mapsto s \cdot t$, $(s,t) \mapsto t\backslash s$ and $(s,t) \mapsto s/t$ from $E\Delta E$ to E are continuous.

Definition 3.6. A sheaf space of po-quasigroups (E, X, σ) is said to be a *sheaf space of l-quasigroups* if each fibre E_x is an l-quasigroup and the mappings

$$(s,t) \mapsto s \vee t, \qquad (s,t) \mapsto s \wedge t$$

from $E\Delta E$ to E are continuous.

Let (E, X, σ) be a sheaf space of po-quasigroups. Let f, g be continuous sections defined over the same open set $U \subseteq X$. Define fg, $g\backslash f$ and f/g by

$$(fg)(x) = f(x) \cdot g(x); \quad (g\backslash f)(x) = g(x)\backslash f(x); \quad (f/g)(x) = f(x)/g(x).$$

Since $\cdot, \backslash, /$ are continuous mappings from $E\Delta E$ to E, fg, $g\backslash f$ and f/g are continuous sections over U.

Lemma 3.7. *Let (E, X, σ) be a sheaf space of po-quasigroups and let $f : U \to E$ be a continuous local section over an open set $U \subseteq X$. Then the mapping $\varphi_f : E_U \to E_U;\ E_x \ni s \mapsto f(x)/s$ is a homeomorphism.*

Proof. By Lemma 3.4, E_U is an open set in E. Clearly, $\varphi_f : E_U \to E_U;\ E_x \ni s \mapsto f(x)/s$ is a bijection. Using (2) it is easy to verify that the inverse mapping $\varphi_f^{-1} : E_U \to E_U$ is defined by $E_x \ni s \mapsto s\backslash f(x)$.

Let $s \in E_U$, $\sigma(s) = x \in U$. Let $W \subseteq E_U$ be an open set, $f(x)/s \in W$. In view of Proposition 3.3(i) for the proof of the continuity of φ_f we may suppose that $\sigma|_W$ is a homeomorphism. Denote $(\sigma|_W)^{-1} = g$. Clearly, g is a continuous local section over $U_0 = \sigma(W)$ and $g(x) = f(x)/s$. Put $V = (g\backslash f)(U_0)$. Since $g\backslash f$ is a continuous local section, by Proposition 3.2(iv), V is open in E_U. Moreover, since $(g\backslash f)(x) = g(x)\backslash f(x) = (f(x)/s)\backslash f(x) = s$, we have $s \in V$. Further, if $t \in \varphi_f(V)$, then there is $u \in U_0$ such that $t = \varphi_f(g(u)\backslash f(u)) = f(u)/(g(u)\backslash f(u)) = g(u) \in W$. Thus $\varphi_f(V) \subseteq W$, and we can conclude that φ_f is continuous. The proof of the continuity of φ_f^{-1} is analogous. □

Let (E, X, σ) be a sheaf space of po-quasigroups. Consider the following condition:

(C) *if f, g are continuous local sections over the same open set $U \subseteq X$ such that* $\sup\{f(u), g(u)\}$ *exists for each $u \in U$, then the set* $\{\sup\{f(u), g(u)\} \mid u \in U\}$ *is open in E.*

Lemma 3.8. *Let (E, X, σ) be a sheaf space of po-quasigroups where fibres E_x are lattice ordered quasigroups. Then (E, X, σ) is a sheaf space of l-quasigroups if and only if (E, X, σ) satisfies the condition* (C).

Proof. Suppose that (E, X, σ) satisfies the condition (C). Firstly we will show that $\vee$ is continuous. Let (s, t) be an arbitrary point of $E\Delta E$, i.e., $s, t \in E_x$ for some $x \in X$. Let $W_{s\vee t}$ be an open set in E, $s \vee t \in W_{s\vee t}$. By Proposition 3.2(i) there exist an open set $U \subseteq X$, $x \in U$, and continuous local sections f, g over U with $f(x) = s$, $g(x) = t$. By (C), the set $W_{\sup} = \{f(u) \vee g(u) \mid u \in U\}$ is open in E. Denote $W_0 = W_{\sup} \cap W_{s\vee t}$. By Proposition 3.1($i$), the set $U_0 = \sigma(W_0)$ is open in X which implies that $f(U_0)$ and $g(U_0)$ are open in E, and $\{(f(u),\, g(u)) \mid u \in U_0\} = (f(U_0) \times g(U_0)) \cap (E\Delta E)$ is open in $E\Delta E$ containing the point $(s, t) \in E\Delta E$. Since $f(U_0) \vee g(U_0) \equiv \{(f(u) \vee g(u)) \mid u \in U_0\} \subseteq W_0 \subseteq W_{s\vee t}$, we can conclude that $\vee$ is continuous.

We are going to show that $\wedge$ is continuous. Let $s, t \in E_x$. Let $W_{s\wedge t}$ be an open set in E, $s \wedge t \in W_{s\wedge t}$. In view of Proposition 3.3(i) for the proof of the continuity of $\wedge$ we may suppose that $\sigma|_{W_{s\wedge t}}$ is a homeomorphism. Denote $f = (\sigma|_{W_{s\wedge t}})^{-1}$. Clearly, f is a continuous local section over $U = \sigma(W_{s\wedge t})$. By Lemma 3.7, the mapping $\varphi_f : E_U \to E_U$; $E_z \ni r \mapsto f(z)/r$ is a homeomorphism. Thus $W = \varphi_f(f(U))$ is open in E and $f(x)/(s \wedge t) \in W$. By (L3), $f(x)/(s \wedge t) = (f(x)/s) \vee (f(x)/t)$ and since $\vee$ is continuous, there exist neighborhoods V_s of $f(x)/s$ and V_t of $f(x)/t$, $\sigma(V_s) = \sigma(V_t) \subseteq U$, such that $V_s \vee V_t \subseteq W$. Denote $W_s = \varphi_f^{-1}(V_s)$ and $W_t = \varphi_f^{-1}(V_t)$. Since $\varphi_f^{-1}(f(x)/s) = (f(x)/s)\backslash f(x) = s$, we have $s \in W_s$. Analogously, $t \in W_t$. Further, if $p \in W_s$, $r \in W_t$, $\sigma(p) = \sigma(r) = z$, then $\varphi_f(p) \vee \varphi_f(r) = (f(z)/p) \vee (f(z)/r) \in V_s \vee V_t \subseteq W$, which yields $f(z)/(p \wedge r) \in W$. Hence $\varphi_f^{-1}(f(z)/(p \wedge r)) = p \wedge r \in f(U) \subseteq W_{s\wedge t}$. Thus $W_s \wedge W_t \subseteq W_{s\wedge t}$, and we can conclude that $\wedge$ is continuous.

Conversely, let (E, X, σ) be a sheaf space of l-quasigroups. Suppose that f, g are continuous local sections over the same open set $U \subseteq X$. We are going to show that $W_{\sup} = \{f(u) \vee g(u) \mid u \in U\}$ is open in E. Let $x \in U$. By Proposition 3.3(i) there exists an open set W in E, $f(x) \vee g(x) \in W$, such that $\sigma|_W : W \to \sigma(W)$ is a homeomorphism. Since $\vee$ is continuous, there exist an open set $U_0 \subseteq U \subseteq X$, $x \in U_0$, such that $W_0 = f(U_0) \vee g(U_0) \subseteq W$. Clearly, $W_0 \subseteq W_{\sup}$ and, since $W_0 = E_{U_0} \cap W$, by Lemma 3.4, W_0 is open. Thus we can conclude that $W_{\sup}$ can be covered by open sets, which means that $W_{\sup}$ is open in the topology of E. □

The sheaf space of l-groups is defined as a triplet (E, X, σ) such that each fibre E_x is an l-group, the mappings $\cdot$, $\vee$, $\wedge$ are continuous from $E\Delta E$ to E and $^{-1}$ is continuous from E to E (see [2]). In view of Lemma 3.7 and Lemma 3.8 we have

Corollary 3.9. *Let (E, X, σ) be a sheaf space of po-quasigroups satisfying* (C)*. If E_x is an l-group for each $x \in X$, then (E, X, σ) is a sheaf space of l-groups.*

Proof. Clearly, $\cdot$ is continuous from $E \Delta E$ to E and, by Lemma 3.8, the lattice operations $\vee$ and $\wedge$ are also continuous. Consider the global section $e : X \to E$; $e(x) = e_x$, where e_x is the identity element of E_x; e is a continuous global section (see [4]). Since for $s \in E_x$ we have $s^{-1} = e_x/s = e(x)/s$ and, by Lemma 3.7, $s \mapsto e(x)/s$ is a homeomorphism, we can conclude that $^{-1}$ is a continuous mapping from E to E. □

Let (E, X, σ) be a sheaf space of po-quasigroups. Clearly, the direct product $\prod_{x \in X} E_x$ of po-quasigroups E_x is a po-quasigroup. Denote by $\mathcal{R}$ the set of all continuous global sections of σ and define the relation $\leqslant$ on $\mathcal{R}$ by

$$g \leqslant h \Longleftrightarrow g(x) \leqslant h(x) \text{ for all } x \in X. \tag{4}$$

Let $\mathcal{R} \neq \emptyset$. Then $\mathcal{R}$ with the operations $\cdot$, $/$, $\backslash$ defined componentwise and the relation $\leqslant$ defined by (4) is a po-quasigroup. Moreover, it is easy to see that

Lemma 3.10. *If $\mathcal{R} \neq \emptyset$, then $\mathcal{R}$ is a po-subquasigroup of the direct product $\prod_{x \in X} E_x$.*

The following theorem generalizes the analogous result valid for lattice ordered groups (see [2, Theorem 49.4]).

Theorem 3.11. *Let $\mathcal{Q}$ be a po-quasigroup and let X be a topological space. Suppose that for each $x \in X$ there exists a convex congruence relation θ_x on $\mathcal{Q}$ such that the following conditions are satisfied*

(*i*) *for all $g, h \in Q$, the set $U_{gh} = \{x \in X \mid [g]\theta_x = [h]\theta_x\}$ is open in X,*

(*ii*) *if $[g]\theta_x \leqslant [h]\theta_x$ for each $x \in X$, then $g \leqslant h$.*

Then $\mathcal{Q}$ can be o-embedded into a po-quasigroup of the continuous global sections of some sheaf space of po-quasigroups over X. Especially, if $\mathcal{Q}$ is an l-quasigroup and θ_x are directed convex congruence relations on $\mathcal{Q}$ satisfying (*i*) *and* (*ii*)*, then $\mathcal{Q}$ can be o-embedded into an l-quasigroup of the continuous global sections of some sheaf space of l-quasigroups over X.*

Proof. Let $\mathcal{Q}$ be a po-quasigroup such that (*i*) and (*ii*) are valid. We follow the idea of the construction of a sheaf space which was used for l-groups in the proof of Theorem 49.4 in [2]. Denote

$$E = \bigcup_{x \in X} E_x,$$

where $E_x = \mathcal{Q}/\theta_x \times \{x\}$ and define

$$\sigma : E \to X; \quad ([g]\theta_x, x) \mapsto x.$$

Clearly, σ is a surjection. Further, for each $g \in Q$ we define

$$\widehat{g} : X \to E; \quad x \mapsto ([g]\theta_x, x)$$

and consider the finest topology τ on E such that each $\widehat{g}$ is continuous. Denote

$$\mathbb{B} = \{\widehat{g}(U) \mid U \text{ is open in } X, g \in Q\}.$$

Let $\widehat{g}(U), \widehat{h}(V) \in \mathbb{B}$. By (i), $T = \{x \in X \mid \widehat{g}(x) = \widehat{h}(x)\}$ is an open set in X. Let $W = T \cap U \cap V$. Clearly, W is open in X, and $\widehat{g}(W) = \widehat{h}(W) \subseteq \widehat{g}(U) \cap \widehat{h}(V)$. Conversely, if $t \in \widehat{g}(U) \cap \widehat{h}(V)$, then $t = ([g]\theta_u, u) = ([h]\theta_u, u)$, $u \in W$, which yields $t \in \widehat{g}(W)$. Therefore $\widehat{g}(U) \cap \widehat{h}(V) = \widehat{g}(W)$ and, since W is open in X, we can conclude that $\widehat{g}(U) \cap \widehat{h}(V) \in \mathbb{B}$. Thus $\mathbb{B}$ is a basis for some topology τ_B on E. By (i), for any $\widehat{h}(U) \in \mathbb{B}$ and $g \in Q$ the set $(\widehat{g})^{-1}(\widehat{h}(U)) = U \cap \{x \in X \mid [g]\theta_x = [h]\theta_x\}$ is open in X, which yields $\tau_B \subseteq \tau$. On the other hand, let V be a τ-open set in E. For every $v = ([g]\theta_x, x) \in V$ the set $U = (\widehat{g})^{-1}(V)$ is open in X, $\widehat{g}(U) \subseteq V$ and $v \in \widehat{g}(U)$. Thus V is covered by τ_B-open sets. Therefore $\tau \subseteq \tau_B$ and so $\tau = \tau_B$.

Let $s \in E$, $s = ([g]\theta_x, x)$ and let U be a neighborhood of $x = \sigma(s)$ in X. Then $V = \widehat{g}(U)$ is open in E, $s \in V$ and

$$\sigma\mid_V \circ \widehat{g}\mid_U = \mathrm{id}_U, \quad \widehat{g}\mid_U \circ \sigma\mid_V = \mathrm{id}_V.$$

Thus $\sigma : E \to X : ([g]\theta_x, x) \mapsto x$ is a continuous mapping and $\sigma\mid_V : V \to U$ is a homeomorphism. We have that $\sigma : E \to X$ is a local homeomorphism with the fibres $E_x = \{\widehat{g}(x) \mid g \in Q\}$. Each fibre E_x is a po-quasigroup under the operations

$$\widehat{g}(x) \cdot \widehat{h}(x) = (\widehat{gh})(x); \quad (\widehat{g}(x)/\widehat{h}(x) = (\widehat{g/h})(x); \quad \widehat{g}(x)\backslash\widehat{h}(x) = (\widehat{g\backslash h})(x)$$

and the partial order

$$\widehat{g}(x) \leqslant \widehat{h}(x) \text{ iff there exist } g' \in [g]\theta_x, h' \in [h]\theta_x \text{ such that } g' \leqslant h'.$$

For every open set W in E such that $\widehat{gh}(x) \in W$ there exists an open set U in X, $x \in U$, such that $\widehat{gh}(U) \subseteq W$. Since $V = \{(\widehat{g}(u), \widehat{h}(u)) \mid u \in U\}$ is open in $E\Delta E$ and $\widehat{g}(u) \cdot \widehat{h}(u) = \widehat{gh}(u)$ for each $u \in U$, we can conclude that the operation $\cdot$ is continuous. Analogously, the operations $\backslash, /$ are continuous. Thus (E, X, σ) is a sheaf space of po-quasigroups.

Let $\mathcal{R}$ be a po-quasigroup of all continuous global sections of (E, X, σ). Define

$$\Phi : \mathcal{Q} \to \mathcal{R}; \quad g \mapsto \widehat{g}.$$

Clearly, Φ preserves the quasigroup operations. Further, by (ii), we have

$$g \leqslant h \Leftrightarrow [g]\theta_x \leqslant [h]\theta_x \text{ for all } x \in X \Leftrightarrow \widehat{g}(x) \leqslant \widehat{h}(x) \text{ for all } x \in X \Leftrightarrow \widehat{g} \leqslant \widehat{h}.$$

Thus Φ is an o-embedding of $\mathcal{Q}$ into $\mathcal{R}$.

If $\mathcal{Q}$ is an l-quasigroup and θ_x are directed convex congruence relations on $\mathcal{Q}$, then $\mathcal{Q}/\theta_x$ are l-quasigroups, which yields that the fibres E_x are lattice ordered quasigroups under the lattice operations

$$\widehat{g}(x) \vee \widehat{h}(x) = (\widehat{g \vee h})(x); \quad \widehat{g}(x) \wedge \widehat{h}(x) = (\widehat{g \wedge h})(x).$$

By the same way as in the case of the quasigroup operations we can see that the mappings $\vee$ and $\wedge$ are continuous. Thus (E, X, σ) is a sheaf space of l-quasigroups. Clearly, $\mathcal{R}$ is an l-quasigroup and $\Phi : g \mapsto \widehat{g}$ is an o-embedding of $\mathcal{Q}$ into $\mathcal{R}$. $\square$

Remark. Let (E, X, σ) be the sheaf space constructed in the proof of Theorem 3.11. Let X be a Hausdorff space. Then E is a Hausdorff space if for all $g, h \in Q$, the set $U_{gh} = \{x \in X \mid [g]\theta_x = [h]\theta_x\}$ is open and also close in X. To prove this statement it suffices to use the same topological arguments as in the proof of Theorem 49.4 in [2].

References

[1] **V. D. Belousov**, *Foundations of the theory of quasigroups and loops*, (Russian), Nauka, Moscow, 1967.

[2] **M. R. Darnel**, *Theory of latice-ordered groups*, Marcel Dekker, Inc. New York, 1995.

[3] **M. Demko**, *On congruences and ideals of partially ordered quasigroups*, Czech. Math. J. **58** (2008), 637 – 650.

[4] **D. Krupka**, *The geometry of Lagrange structures II. Elementary Sheaf Theory*, Department of Mathematics, Silesian University, Opava, 1998.

[5] **H. Pflugfelder**, *Quasigroups and Loops: Introduction*, Heldermann Verlag, Berlin, 1990.

Received March 08, 2013

Department of Physics, Mathematics and Techniques, University of Prešov, Ul. 17. novembra 1, 081 16 Prešov, Slovakia
E-mails: jan.brajercik@unipo.sk, milan.demko@unipo.sk

On two-sided bases of an ordered semigroup

Thawhat Changphas and Pisan Sammaprab

Abstract. We introduce the concept of two-sided base of an ordered semigroup, and study the structure of an ordered semigroup containing two-sided bases.

1. Preliminaries

Given a semigroup S, a subset A of S is called a *two-sided base* of S if it satisfies the following conditions: $S = A \cup SA \cup AS \cup SAS$, and if B is a subset of A such that $S = B \cup SB \cup BS \cup SBS$ then $B = A$. This notion was introduced and studied by Fabrici [2]. Indeed, the author described the structure of semigroups containing two-sided bases. The purpose of this paper is to introduce the concept of two-sided base of an ordered semigroup, and extend the Fabrici's results to ordered semigroups.

A semigroup $(S, \cdot)$ together with a partial order $\leqslant$ that is *compatible* with the semigroup operation, meaning that, for any x, y, z in S,

$$x \leqslant y \text{ implies } zx \leqslant zy \text{ and } xz \leqslant yz,$$

is called a *partially ordered semigroup*, or simply an *ordered semigroup* [1]. A nonempty subset T of an ordered semigroup $(S, \cdot, \leqslant)$ is called a *subsemigroup* of S if, for any x, y in T, $xy \in T$.

Let $(S, \cdot, \leqslant)$ be an ordered semigroup. For A, B nonempty subsets of S, we write AB for the set of all elements xy in S where $x \in A$ and $y \in B$, and write $(A]$ for the set of all elements $x \in S$ such that $x \leqslant a$ for some $a \in A$, i.e.,

$$(A] = \{x \in S \mid x \leqslant a \text{ for some } a \in A\}.$$

In particular, we write Ax for $A\{x\}$, and xA for $\{x\}A$. It was shown in [7] that the following hold:

(1) $A \subseteq (A]$;

(2) $A \subseteq B \Rightarrow (A] \subseteq (B]$;

(3) $(A](B] \subseteq (AB]$;

(4) $(A \cup B] = (A] \cup (B]$;

2010 Mathematics Subject Classification: 06F05
Keywords: ordered semigroup, two-sided ideal, maximal ideal, two-sided base.

(5) $((A]] = (A]$.

The concepts of left, right and two-sided ideals of an ordered semigroup can be found in [3]. Let $(S, \cdot, \leqslant)$ be an ordered semigroup. A nonempty subset A of S is called a *left* (respectively, *right*) *ideal* of S if it satisfies the following conditions:

(i) $SA \subseteq A$ (respectively, $AS \subseteq A$);

(ii) $A = (A]$, that is, for any x in A and y in S, $y \leqslant x$ implies $y \in A$.

If A is both a left and a right ideal of S, then A is called a *two-sided ideal*, or simply an *ideal* of S. If A and B are ideals of S, then the union $A \cup B$ is an ideal of S.

If A is a nonempty subset of an ordered semigroup $(S, \cdot, \leqslant)$, then the intersection of all ideals containing A of S, denoted by $I(A)$, is an ideal containing A of S, and it is of the form

$$I(A) = (A \cup SA \cup AS \cup SAS].$$

In particular, we write $I(\{a\})$ by $I(a) = (a \cup Sa \cup aS \cup SaS]$ (this is called the *principal ideal generated by* a).

A proper ideal M of an ordered semigroup $(S, \cdot, \leqslant)$ is said to be *maximal* if there is no a proper ideal A of S such that $M \subset A$. The symbol $\subset$ stands for proper inclusion for sets.

2. Ordered semigroups containing two-sided bases

We begin this section with the definition of two-sided base of an ordered semigroup; it is more general than that of a two-sided base of a semigroup (without order).

Definition 2.1. Let $(S, \cdot, \leqslant)$ be an ordered semigroup. A subset A of S is called a *two-sided base* of S if it satisfies the following conditions:

(i) $S = I(A)$;

(ii) if B is a subset of A such that $S = I(B)$, then $B = A$.

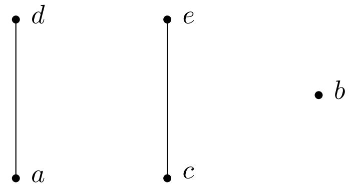
Example 2.2. ([6]) Let $(S, \cdot, \leqslant)$ be an ordered semigroup such that the multiplication and the partial order are defined by:

$\cdot$	a	b	c	d	e
a	a	e	c	d	e
b	a	b	c	d	e
c	a	e	c	d	e
d	a	e	c	d	e
e	a	e	c	d	e

$$\leqslant = \{(a, a), (b, b), (c, c), (d, d), (e, e), (a, d), (c, e)\}.$$

The covering relation and the figure of S are given by:

$$\prec = \{(a,d),(c,e)\}$$



We have $\{b\}$ is the only one two-sided base of S.

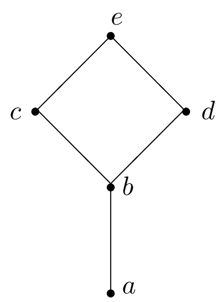
Example 2.3. ([5]) Let $(S,\cdot,\leqslant)$ be an ordered semigroup such that the multiplication and the order relation are defined by:

$\cdot$	a	b	c	d	e
a	a	a	c	a	c
b	a	a	c	a	c
c	a	a	c	a	c
d	d	d	e	d	e
e	d	d	e	d	e

$$\begin{aligned}\leqslant = \{&(a,a),(a,b),(a,c),(a,d),(a,e),(b,b),(b,c),\\ &(b,d),(b,e),(c,c),(c,e),(d,d),(d,e),(e,e)\}.\end{aligned}$$

The covering relation and the figure of S are given by:

$$\prec = \{(a,b),(a,c),(a,d),(a,e),(b,c),(b,d),(b,e),(c,e),(d,e)\}$$



The two-sided bases of S are $\{a\}$, $\{b\}$, $\{c\}$, $\{d\}$ and $\{e\}$.

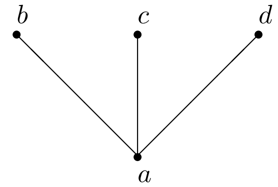
Example 2.4. ([9]) Let $(S,\cdot,\leqslant)$ be an ordered semigroup such that the multiplication and the order relation are defined by:

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	a	a	a
c	a	a	b	a
d	a	a	b	b

$$\leqslant = \{(a,a),(a,b),(a,c),(a,d),(b,b),(c,c),(d,d)\}.$$

The covering relation and the figure of S are given by:

$$< \, = \{(a,b),(a,c),(a,d)\}$$



The two-sided base of S is $\{c,d\}$.

Beside the partial order $\leqslant$ on an ordered semigroup $(S,\cdot,\leqslant)$, we define $\preceq_I$ a quasi-order on S as follows: for any a,b in S, let

$$a \preceq_I b \text{ if and only if } I(a) \subseteq I(b).$$

The symbol $a \prec_I b$ stands for $a \preceq_I b$, but $a \neq b$. It is clear that, for any a,b in S, $a \leqslant b$ implies $a \preceq_I b$. The following example shows that the converse statement is not valid in general.

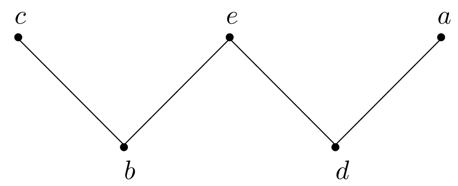
Example 2.5. ([4]) Let $(S,\cdot,\leqslant)$ be an ordered semigroup such that the multiplication and the order relation are defined by:

$\cdot$	a	b	c	d	e
a	b	d	a	b	e
b	d	b	b	d	e
c	d	b	c	d	e
d	b	d	d	b	e
e	e	e	e	e	e

$$\leqslant = \{(a,a),(b,b),(b,c),(b,e),(c,c),(d,a),(d,d),(d,e),(e,e)\}.$$

The covering relation and the figure of S are given by:

$$< \, = \{(b,c),(b,e),(d,a),(d,e)\}$$



We have $b \preceq_I a$, but $b \leqslant a$ is false.

Theorem 2.6. *A subset A of an ordered semigroup $(S, \cdot, \leqslant)$ is a two-sided base of S if and only if it satisfies the following conditions*:

(i) *for any x in S there exists a in A such that $x \preceq_I a$;*

(ii) *for any $a, b \in A$, if $a \neq b$, then neither $a \preceq_I b$ nor $b \preceq_I a$.*

Proof. Assume that A is a two-sided base of S. If $x \in S$, then $x \in I(A)$; hence $x \preceq_I a$ for some a in A. This shows that (i) holds. Let a, b be elements of A such $a \neq b$. Suppose $a \preceq_I b$. We set $B = A \setminus \{a\}$. Then $b \in B$. Let x be an element of S. By (i), there exists c in A such that $x \preceq_I c$. There are two cases to consider. If $c \neq a$, then $c \in B$; thus $I(x) \subseteq I(c) \subseteq I(B)$. Hence $S = I(B)$. This is a contradiction. If $c = a$, then $x \preceq_I b$; hence $x \in I(B)$ since $b \in B$. We have $S = I(B)$. This is a contradiction. The case $b \preceq_I a$ is proved similarly. Thus (ii) holds true.

Conversely, assume that the conditions (i) and (ii) hold. It follows from (i) that $S = I(A)$. Suppose that $S = I(B)$ for some a proper subset B of A. Let a be an element of $A \setminus B$. We have $a \in I(B)$. By (iii), $a \in (SB \cup BS \cup SBS]$. This implies that $a \preceq_I b$ for some b in B. This contradicts to (ii). Hence A is a two-sided base of S. □

Lemma 2.7. *Let A be a two-sided base of an ordered semigroup $(S, \cdot, \leqslant)$. For any a, b in A, if $a \in (Sb \cup bS \cup SbS]$, then $a = b$.*

Proof. Let a, b be any elements of A such that $a \in (Sb \cup bS \cup SAS]$ and $a \neq b$. We set $B = A \setminus \{a\}$. Then $b \in B$. Since

$$I(a) \subseteq (Sb \cup bS \cup SbS] \subseteq I(b) \subseteq I(B),$$

it follows that $I(A) \subseteq I(B)$, and so $S = I(B)$. This is a contradiction since A is a two-sided base of S. Hence $a = b$. □

Theorem 2.8. *Let A be a two-sided base of an ordered semigroup $(S, \cdot, \leqslant)$ such that $I(a) = I(b)$ for some a in A and b in S. If $a \neq b$, then S contains at least two two-sided bases.*

Proof. Assume that $a \neq b$. Suppose $b \in A$. Since $a \preceq_I b$, it follows by Theorem 2.6 that $a \in (Sb \cup bS \cup SbS]$; hence $a = b$ by Lemma 2.7. This is a contradiction. Thus $b \in S \setminus A$. We set $A_1 = (A \setminus \{a\}) \cup \{b\}$. If A_1 is a two-sided base of S, then we obtain the assertion since $A_1 \neq A$. This is proved using Theorem 2.6 as follows.

Let $x \in A \setminus \{a\}$. If $x \preceq_I b$, then by $I(b) = I(a)$ it follows that $I(x) \subseteq I(a)$. By Lemma 2.7, $x = a$. This is a contradiction. Thus $x \preceq_I b$ is false. Similarly, if $b \preceq_I x$, then $b \preceq_I x$ is false. Let x be an element of S. Then there exists $c \in A$ such that $x \preceq_I c$. If $c \neq a$, then $c \in A_1$. If $c = a$, then $I(c) = I(b)$; hence $x \preceq_I b$. □

The following corollary follows directly from Theorem 2.8.

Corollary 2.9. *Let A be a two-sided base of an ordered semigroup $(S, \cdot, \leqslant)$, and let $a \in A$. If $I(a) = I(x)$ for some x in S, then x is in a two-sided base which is different from A.*

Theorem 2.10. *Any two two-sided bases of an ordered semigroup $(S, \cdot, \leqslant)$ have the same cardinality.*

Proof. Let A and B be two two-sided bases of an ordered semigroup $(S, \cdot, \leqslant)$. Let $a \in A$. Since B is a two-sided base of S, we have $a \preceq_I b$ for some b in B. Similarly, since A is a two-sided base of S we have $b \preceq_I a'$ for some a' in A. By $a \preceq_I a'$, $a = a'$. This implies $I(a) = I(b)$. Define a mapping

$$\varphi : A \to B \text{ by } \varphi(a) = b \text{ for all } a \text{ in } A.$$

If $a_1, a_2 \in A$ such that $\varphi(a_1) = \varphi(a_2)$, then $I(a_1) = I(a_2)$; hence $a_1 = a_2$ by Theorem 2.6. This shows that φ is one to one. Let $b \in B$. Then there exists a in A such that $b \preceq_I a$. Similarly, there exists b' in B such that $a \preceq_I b'$. Then $b \preceq_I b'$. Since $I(b) = I(b')$, so $I(a) = I(b)$. Thus φ is onto. □

In Example 2.3, it is easy to see that $\{b\}$ is a two-sided base of S, but it is not a subsemigroup of S. This shows that a two-sided base of an ordered semigroup need not to be a subsemigroup in general. An element e of an ordered semigroup $(S, \cdot, \leqslant)$ is called an *idempotent* if $e^2 = e$. The following theorem gives necessary and sufficient conditions of a two-sided base of S to be a subsemigroup of S.

Theorem 2.11. *Let A be a two-sided base of an ordered semigroup $(S, \cdot, \leqslant)$. Then A is a subsemigroup of S if and only if $A = \{a\}$ where $a^2 = a$.*

Proof. Assume that A is a subsemigroup of S. Let a, b be elements of A. Then $ab \in A$. Since $ab \in (Sb \cup bS \cup SbS]$, it follows by Lemma 2.7 that $a = b$. By $ab \in (Sa \cup aS \cup SaS]$, we have $ab = a$. Hence $a = b$. The converse statement is obvious. □

This is a consequence of Theorem 2.11.

Corollary 2.12. *Any ordered semigroup $(S, \cdot, \leqslant)$ containing a two-sided base which is a subsemigroup contains an idempotent element.*

Theorem 2.13. *Let $(S, \cdot, \leqslant)$ be an ordered semigroup, and let A be the union of all two-sided bases of S. If $S \setminus A$ is nonempty, then it is an ideal of S.*

Proof. Assume that $S \setminus A$ is nonempty. Let $a \in S \setminus A$, and let $x \in S$. To show that $xa \in S \setminus A$, we assume that $xa \in A$. Then $xa \in A_1$ for some a two-sided base A_1 of S. Let $xa = b$ for some b in A_1. Then $b \in Sa$; thus $I(b) \subseteq I(a)$. If $I(b) = I(a)$, then by Corollary 2.9 we have $a \in A$. This is a contradiction. Hence $b \prec_I a$. Since A_1 is a two-sided base, there exists c in A_1 such that $a \preceq_I c$. We have $b \prec_I a \preceq_I c$. This is a contradiction. Hence $xa \in S \setminus A$. Similarly, we have $ax \in S \setminus A$. Let $x \in S \setminus A$ and $y \in S$ such that $y \leqslant x$. If $y \in A$, then $y \in A_2$ for some a two-sided base A_2 of S. Let $z \in A_2$ be such that $x \preceq_I z$. Since $y \preceq_I x$, so $y \preceq_I z$. This is a contradiction. Hence $S \setminus A$ is an ideal of S. □

Theorem 2.14. *Let A be the union of all two-sided bases of an ordered semigroup $(S, \cdot, \leqslant)$ such that $\emptyset \neq A \subset S$. Let M^* be a proper ideal of S containing every proper ideal of S. The following statements are equivalent*:

(1) *$S \setminus A$ is a maximal ideal of S*;

(2) *$A \subseteq I(a)$ for every a in A*;

(3) $S \setminus A = M^*$;

(4) *Every two-sided bases of S is a singleton set.*

Proof. The proof is a modification of the proof of Theorem 6 in [2].

(1) $\Leftrightarrow$ (2). If there is an element a of A such that $A \subseteq I(a)$ is false, then $(S \setminus A) \cup I(a)$ is a proper two-sided ideal of S. This contradicts to the maximality of $S \setminus A$. Conversely, assume that for every element a in A, $A \subseteq I(a)$. By Theorem 2.13, $S \setminus A$ is an ideal of S. Let M be an ideal of S such that $S \setminus A \subset M \subset S$. Then $M \cap A$ is nonempty, i.e., there is an element c in $M \cap A$. We have

$$(Sc] \subseteq (SM] \subseteq M,\ (cS] \subseteq (MS] \subseteq M,\ (ScS] \subseteq (SMS] \subseteq (SM] \subseteq M.$$

Thus

$$S = (S \setminus A) \cup A \subseteq (S \setminus A) \cup I(c) \subseteq M.$$

This is a contradiction. Hence $S \setminus A$ is a maximal ideal of S.

(3) $\Leftrightarrow$ (4). Assume that $S \setminus A = M^*$. Let $a \in A$. Then $S \setminus A \subseteq I(a)$. Since $A \subseteq I(a)$, so $S = I(a)$. Hence $\{a\}$ is a two-sided base of S. Conversely, assume that every two-sided base of S is a singleton set. Then $S = I(a)$ for all a in A. Let M be an ideal of S such that M is not contained in $S \setminus A$. Then there exists x in $A \cap M$. Since

$$(Sx] \subseteq (SM] \subseteq M,\ (xS] \subseteq (MS] \subseteq M \text{ and } (SxS] \subseteq (SMS] \subseteq M,$$

we have $S = I(x) \subseteq M$, and so $S = M$.

(1) $\Leftrightarrow$ (3). Assume that $S \setminus A$ is a maximal ideal of S. Let M be an ideal of S such that M is not contained in $S \setminus A$. Then $M = A \cup X$ for some $X \subseteq S \setminus A$. This implies that $M = S$. Thus $S \setminus A = M^*$. The converse is obvious. □

References

[1] **G. Birkhoff**, *Lattice Theory*, 25, Rhode Island, American Mathematical Society Colloquium Publications, Am. Math. Soc, Providence, 1984.

[2] **I. Fabrici**, *Two-sided bases of semigroups*, Matematicky casopis, **25** (1975), 173-178.

[3] **N. Kehayopulu**, *On weakly prime ideals of ordered semigroups*, Math. Japonica, **35** (1990), 1051 – 1056.

[4] **N. Kehayopulu**, **M. Tsingelis**, *A note on ordered groupoids-semigroups*, Scientiae Math., **3** (2000), 251 – 255.

[5] **N. Kehayopulu**, *On completely regular ordered semigroups*, Scinetiae Math., **1** (1998), 27 − 32.

[6] **N. Kehayopulu and M. Tsingelis**, *On subdirectly irreducible ordered semigroups*, Semigroup Forum, **50** (1995), 161 − 177.

[7] **N. Kehayopulu and M. Tsingelis**, *On left regular ordered semigroups*, Southeast Asian Bull. Math., **25** (2002), 609 − 615.

[8] **T. Tamura**, *One sided-bases and translations of a semigroup*, Math. Japan, **3** (1955), 137 − 141.

[9] **X. Y. Xie and J. Tang**, *Regular ordered semigroups and intra-regular ordered semigroups in terms of fuzzy subsets*, Iranian J. Fuzzy Systems, **7** (2010), 121 − 140.

Received January 14, 2014

Department of Mathematics
Faculty of Science
Khon Kaen University
Khon Kaen 40002
Thailand
E-mail: thacha@kku.ac.th

Quasigroups and Relates Systems **22** (2014), 67 − 70

Free covering semigroups of topological n-ary semigroups

Wieslaw A. Dudek and *Vladimir V. Mukhin*

Abstract. Connections between the topology of an n-ary semigroup and the topology of its free covering semigroup are described.

Investigations of topological n-ary groups and n-ary semigroups were initiated by Čupona in 1970 when he studied the problem of embedding of some topological universal algebras into topological semigroups (see [4, 5] and [7]). By the way it turned out that topological n-ary groups may be defined in various ways. For $n > 2$ these definitiona are equivalent, but for $n = 2$ some of these are not valid (for details see [14]). Properties of topological n-ary groups are strongly connected with the properties of their retracts [15]. On the other hand, each toplogical n-ary group can be embedded into some topological group (see [3] and [6]). The topology of this covering group is strongly connected with the topology of an initial n-ary group. Namely, Endres proved in [10] that topological properties of this topological group may be moved to its initial topological n-ary groups and conversely. For n-ary semigroups the situation is more complicated.

The topology on the n-ary semigroups can be defined by the systems of some maps [1]. Conditions under which a topology determined by the families of left invariant derivations is compatible with the n-ary operation are given in [9]. The problem of the embedding of some locally compact n-ary semigroups into locally compact n-ary groups is studied in [12]. Conditions under which an n-ary semigroup with a locally compact topology can be topologically embedded into a locally compact binary group as an open set were found in [11]. In [13] for topological n-ary semigrous in which all translations (shifts) are continous and open the covering semigroup is constructed in this way that the topology of an initial topological n-ary semigroup can be extended to a topology compatible with the semigroup operation on the covering semigroup.

Below we describe connections between the the topology of an n-ary semigroup and the topology of its free covering semigroup. For this we use the construction of free covering semigroup proposed in [8] and the following proposition from [2] (Chapter 1, §6, Proposition 6).

2010 Mathematics Subject Classification: 20N15
Keywords: n-ary semigroup, covering semigroup, topological semigroup.

Proposition 1. *Let ρ be an equivalence relation on a topological space X. Then a map f of X/ρ into a topological space Y is continuous if and only if $f \circ \varphi$, where φ is a cannonical map of X onto X/ρ, is continuous on X.* $\square$

Let $(G, [\,])$ be an n-ary semigroup. Further, for simplicity we will omit the operator symbol $[\,]$ and instead of $[...[[x_1 \ldots x_n]x_{n+1} \ldots x_{2n-1}]x_{2n} \ldots x_p]$, where $p = k(n-1)+1$, we will write $[x_1, \ldots, x_p]$. Additionaly we put $[x] = x$ for $k = 0$.

Let F be the set of non-empty words over G, i.e.,

$$F = \bigcup_{k \in \mathbb{N}} G^k = \{(x_1, \ldots, x_k) \mid k \in \mathbb{N}, x_j \in G\}.$$

On F we introduce the product $(x_1, \ldots, x_k) \diamond (y_1, \ldots, y_t) = (x_1, \ldots, x_k, y_1, \ldots, y_t)$. Then F with this product is a free semigroup.

Two elements $\alpha = (a_1, \ldots, a_p)$, $\beta = (b_1, \ldots, b_q)$ of F are *strongly linked* if and only if there exists an element $(d_1, \ldots, d_t) \in F$ and two sequences of non-negative integers $k_1 < k_2 < \ldots, k_p = t$, $m_1 < m_2 < \ldots < m_q = t$ such that

$$a_1 = [d_1 \ldots d_{k_1}], \quad a_2 = [d_{k_1+1} \ldots d_{k_2}], \ \ldots \ a_p = [d_{k_{p-1}+1} \ldots d_{k_p}],$$

$$b_1 = [d_1 \ldots d_{m_1}], \quad b_2 = [d_{m_1+1} \ldots d_{m_2}], \ \ldots \ b_q = [d_{m_{p-1}+1} \ldots d_{m_p}].$$

Two strongly linked elements $\alpha, \beta \in F$ are denoted by $\alpha \sim \beta$. The relation $\sim$ is reflexive and symmetric. Its transitive closure $\approx$ is a congruence on F (for details see [8]). The quotient semigroup $(F/\!\approx, *)$ is called the *free covering semigroup* of an n-ary semigroup $(G, [\,])$ and is denoted by F^*. The equivalence class of α, i.e., an element of F^* induced by α, is denoted by α^*.

The set $G^* = \{a^* \mid a \in G\}$ is an n-ary subsemigroup of $F/\!\approx$ with the operation

$$[a_1^* a_2^* \ldots a_n^*] = a_1^* * a_2^* * \cdots * a_n^*.$$

The canonical mapping $\varphi(a) = a^*$ is an isomorphism from G onto G^*. So, we can identify the element $a \in G$ with the class a^* and G with G^*. Moreover, since $a^* = \beta^*$ if and only if $a = [b_1 \ldots b_q]$, we can write F^* in the form

$$F^* = G_1 \cup G_2 \cup G_3 \cup \ldots \cup G_{n-1},$$

where $G_j = \{a_1 * a_2 * \cdots * a_j \mid a_1, \ldots, a_j \in G\}$ and $G_i \cap G_j = \emptyset$ for $i \neq j$.

Let τ be a topology on G and let τ_k be a topology on the Cartesian product G^k obtained as a product of k topologies τ defined on k factors G. The sum of all topologies τ_k, $(k = 1, 2, 3, \ldots)$, where $\tau_1 = \tau$, is denoted by $\tau_{_F}$. By $\tau_{_{F^*}}$ we denote the factor topology on a free covering semigroup F^*.

Theorem 1. *Let $(G, [\,])$ be an n-ary semigroup. Then:*

1) *The semigroup $(F, \diamond)$ endowed with a topology $\tau_{_F}$ is a topological semigroup.*
2) *Each subset G^k is an open-closed subset of a topological space $(F^*, \tau_{_{F^*}})$.*

3) *The free covering semigroup* $(F^*, *)$ *endowed with the topology* τ_{F^*} *has continuous left and right shifts.*

Proof. The first statement is obvious. The second follows from the fact that

$$\varphi^{-1}(G_i) = \bigcup_{k=0}^{\infty} G^{k(n-1)+i} \in \tau_F$$

and it are saturated by the relation $\approx$.

To prove the third statement observe that each right shift $R_a(x) = x \diamond a$ by an element $a \in F$ is continuous on a semigroup $(F, \diamond)$. Therefore, the composition $\varphi \circ R_a$ is continuous. Since $\varphi \circ R_a = r_a \circ \varphi$, where $r_a(x^*) = x^* * a^*$, Proposition 1 implies that $r_a : F^* \to F^*$ also is continuous.

Similarly we can prove the continuity of each left shift of F^*. $\square$

An n-ary semigroup $(G, [\ ])$ with a topology τ is called a *topological n-ary semigroup* if (G, τ) is a topological space such that the n-ary operation $[\ ]$ is continuous (in all variables together).

Theorem 2. *Let* $(G, [\ ])$ *be a topological n-ary semigroup with the topology* τ. *Then the restriction of the topology* τ_{F^*} *to* G *coincides with the topology* τ.

Proof. Let $U \in \tau_{F^*}$ be an arbitrary non-empty subset of G. Then $\varphi^{-1}(U) \in \tau_F$. Hence, $U = \varphi^{-1}(U) \cap G \in \tau$.

Conversely, let $U \in \tau$ and $\alpha = (a_1, \ldots, a_p)$, where $p = t(n-1)+1$, be an arbitrary element of $\varphi^{-1}(U)$. Then $a_1^* * a_2^* * \cdots * a_p^* \in U$. Thus $a_1^* * a_2^* * \cdots * a_p^* = [a_1 a_2 \ldots a_p]$. Since the operation $[\ ]$ is continuous, there are some open (in the topology τ) neighborhoods $V_1, \ldots, V_p$ of points $a_1^*, \ldots, a_p^*$ such that for all $x_i \in V_i$, $i = 1, \ldots, p$, we have $[x_1 \ldots x_p] \in U$. Consequently, $\varphi(x_1, \ldots, x_p) = x_1^* * \cdots * x_p^* = [x_1 \ldots x_p] \in U$, i.e., $\varphi^{-1}(U) \supset V_1 \times \cdots \times V_p \in \tau_F$. Hence, $\varphi^{-1}(U) \in \tau_F$ and $\varphi^{-1}(U)$ is saturated by the relation $\approx$. This implies that $U \in \tau_{F^*}$. $\square$

It is clear that the Cartesian product $F \times F$ with the operation $(x, y) \otimes (s, t) = (x \diamond s, y \diamond t)$ and the topology $\tau_{F\times F} = \tau_F \times \tau_F$ is a topological semigroup.

Consider on $F \times F$ the relation $\approx_{F\times F}$ defined by

$$(x, y) \approx_{F\times F} (s, t) \iff x \approx s \text{ and } y \approx t.$$

This relation is a congruence on $F \times F$ and $(F \times F)^* = F \times F/{\approx_{F\times F}}$ with the standard factor-operation $*$ is a semigroup. Then obviously

$$(x, y)^* * (s, f)^* = ((x, y) \otimes (s, t))^* = (x \diamond s, y \diamond t)^* = (x^* * s^*, y^* * t^*)$$

and $(x, y)^* = (x^*, y^*)$. Therefore $(F \times F)^* = F^* \times F^*$. Hence, the canonical map ω of $F \times F$ onto $(F \times F)^*$ has the form $\omega = (\varphi, \varphi)$.

By $\tau_{(F\times F)^*}$ we denote the factor topology on the semigroup $(F \times F)^*$.

Theorem 3. *The operation* $*$ *from* $F^* \times F^*$ *with the topology* $\tau_{(F\times F)^*}$ *to* F^* *is a continuous.*

Proof. Since $\diamond$, φ, ω are continuous and $(\varphi\circ\diamond)(\alpha,\beta)=(*\circ\omega)(\alpha,\beta)$ for all $\alpha,\beta\in F$, the proof follows from Proposition 1. $\square$

Corollary 1. *If the topologies $\tau_{(F\times F)^*}$ and $\tau_{F^*}\times\tau_{F^*}$ coincides, then the semigroup $(F^*,*)$ endowed with the topology τ_{F^*} is a topological semigroup.* $\square$

References

[1] **H. Boujouf**, *The topology in the n-ary semigroups, definable by the deflection systems*, (Russian), Voprosy Algebry **10** (1996), 187 – 189.

[2] **N. Bourbaki**, *Topologie générale. Structures topologiques*, Hermann, Pais, 1965.

[3] **G. Crombez, G. Six**, *On topological n-groups*, Abh. Math. Sem. Univ. Hamburg **41** (1974), 115 – 124.

[4] **G. Čupona**, *Imbeddings of topological algebras into topological semigroups*, (Macedonian), Bull. Soc. Math. Phys. Macedoine **21** (1970), 37 – 42.

[5] **G. Čupona**, *On Cohn-Rebane's theorem*, (Macedonian), Fac. Sci. Nat. Univ. Kiril et Metodij, Skopje, Annuaire, Math. Phys. Chim. **20** (1970), 5 – 14.

[6] **G. Čupona**, *On topological n-groups*, Bull. Soc. Math. Phys. Macedoine Sci. and Arts, Contributions **6** (1974), 23 – 24.

[7] **G. Čupona**, *On a representation of algebras in semigroups*, Makedon. Akad. Nauk. Umet. Oddel. Prirod.-Mat. Nauk. Prilozi **10** (1978), 518.

[8] **G. Čupona, N. Celakoski**, *On representation of n-associatives into semigroups*, Maced. Akad. Sci. and Arts, Contributions **6** (1974), 23 – 24.

[9] **W. A. Dudek, V. V. Mukhin**, *On topological n-ary semigroups*, Quasigroups and Related Systems **3** (1996), 73 – 88.

[10] **N. Endres**, *On topological n-groups and their corresponding groups*, Discuss. Math. Algebra Stochastic Methods **15** (1995), 163 – 169.

[11] **V. V. Mukhin**, *On topological n-semigroups*, Quasigroups and Related Systems **4** (1997), 39 – 49.

[12] **V. V. Mukhin, H. Boujouf**, *On the embedding of n-ary abelian topological semigroups into n-ary topological groups*, (Russian), Voprosy Algebry **9** (1996), 157 – 160.

[13] **V. V. Mukhin, H. Boujouf**, *Topological n-ary semigroups*, (Russian), Vestsi Nats. Akad. Navuk Belarusi Ser. Fiz.-Mat. Navuk **1** (1999), 45 – 48.

[14] **S. A. Rusakov**, *Two definitions of a topological n-ary group*, (Russian), Voprosy Algeby **5** (1990), 86 – 91.

[15] **M. Žižvić**, *A topological analogue of the Hosszú–Gluskin theorem*, Mat. Vesnik **13(28)** (1976), 233 – 235.

Received June 21, 2013

W.A. Dudek
Institute of Mathematics, Wroclaw University of Technology, 50-370 Wroclaw, Poland
E-mail: wieslaw.dudek@pwr.edu.pl

V.V. Mukhin
Department of Mathematics, Cherepovets State University, 162 600 Cherepovets, Russia
E-mail: mukhin@chsu.ru

Quasigroups and Related Systems **22** (2014), 71 − 80

On δ-primary co-ideals of a commutative semiring

Shahabaddin Ebrahimi Atani, Saboura Dolati Pish Hesari and Mehdi Khoramdel

Abstract. We introduce the notion of a δ-primary co-ideal of a commutative semiring R and study some of it properties. Here δ is a mapping that assigns to each co-ideal J a co-ideal $\delta(J)$ of the same semiring. We investigate the relationship between the minimal prime co-ideals of R/I and $\delta(I)/I$, when I is a δ-primary Q-co-ideal. We also prove that every identity summand of R/I is contained in $\delta(I)/I$ and $\delta(I)$ contains all minimal prime co-ideals which contains I.

1. Introduction

The most trivial example of a semiring which is not a ring is the first algebraic structure we encounter in life: the set of nonnegative integers $\mathbb{N}$, with the usual addition and multiplication. Similarly, the set of nonnegative real numbers $\mathbb{R}^+$ with the usual addition and multiplication is a semiring which is not a ring. The nontrivial examples of semirings first appear in the work of Richard Dedekind in 1894, in connection with the algebra of ideals of a commutative ring and were later studied independently by algebraists, especially by H. S. Vandiver, who worked very hard to get them accepted as a fundamental algebraic structure, being basically the best structure which includes both rings and bounded distributive lattices. Semirings have been found useful for solving problems in different areas of applied mathematics and information sciences, since the structure of a semiring provides an algebraic framework for modelling and studying the key factors in these applied areas and, hence, ought to be in the literature [9, 11].

In this paper, we introduce the notion of co-ideal expansion and δ-primary co-ideals that is motivated from the notion of δ-primary ideals in semirings (resp. rings) [2] (resp. [7]). A number of results concerning of these class of co-ideals are given. For example, we investigate the relationship between the minimal prime co-ideals of R/I and $\delta(I)/I$, when I is a δ-primary Q-co-ideal. We also prove that I is δ-primary if and only if every identity-summand element of R/I is contained in $\delta(I)/I$.

In order to make this paper easier to follow, we recall various notions which will be used in the sequel. A commutative semiring R is defined as an algebraic system $(R, +, \cdot)$ such that $(R, +)$ and $(R, \cdot)$ are commutative semigroups, connected

2010 MSC: 16Y60
Keywords: Semiring, δ-primary co-ideal, minimal prime co-ideal, identity-summand elements

by $a(b+c) = ab+ac$ for all $a, b, c \in R$, and there exist $0, 1 \in R$ such that $r+0 = r$, $r0 = 0r = 0$ and $r1 = 1r = r$ for each $r \in R$. In this paper all semirings considered will be assumed to be commutative semirings with non-zero identity.

Definition 1.1. Let R be a semiring.

• A nonempty subset I of R is called *co-ideal*, denoted by $I \trianglelefteq^c R$, if it is closed under multiplication and satisfies the condition $r + a \in I$ for all $a \in I$ and $r \in R$ (clearly, $0 \in I$ if and only if $I = R$) [4].

• A co-ideal I of R is called *subtractive* if $x, xy \in I$, then $y \in I$ (so every subtractive co-ideal is a strong co-ideal) [4].

• A proper co-ideal P of R is called *prime* if $x + y \in P$, then $x \in P$ or $y \in P$. A proper co-ideal I of R is called *primary* if $x+y \in I$, then $x \in I$ or $y \in$ co-rad(I) $= \{r \in R : nr \in I$ for some positive integer $n\}$ [4].

• A semiring R is called *co-semidomain*, if $a + b = 1$ $(a, b \in R)$, then either $a = 1$ or $b = 1$ [4].

• We say that a subset $T \subseteq R$ is *additively closed* if $0 \in T$ and $a + b \in T$ for all $a, b \in T$.

• If D is an arbitrary nonempty subset of R, then the set $F(D)$ consisting of all elements of R of the form $d_1 d_2 \cdots d_n + r$ (with $d_i \in D$ for all $1 \leqslant i \leqslant n$ and $r \in R$) is a co-ideal of R containing D [4, 11].

• A semiring R is called an *I-semiring* if $r + 1 = 1$ for all $r \in R$ [6].

A strong co-ideal I of a semiring R is called a *partitioning strong co-ideal* (*Q-strong co-ideal*) if there exists a subset Q of R such that $R = \cup\{qI : q \in Q\}$, where $qI = \{qt : t \in I\}$ and if $q_1, q_2 \in Q$, then $(q_1 I) \cap (q_2 I) \neq \emptyset$ if and only if $q_1 = q_2$ [4]. Let I be a Q-strong co-ideal of a semiring R and let $R/I = \{qI : q \in Q\}$. Then R/I forms a semiring under the binary operations $\oplus$ and $\odot$ defined as follows: $(q_1 I) \oplus (q_2 I) = q_3 I$, where q_3 is the unique element in Q such that $(q_1 I + q_2 I) \subseteq q_3 I$, and $(q_1 I) \odot (q_2 I) = q_3 I$, where q_3 is the unique element in Q such that $(q_1 q_2) I \subseteq q_3 I$ [4]. If q_e is the unique element in Q such that $1 \in q_e I$, then $q_e I = I$ is the identity of R/I [4]. Note that every Q-strong co-ideal is subtractive [4].

Throughout this paper we shall assume unless otherwise stated, that $q_0 I$ (resp. $q_e I$) is the zero element (resp. the identity element) of R/I.

2. Definition and basic structure

We begin with the key definition of this paper.

Definition 2.1. Let R be a semiring with co-Id(R) its set of co-ideals.

(i) A *co-ideal expansion* is a function δ : co-Id$(R) \longrightarrow$ co-Id(R), which satisfies the following conditions:

(1) $I \subseteq \delta(I)$ for each co-ideal I of R;

(2) $I \subseteq J$ implies $\delta(I) \subseteq \delta(J)$ for all co-ideals I, J of R.

(*ii*) A *Q-co-ideal* (resp. *subtractive co-ideal*) *expansion* is a co-ideal expansion which assigns to each Q-co-ideal (resp. subtractive co-ideal) I of a semiring R to another Q-co-ideal (resp. subtractive co-ideal) $\delta(I)$ of the same semiring.

Remark 2.2. Since the intersection of any collection of co-ideals is a co-ideal of R, the intersection of any collection of co-ideal expansions is a co-ideal expansion.

The proof of the following lemma is well-known, but we give the details for convenience.

Lemma 2.3. *If I is a Q-strong co-ideal of R and q_eI is the identity element in R/I, then $q_eI \oplus qI = q_eI$ and $qI \oplus qI = qI$ for each $qI \in R/I$.*

Proof. Let $q_eI \oplus qI = q'I$, where q' is the unique element in Q such that $q_eI + qI \subseteq q'I$. Since I is co-ideal, $q_eI + qI \subseteq I = q_eI$ which gives $q'I = q_eI = I$. Finally, $qI \oplus qI = qI \odot (q_eI \oplus q_eI) = qI \odot q_eI = qI$. □

Proposition 2.4. *Let I be a co-ideal of a semiring R.*

(1) *The set* $\mathrm{cl}(I) = \{a \in R : ac = d \ for\ some\ c, d \in I\}$ *is a co-ideal of R (we call* $\mathrm{cl}(I)$ *the co-closure of I).*

(2) *I is subtractive if and only if* $\mathrm{cl}(I) = I$.

Proof. (1). Let $a_1, a_2 \in \mathrm{cl}(I)$; we show that $a_1a_2 \in \mathrm{cl}(I)$. By assumption, there exist $c_1, c_2, d_1, d_2 \in I$ such that $a_1c_1 = d_1$, $a_2c_2 = d_2$, hence $(a_1a_2)(c_1c_2) = d_1d_2$. Since I is a co-ideal of R, we have $a_1a_2 \in \mathrm{cl}(I)$. Now, let $a \in \mathrm{cl}(I)$ and $r \in R$; we show that $a+r \in \mathrm{cl}(I)$. Since $a \in \mathrm{cl}(I)$, there exist $c, d \in I$ such that $ac = d$. As I is a co-ideal of R, $(a + r)c = ac + cr \in I$; so $a + r \in \mathrm{cl}(I)$. Thus $\mathrm{cl}(I)$ is a co-ideal of a semiring R.

(2). Assume that I is a subtractive co-ideal of R (so it is a strong co-ideal) and let $x \in I$. Then $x = x1 \in I$ gives $I \subseteq \mathrm{cl}(I)$. For the reverse incusion, let $y \in \mathrm{cl}(I)$. Then $yc \in I$ for some $c \in I$; hence $y \in I$ since I is subtractive, and so we have equality. The other implication is clear. □

Example 2.5. (1) For each $I \in \text{co-Id}(R)$, define $\delta_1(I) = I$, $\delta_2(I) = \text{co-rad}(I)$ and $\delta_3(I) = \mathrm{cl}(I)$. Then δ_1, δ_2 and δ_3 are expansions of co-ideals.

(2) By [4, Proposition 2.1], if I is a proper co-ideal of R, then there exists a maximal co-ideal M of R such that $I \subseteq M$. Now for each proper co-ideal I, let $\delta_4(I)$ be the intersection of all maximal co-ideals containing I, and $\delta_4(R) = R$. Then δ_4 is an expansion of co-ideals. □

Theorem 2.6. Let R be a semiring.

(1) $\delta_1(I) \subseteq \delta_2(I) \subseteq \delta_3(I) \subseteq \delta_4(I)$ for each strong co-ideal I of R.

(2) If I is a subtractive co-ideal of R, then $\delta_1(I) = \delta_2(I) = \delta_3(I)$.

(3) δ_1, δ_2 and δ_3 are Q-co-ideal expansions.

Proof. (1). It is clear that $\delta_1(I) \subseteq \delta_2(I)$. Let $x \in \delta_2(I) = \text{co-rad}(I)$. So there exists $n \in \mathbb{N}$ such that $nx \in I$; hence $x \in cl(I)$, and so $\delta_2(I) \subseteq \delta_3(I)$. Now, let $x \in \delta_3(I) = cl(I)$. So there exists $a \in I$ such that $ax \in I$. It suffices to show that $x \in \cap M$, where M is a maximal co-ideal of R containing I. Let $x \notin M$ for some maximal co-ideal M of R containing I. So $F(M \cup \{x\}) = R$, which implies $0 = ax^n + r$ for some $a \in M$. Since $x \in \text{cl}(I)$, there exists $b \in I$ such that $bx \in I \subseteq M$. As M is a co-ideal of R, $0 = ab^n x^n + rb^n \in M$, a contradiction. Thus $\delta_3(I) \subseteq \delta_4(I)$.

(2). Suppose that I is a subtractive co-ideal of R and let $x \in \delta_2(I)$. So there exists $n \in \mathbb{N}$ such that $nx \in I$; hence $x \in I$, and so $\delta_1(I) = \delta_2(I)$ by (1). Now, let $x \in \text{cl}(I)$. Then $ax \in I$ for some $a \in I$, so $x \in I$ since I is subtractive. Thus $\delta_2(I) = \delta_3(I)$.

(3). It is clear that δ_1 is a Q-co-ideal expansion. We show that δ_2 is Q-co-ideal expansion. For this lLet I be a Q-co-ideal. Since we have $I \subseteq \text{co-rad}(I)$, $R = \cup\{qI : q \in Q\} \subseteq \cup\{q(\text{co-rad}(I)) : q \in Q\}$, so $R = \cup\{q(\text{co-rad}(I)) : q \in Q\}$. Let $x \in q_1(\text{co-rad}(I)) \cap q_2(\text{co-rad}(I))$, so $x = q_1a_1 = q_2a_2$, where $a_1, a_2 \in$co-rad(I). Thus there exist positive integer elements n, m such that $na_1, ma_2 \in I$. Suppose, without loss of generality, $n \geqslant m$. Hence $nx = q_1(na_1) = q_2(na_2) \in q_1I \cap q_2I$. So $q_1 = q_2$ which gives co-rad(I) is a Q-strong co-ideal of R.

Now, we show that δ_3 is a Q-co-ideal expansion. It is clear that we have $R = \cup\{q(\text{cl}(I)) : q \in Q\}$. Let $x \in q_1(\text{cl}(I)) \cap q_2(\text{cl}(I))$. So $x = q_1a_1 = q_2a_2$ for some $a_1, a_2 \in \text{cl}(I)$. Since I is a Q-co-ideal of R, there exists $q \in Q$ such that $xI \subseteq qI$. Since $a_1, a_2 \in \text{cl}(I)$, there exist $b_1, b_2 \in I$ such that $a_1b_1, a_2b_2 \in I$. Hence $xb_1 = q_1a_1b_1 \in q_1I \cap qI$ and $xb_2 = q_2a_2b_2 \in q_2I \cap qI$ for some $b_1, b_2 \in I$. Thus $q_1 = q = q_2$. □

3. δ-primary co-ideals

In this section, we investigate δ-primary co-ideals of a commutative semiring R which unify prime co-ideals and primary co-ideals of R.

Definition 3.1. Let R be a semiring and δ be a co-ideal expansion. A proper co-ideal I of a semiring R is called *δ-primary* if $a+b \in I$ and $a \notin I$, then $b \in \delta(I)$.

One can easily show that I is δ_1-primary if and only if it is a prime co-ideal of R and I is δ_2-primary if and only if I is a primary co-ideal of R.

Remark 3.2. Let I, J be co-ideals of the semiring R. The *co-ideal quotient* of I, J, denoted by (I : J), is the set $\{r \in R : r+J \subseteq I\} = \{r \in R : r+x \in I \text{ for all } x \in J\}$ such that (I : J) is closed under multiplication. For each $a \in R$, (I : a) denotes the set $\{r \in R : r + a \in I\}$ such that (I : a) is closed under multiplication. By [4, Lemma 2.4], $(I : J)$ is a co-ideal of R with $I \subseteq (I : J)$, and $(I : a)$ is a co-ideal of R for each $a \in R$. Also, by [4, Example 2.2], the condition "$(I : J)$ is closed under multiplication" is not superficial in the above definition. □

Theorem 3.3. *Let R be a semiring and δ be a co-ideal expansion.*

(1) *If P is a δ-primary co-ideal of R and $I \nsubseteq \delta(P)$, then $(P : I) = P$.*

(2) *For any δ-primary co-ideal P and any subset T of R, $(P : T)$ is δ-primary co-ideal of R.*

(3) *The union of any directed collection of δ-primary co-ideals is δ-primary.*

(4) *If $\delta(I) \subseteq \text{co-rad}(I)$ for every δ-primary co-ideal I, then $\delta(I) = \text{co-rad}(I)$.*

Proof. (1). It is clear that $P \subseteq (P : I)$. Let $x \in (P : I)$ and $a \in I \setminus \delta(P)$. So $x + a \in P$. Since P is δ-primary and $a \notin \delta(P)$, $x \in P$. So $(P : I) \subseteq P$, which gives $(P : I) = P$.

(2). Let $a + b \in (P : T)$ and $a \notin (P : T)$ for some $a, b \in R$. So $a + t \notin P$ and $a + b + t \in P$ for some $t \in T$. This implies $b \in \delta(P) \subseteq \delta(P : T)$ since P is δ-primary. Thus $(P : T)$ is a δ-primary co-ideal of R.

(3). Let $\sum = \{I_i \ : \ i \in D\}$ be a directed collection of primary co-ideals and $I = \cup_{i\in D} I_i$. Let $a + b \in I$ and $a \notin I$. So there is $i \in D$ such that $a + b \in I_i$ and $a \notin I_i$. So $b \in \delta(I_i) \subseteq \delta(I)$. Hence I is δ-primary.

(4). If $I = \text{co-rad}(I)$, then $\delta(I) = I = \text{co-rad}(I)$. Suppose $I \neq \text{co-rad}(I)$. Let $x \in \text{co-rad}(I)$. Then $nx \in I$ for some the least positive integer $n > 1$. Now $nx \in I$ and $(n - 1)x \notin I$ gives $x \in \delta(I)$, and so we have equality. □

Definition 3.4. Let R be a semiring. A co-ideal expansion δ is said to be *intersection preserving* if $\delta(I \cap J) = \delta(I) \cap \delta(J)$ for all co-ideals I, J of R.

Theorem 3.5. *Let R be a semiring.*

(1) *$\delta_1, \delta_2, \delta_3$ and δ_4 are intersection preserving co-ideal expansions.*

(2) *Assume that δ is an intersection preserving co-ideal expansion and let $Q_1, \ldots, Q_n$ be δ-primary co-ideals of R with $P = \delta(Q_i)$ for all $1 \leqslant i \leqslant n$. Then $Q = \bigcap_{i=1}^{n} Q_i$ is δ-primary.*

Proof. (1). It is clear that δ_1 is intersection preserving co-ideal expansion. By [4, Lemma 2.2], δ_2 is intersection preserving co-ideal expansion. We show that $\text{cl}(I \cap J) = \text{cl}(I) \cap \text{cl}(J)$. It is clear that $\text{cl}(I \cap J) \subseteq \text{cl}(I) \cap \text{cl}(J)$. Let $x \in \text{cl}(I) \cap \text{cl}(J)$. So there exist $a \in I$ and $b \in J$ such that $ax \in I$ and $bx \in J$. Since I, J are co-ideals of R, $a + b \in I \cap J$. Hence $x(a + b) = xa + xb \in I \cap J$, so $x \in \text{cl}(I \cap J)$. Thus $\text{cl}(I \cap J) = \text{cl}(I) \cap \text{cl}(J)$. By an argument like that in [2, Lemma 2.2], $\delta_4(I \cap J) = \delta_4(I) \cap \delta_4(J)$.

(2). Let $x + y \in Q$ and $x \notin Q$. So $x \notin Q_i$ for some $1 \leqslant i \leqslant n$. Since $x + y \in Q_i$ and Q_i is δ-primary, $y \in \delta(Q_i)$. As δ is intersection preserving, $\delta(Q) = \delta(\bigcap_{i=1}^{n} Q_i) = \bigcap_{i=1}^{n} \delta(Q_i) = P$, we have $y \in \delta(Q)$. Thus Q is δ-primary. □

Definition 3.6. Let R be a semiring with co-ideal expansion δ. An element x of R is called *δ-co-nilpotent* if $x \in \delta(F(\{1\}))$.

Remark 3.7. Let I be a Q-strong co-ideal of a semiring R with a subtractive co-ideal expansion δ. Then an inspection will show that $\overline{\delta}: \mathrm{Id}(R/I) \to \mathrm{Id}(R/I)$ is a subtractive co-ideal expansion of R/I, where $\overline{\delta}(J/I) = \delta(J)/I$ for each co-ideal J/I of R/I (see [4, Theorem 3.4 and Theorem 3.5]). So $\overline{\delta}(\{q_e I\}) = \overline{\delta}(\{I\}) = \delta(I)/I$.

Theorem 3.8. *Let I be a Q-strong co-ideal of a semiring R with a subtractive co-ideal expansion δ. If J is a subtractive co-ideal of R with $J \supseteq I$, then J/I is a $\overline{\delta}$-primary co-ideal of R/I if and only if J is a δ-primary co-ideal of R.*

Proof. Suppose that J/I is a $\overline{\delta}$-primary co-ideal of R/I; we show J is a δ-primary co-ideal of R. Let $a + b \in J$ and $a \notin J$. Since I is a Q-strong co-ideal of R, there exist $q_1, q_2 \in Q$ such that $a \in q_1 I$ and $b \in q_2 I$. Let $q_1 I \oplus q_2 I = q_3 I$, where q_3 is the unique element of Q such that $q_1 I + q_2 I \subseteq q_3 I$. It follows that $a + b = q_3 d \in J$ for some $d \in I$; so $q_3 \in J$ since J is subtractive; hence $q_1 I \oplus q_2 I = q_3 I \in J/I$. Clearly, $q_1 I \notin J/I$. Now J/I $\overline{\delta}$-primary gives, $q_2 I \in \overline{\delta}(J/I) = \delta(J)/I$; so $q_2 \in \delta(J)$. Hence $b \in \delta(J)$.

Conversely, assume that J is a δ-primary co-ideal of R. We show J/I is $\overline{\delta}$-primary. Let $q_1 I \oplus q_2 I \in J/I$ and $q_1 I \notin J/I$ (so $q_1 \notin J$). Let q_3 be the unique element of Q such that $q_1 I \oplus q_2 I = q_3 I$, where $q_1 I + q_2 I \subseteq q_3 I$. Since $q_3 I \in J/I$, $q_3 \in J$. Therefore $q_1 + q_2 = q_3 j \in J$ for some $j \in I$. As J is δ-primary and $q_1 \notin J$, $q_2 \in \delta(J)$. Therefore $q_2 I \in \overline{\delta}(J/I) = \delta(J)/I$. Thus J/I is a $\overline{\delta}$-primary co-ideal of a semiring R. □

An element r of a commutative semiring R with identity is said to be *identity-summand* if there exists $1 \neq a \in R$ such that $r + a = 1$. The set of all identity-summand elements of R is denoted by $S(R)$.

Theorem 3.9. *Let I be a Q-strong co-ideal of a semiring R with a subtractive co-ideal expansion δ. Then the following statements are equivalent:*

(1) *I is δ-primary,*
(2) $S(R/I) \subseteq \{qI : q \in Q \cap \delta(I)\} = \delta(I)/I$,
(3) *every identity-summand of R/I is $\overline{\delta}$-co-nilpotent,*
(4) *$P/I \subseteq \delta(I)/I$ for every $P/I \in \min(R/I)$, where $\min(R/I)$ is the set of all minimal prime ideals of R/I.*

Proof. (1) $\Rightarrow$ (2). Let I be a δ-primary and $qI \in S(R/I)$. Hence there exists $I \neq q'I \in R/I$ such that $qI \oplus q'I = q_e I = I$; so $q + q' \in I$. Since I is δ-primary and $q' \notin I$, $q \in \delta(I)$. Thus $qI \in \delta(I)/I$.

(2) $\Rightarrow$ (3). If $qI \in S(R/I)$, then $qI \in \delta(I)/I$ by (2). By Remark 3.7, $\delta(I)/I = \overline{\delta}(\{q_e I\})$, which gives qI is $\overline{\delta}$-co-nilpotent.

(3) $\Rightarrow$ (1). Let $a + b \in I, a \notin I$. Since I is a Q-co-ideal of R, there exist $q_1, q_2 \in Q$ such that $a \in q_1 I, b \in q_2 I$. Let $q_1 I \oplus q_2 I = q_3 I$, where q_3 is the unique element of Q such that $q_1 I + q_2 I \subseteq q_3 I$. So $a + b \in q_3 I \cap I$, which gives $q_3 = q_e$. Hence $q_1 I \oplus q_2 I = q_e I = I$. So $q_2 I$ is an identity summand element of R/I. Thus

q_2I is δ-co-nilpotent, hence $q_2I \in \bar{\delta}(\{q_eI\}) = \delta(I)/I$, which implies $q_2 \in \delta(I)$. Hence $b \in q_2I \subseteq \delta(I)$.

(1) $\Rightarrow$ (4). Let $P/I \in \min(R/I)$. At first, we show that $R/I \setminus P/I = (P/I)^c$ is a maximal additively closed subset of R/I with $q_eI \notin (P/I)^c$. Set

$$\sum = \{S: \ (P/I)^c \subseteq S, \ S \ is \ an \ additively \ closed \ subset \ of \ R/I \ and \ q_eI \notin S\}$$

by Zorn's Lemma, has a maximal element M. Obviously, $(P/I)^c \subseteq M$.

Consider the set

$$\Delta = \{L: \ L/I \ is \ a \ co-ideal \ of \ R/I \ and \ L/I \cap M = \emptyset\}.$$

Since $\{I\}$ is a co-ideal of R/I and $\{I\} \cap M = \emptyset$, $\Delta \neq \emptyset$. By Zorn's Lemma, Δ has maximal element T/I.

We show that T/I is prime. Let $q_1I \oplus q_2I \in T/I$ and $q_1I, q_2I \notin T/I$. Then $T/I \subsetneqq J_i = F(T/I \cup \{q_iI\})$. Thus $J_i \cap M \neq \emptyset$ for each $i = 1, 2$. Let $X_i \in J_i \cap M$ for each $i = 1, 2$. We show $J_1 \cap J_2 = T/I$. It is clear that $T/I \subseteq J_1 \cap J_2$. For $qI \in J_1 \cap J_2$ we have

$$qI = r_1I \oplus c_1I \odot (q_1I)^n = r_2I \oplus c_2I \odot (q_2I)^m$$

for some $r_1I, r_2I \in R/I$, $c_1I, c_2I \in T/I$ and $n, m \in \mathbb{N}$. Since

$$c_1I \odot (q_1I \oplus q_2I)^n = c_1I \odot (q_1I)^n \oplus (q_2I) \odot (tI) \in T/I$$

for some $tI \in R/I$, we have

$$qI \oplus q_2I \odot tI = r_1I \oplus c_1I \odot (q_1I)^n \oplus (q_2I) \odot (tI) \in T/I.$$

Hence $(q_2I) \odot (tI) \in (T/I : qI)$.

It can be easily checked that $(T/I : qI)$ is a co-ideal of R. So $q_2I \odot tI \oplus q_2I \in (T/I : qI)$. By Lemma 2.3, $q_eI \oplus tI = tI$, hence

$$q_2I = q_2I(q_eI \oplus tI) = q_2I \odot tI \oplus q_2I \in T/I.$$

Therefore $(c_2I) \odot (q_2I)^m \in (T/I : qI)$. So $qI = r_2I \oplus c_2I \odot (q_2I)^m \in (T/I : qI)$, because $(T/I : qI)$ is a co-ideal of R/I. Thus $qI \oplus qI = qI \in T/I$. Therefore $J_1 \cap J_2 = T/I$. Hence $X_1 + X_2 \in T/I \cap M$, a contradiction. Thus $q_1I \in T/I$ or $q_2I \in T/I$, which gives T/I is a prime co-ideal of R/I. Since $T/I \cap M = \emptyset$, $M \subseteq (T/I)^c$. So $(P/I)^c \subseteq M \subseteq (T/I)^c$, which implies $T/I \subseteq P/I$. Since $P/I \in \min(R/I)$, $T/I = P/I$. Thus $(P/I)^c$ is a maximal additively closed subset of R/I which $I \notin (P/I)^c$.

Now, let $qI \in P/I$. Then

$$T = \{q'I \oplus n(qI) : I \neq q'I \in (P/I)^c, \ n \in \mathbb{N} \cup \{0\}\}$$

is an additively closed subset of R/I which properly contains $(P/I)^c$. But we showed that $(P/I)^c$ is a maximal additively closed subset of R/I which $I \notin (P/I)^c$. So $I \in T$. Hence $q'I \oplus n(qI) = I$ for some $q'I \in (P/I)^c$, $n \in \mathbb{N}$. Thus $q'I \oplus qI = I$ by Lemma 2.3. So $q+q' \in I$. Since $q' \notin I$ and I is δ-primary, $q \in \delta(I)$ we conclude that $qI \in \delta(I)/I$.

(4) $\Rightarrow$ (1). Let $a+b \in I$ and $a \notin I$. Since I is a Q-strong co-ideal of R, there exist $q_1, q_2 \in Q$ such that $a \in q_1I, b \in q_2I$. Let $q_1I \oplus q_2I = q_3I$. Since $a+b \in q_eI \cap q_3I$, $q_3 = q_e$. So $q_1I \oplus q_2I = I$. It is clear that $I \in P/I$. So $q_1I \oplus q_2I \in P/I$. Hence $q_1I \in P/I$ or $q_2I \in P/I$. Since $P/I \subseteq \delta(I)/I$, $q_1 \in \delta(I)$ or $q_2 \in \delta(I)$. □

Theorem 3.10. *Let I be a Q-strong co-ideal of a semiring R with a subtractive co-ideal expansion δ. If I is δ-primary, then $P \subseteq \delta(I)$ for every subtractive co-ideal $P \in \min(I)$. The converse holds if $\min(R/I)$ is finite.*

Proof. At first we show that if P is subtractive and $P \in \min(I)$, then $P/I \in \min(R/I)$. Let T/I be a prime co-ideal of R/I and $T/I \subseteq P/I$. Since R/I is I-semiring, T/I is a subtractive co-ideal of R/I by [6, Proposition 2.5]. So $T/I = L/I$ where L is a subtractive prime co-ideal of R and $I \subseteq L$ by [4, Theorem 3.6, Theorem 3.7]. We show $L \subseteq P$. Let $x \in L$. Since I is a Q-co-ideal of R, $x = qa$ for some $q \in Q$ and $a \in I$. Because L is subtractive, $q \in L$. Thus $qI \in L/I \subseteq P/I$. Hence $q \in P$. So $x \in P$. Thus $L \subseteq P$ which implies $L = P$ because $P \in \min(I)$. Therefore $P/I = L/I = T/I$. Now, let $x \in P$. Since I is a Q-co-ideal of R, $x = qa$ for some $q \in Q$ and $a \in I$. Since P is subtractive $q \in P$. Hence $qI \in P/I$, where $P/I \in \min(R/I)$ by the above argument. Hence $qI \in \delta(I)/I$ by Theorem 3.9. Thus $q \in \delta(I)$, which gives $x \in \delta(I)$.

Conversely, by [6,Theorem 2.8], $I = \cap_\Lambda P_\alpha/I$, where $P_\alpha/I \in \min(R/I)$. By [6, Proposition 2.5], P_α/I is a subtractive co-ideal of R/I for each $\alpha \in \Lambda$. So $P_\alpha/I = Q\alpha/I$, where Q_α is a subtractive co-ideal of R and $I \subseteq Q_\alpha$. We show that $I = \cap_\Lambda Q_\alpha$. It is clear that $I \subseteq \cap_\Lambda Q_\alpha$. Let $x \in \cap_\Lambda Q_\alpha$. Since I is a Q-co-ideal of R, $x = qa$ for some $q \in Q$ and $a \in I$. So $q \in \cap_\Lambda Q_\alpha$, because $Q_\alpha^{,}$ s are subtractive co-ideals of R. Thus $qI \in \cap Q_\alpha/I = \cap P_\alpha/I = \{q_eI\}$, hence $q = q_e$ and $x \in I$. Therefore $I = \cap_\Lambda Q_\alpha$. Let $L \in \min(I)$. Hence $I = \cap_\Lambda Q_\alpha \subseteq L$. Since $\min(R/I)$ is finite, Λ is finite, which gives $Q_\alpha \subseteq L$, because Q_α is prime by [4, Theorem 3.7]. Thus $Q_\alpha = L$. Now, we show that I is δ-primary. Let $a+b \in I$ for some $a, b \in R$. Hence $a+b \in Q_\alpha$, where Q_α is a subtractive co-ideal and $Q_\alpha \in \min(I)$. By assumption, $Q_\alpha \subseteq \delta(I)$. Because Q_α is prime $a \in Q_\alpha \subseteq \delta(I)$ or $b \in Q_\alpha \subseteq \delta(I)$, which gives I is δ-primary. □

Definition 3.11. A co-ideal I of a semiring R with a co-ideal expansion δ is called a *δ-weakly primary* if $1 \neq a+b \in I$, then $a \in I$ or $b \in \delta(I)$ for each $a, b \in R$.

Theorem 3.12. *Let J be a subtractive co-ideal of an I-semiring R with a subtractive co-ideal expansion δ. Then the following are equivalent.*

(1) *J is δ-weakly primary.*

(2) *For each* $a \in R \setminus \delta(J)$, $(J : a) = J \cup (1 : a)$.
(3) $(J : a) = J$ *or* $(J : a) = (1 : a)$.

Proof. (1) $\Rightarrow$ (2). Let $a \in R \setminus \delta(J)$ and $b \in (J : a)$. Then $a + b \in J$. If $a + b = 1$, then $b \in (1 : a)$. If $a + b \neq 1$, then J δ-weakly primary gives $b \in J$. So $(J : a) \subseteq J \cup (1 : a)$. The converse inclusion is clear.

(2) $\Rightarrow$ (3). Let $(J : a) \neq J$ and $(J : a) \neq (1 : a)$. Then there exists $d \in (J : a)$ and $c \in (J : a)$ such that $d \notin J$ and $c \notin J$. Since J is subtractive, $(J : a)$ is a subtractive co-ideal of R, $cd \in (J : a)$. Therefore $cd \in J$ or $cd \in (1 : a)$. This implies that $c = cd + c \in J$ or $d = cd + d \in (1 : a)$, a contradiction.

(3) $\Rightarrow$ (1). Let $1 \neq a + b \in J$ and $a \notin \delta(J)$. Then $b \in (J : a) = J$. $\square$

Theorem 3.13. *Let R be an I-semiring with a subtractive co-ideal expansion δ. If J is a subtractive δ-weakly primary co-ideal of R which is not δ-primary, then $J = \{1\}$.*

Proof. Let $\{1\} \neq J$. We show that J is δ-primary co-ideal of R. Let $a + b \in J$. If $a + b \neq 1$, then J δ-weakly primary gives $a \in J$ or $b \in \delta(J)$. So we may assume that $a + b = 1$. As $J \neq \{1\}$, there exists $1 \neq c \in J$. So $1 \neq c = ac + bc \in J$ implies that $ac \in J$ or $bc \in \delta(J)$. As J and $\delta(J)$ are subtractive, $a \in J$ or $b \in \delta(J)$. Hence J is δ-primary, a contradiction. $\square$

References

[1] **M. F. Atiyah and I. G. Macdonald**, *Introduction to Commutative Algebra*, Addison Wesley Publishing Company, 1969.

[2] **Z. Dongsheng**, *δ-primary ideals of commutative rings*, Kyungpook Math. J. **41** (2001), 17 – 22.

[3] **S. Ebrahimi Atani**, *The ideal theory in quotients of commutative semirings*, Glas. Math. **42** (2007), 301 – 308.

[4] **S. Ebrahimi Atani, S. Dolati Pish Hesari and M. Khoramdel**, *Strong co-ideal theory in quotients of semirings*, J. Advanced Research in Pure Math. **5(3)** (2013), 19 – 32.

[5] **S. Ebrahimi Atani, S. Dolati Pish Hesari and M. Khoramdel**, *Zariski-topology for co-ideals of commutative semirings*, Quasigroups and Related Systems **21** (2013), 56 – 68.

[6] **S. Ebrahimi Atani, S. Dolati Pish Hesari and M. Khoramdel**, *The identity-summand graph of commutative semirings*, J. Korean Math. Soc. **51** (2014), 189 – 202.

[7] **S. Ebrahimi Atani, Z. Ebrahimi Sarvandi and M. Shajari Kohan**, *On δ-primary ideals of commutative semirings*, Rom. J. Math. Comput. Sci. **3** (2013), 71 – 81.

[8] **S. Ebrahimi Atani and F. Farzalipour**, *On weakly primary ideals*, Georgian Math. J. **3** (2005), 423 − 429.

[9] **J. S. Golan**, *Semirings and their Applications*, Kluwer Academic Publishers Dordrecht, 1999.

[10] **J. Kist**, *Minimal prime ideals in commutative semigroups*, Proc. London Math. Soc. **3** (1963), 31 − 50.

[11] **H. Wang**, *On rational series and rational language*, Theor. Comput. Sci. **205** (1998), 329 − 336.

Received October 20, 2013

Faculty of Mathematical Sciences
University of Guilan
P.O.Box 1914, Rasht, Iran
E-mails: ebrahimi@guilan.ac.ir, saboura_dolati@yahoo.com, mehdikhoramdel@gmail.com

Quasigroups and Related Systems **22** (2014), 81 – 88

Commutants of middle Bol loops

Ion Grecu and Parascovia Syrbu

Abstract. The commutant of a loop is the set of all its elements that commute with each element of the loop. It is known that the commutant of a left or right Bol loop is not a subloop in general. Below we prove that the commutant of a middle Bol loop is an AIP-subloop, i.e., a subloop for which the inversion is an automorphism. A necessary and sufficient condition when the commutant is invariant under the existing isostrophy between middle Bol loops and the corresponding right Bol loops is given.

1. Introduction

Recall that a loop $(Q,\cdot)$ is a *right* (*left*) *Bol loop* if it satisfies the identity $(zx\cdot y)x = z(xy\cdot x)$ (resp. $x(y\cdot xz) = (x\cdot yx)z$). We say that a quasigroup $(Q,\cdot)$ satisfies the *right* (*left*) *inverse property*, if there exists a mapping $\varphi : Q \mapsto Q$, such that $yx\cdot\varphi(x) = y$ (resp. $\varphi(x)\cdot xy = y$), for every $x,y\in Q$. If a loop satisfies the right (left) inverse property then the left inverse of each element coincides with the right inverse ${}^{-1}x = x^{-1}$ and $yx\cdot x^{-1} = y$ (resp., $x^{-1}\cdot xy = y$), $\forall x,y\in Q$. Right (left) Bol loops satisfy the right (resp. left) inverse property. A loop $(Q,\circ)$ is called a *middle Bol loop* if the condition $(x\circ y)^{-1} = y^{-1}\circ x^{-1}$, $\forall x,y\in Q$, called the *anti-automorphic inverse property*, is universal in $(Q,\circ)$, i.e., if every loop isotope of $(Q,\circ)$ satisfies the anti-automorphic inverse property. V. D. Belousov proved in [1] that a loop $(Q,\cdot)$ is middle Bol if and only if the corresponding e-loop $(Q,\cdot,/,\backslash)$ (the operation "/" and, resp. "\", is the left, resp. right, division in $(Q,\cdot)$), satisfies the identity:

$$x\cdot((y\cdot z)\backslash x) = (x/z)\cdot(y\backslash x). \tag{1}$$

Middle Bol loops are studied in [1, 2, 3, 6]. It was proved in [3] that middle Bol loops are isostrophes of right (left) Bol loops. We will consider below the isostrophy between right Bol loops and middle Bol loops. Left Bol loops can be characterized analogously, by a "mirror reflection".

According to [3], a loop $(Q,\circ)$ is middle Bol if and only if there exists a right Bol loop $(Q,\cdot)$ such that, for $\forall x,y\in Q$, the following equality holds:

$$x\circ y = (y\cdot xy^{-1})y, \tag{2}$$

2010 Mathematics Subject Classification: 20N05
Keywords: right Bol loop, middle Bol loop, isostrophy, commutant.

which is equivalent to

$$x \circ y = y^{-1} \backslash x, \tag{3}$$

and to

$$x \cdot y = y // x^{-1}, \tag{4}$$

where "\" is the right division in the right Bol loop $(Q, \cdot)$, and "//" is the left division in the middle Bol loop $(Q, \circ)$.

The connection between middle and left Bol loops is analogous [6].

A middle Bol loop satisfies the right or left inverse property if and only if it is a Moufang loop (see [3]). It is known (see [2, 6]) that two middle Bol loops are isotopic (resp. isomorphic) if and only if the corresponding right Bol loops are isotopic (resp. isomorphic). Note also that a middle Bol loop $(Q, \circ)$ and its corresponding right Bol loop $(Q, \cdot)$ have a common unit and that the inverse of each element x in $(Q, \circ)$ is equal to the inverse of x in $(Q, \cdot)$. Moreover, middle Bol loops, as well as their corresponding right Bol loops, are power-associative (i.e., every subloop generated by one element is associative).

The *commutant of a loop* $(Q, \cdot)$ is the set of all elements that commute with each element of the loop $(Q, \cdot)$. This notion is known also as: *centrum, commutative center, semicenter*, etc. In groups the commutant is the center and a normal subgroup. In loops the commutant is not always a subloop. But it is known, for example, that the commutant of a Moufang loop is a subloop.

The commutants of left Bol loops are studied in [4] and [5] where examples of finite left Bol loops with non-subloop commutants are given and necessary conditions when the commutants of finite left Bol loops are subloops are found.

Below is proved that the commutants of middle Bol loops are AIP-subloops, i.e., subloops with automorphic inverse property: $(x \cdot y)^{-1} = x^{-1} \cdot y^{-1}$. Also, necessary and sufficient conditions when the commutant of a middle Bol loop and the commutant of the corresponding right Bol loop coincide are found. In the last section the "normality" of the commutants in middle Bol loops is partially examined.

2. The commutants of middle Bol loops

Let's denote the commutant of a loop $(Q, \cdot)$ by $C^{(\cdot)}$, so:

$$C^{(\cdot)} = \{a \in Q \,|\, a \cdot x = x \cdot a, \forall x \in Q\}.$$

Lemma 2.1. *Let $(Q, \circ)$ be a middle Bol loop. If $a \in C^{(\circ)}$, then $a^{-1} \in C^{(\circ)}$.*

Proof. If $a \in C^{(\circ)}$, then $a \circ x = x \circ a$, $\forall x \in Q$. So, as $(Q, \circ)$ satisfies the anti-automorphic inverse property, the last equality implies $x^{-1} \circ a^{-1} = a^{-1} \circ x^{-1}$, $\forall x \in Q$, i.e., $a^{-1} \in C^{(\circ)}$. □

Lemma 2.2. *Let $(Q, \circ)$ be a middle Bol loop and let $(Q, \cdot)$ be the corresponding right Bol loop. For $a \in Q$, the following statements hold:*

1. $a \in C^{(\circ)}$ *if and only if, for* $\forall z \in Q$*:*

$$(a \cdot z)^{-1} = a^{-1} \cdot z^{-1}; \tag{5}$$

2. $a \in C^{(\circ)}$ *if and only if, for* $\forall z \in Q$*:*

$$(z \cdot a)^{-1} = z^{-1} \cdot a^{-1}. \tag{6}$$

Proof. 1. According to the definition of $C^{(\circ)}$, $a \in C^{(\circ)}$ if and only if $a \circ x = x \circ a$, $\forall x \in Q$. So, using (3), we get $x^{-1} \backslash a = a^{-1} \backslash x$, $\forall x \in Q$, where "$\backslash$" is the right division in the corresponding right Bol loop $(Q, \cdot)$. Denoting $a^{-1} \backslash x$ by z and applying the right inverse property of $(Q, \cdot)$, we obtain:

$$(a^{-1} \cdot z)^{-1} \backslash a = z \Leftrightarrow (a^{-1} \cdot z)^{-1} \cdot z = a \Leftrightarrow (a^{-1} \cdot z)^{-1} = a \cdot z^{-1}.$$

The last equality is equivalent to (5).

2. Using (2), the right Bol identity, the right inverse property and the power-associativity of $(Q, \cdot)$, we have:

$$a \in C^{(\circ)} \Leftrightarrow a \circ x = x \circ a \Leftrightarrow (x \cdot ax^{-1}) \cdot x = (a \cdot xa^{-1}) \cdot a \Leftrightarrow$$
$$x^{-1} \cdot [(x \cdot ax^{-1}) \cdot x] = x^{-1}[(a \cdot xa^{-1}) \cdot a] \Leftrightarrow$$
$$ax^{-1} \cdot x = (x^{-1}a \cdot xa^{-1}) \cdot a \Leftrightarrow a = (x^{-1}a \cdot xa^{-1}) \cdot a \Leftrightarrow$$
$$e = x^{-1}a \cdot xa^{-1} \Leftrightarrow (x \cdot a^{-1})^{-1} = x^{-1} \cdot a \Leftrightarrow (x \cdot a)^{-1} = x^{-1} \cdot a^{-1},$$

for every $x \in Q$, where e is the common unit of $(Q, \circ)$ and $(Q, \cdot)$. $\square$

Remark 2.3. (I). According to Lemma 2.2,

$$C^{(\circ)} = \{a \in Q \mid (a \cdot x)^{-1} = a^{-1} \cdot x^{-1}, \forall x \in Q\} = \{a \in Q \mid (x \cdot a)^{-1} = x^{-1} \cdot a^{-1}, \forall x \in Q\},$$

where $(Q, \circ)$ is a middle Bol loop and $(Q, \cdot)$ is the corresponding right Bol loop.

(II). Let $(Q, \circ)$ be a middle Bol loop and let $a \in C^{(\circ)}$. Using (1), we have:

$$a \circ [(y \circ z) \backslash\backslash a] = (a // z) \circ (y \backslash\backslash a),$$

for every $y, z \in Q$, where "$\backslash\backslash$" ("$//$") is the right (respectively, left) division in $(Q, \circ)$. Puting $y = e$, where e is the unit of $(Q, \circ)$, and using the fact that $a \in C^{(\circ)}$, the previous equality implies:

$$a \circ (z \backslash\backslash a) = (a // z) \circ a = a \circ (a // z),$$

for every $z \in Q$, so $(Q, \circ)$ satisfies the equality

$$z \backslash\backslash a = a // z, \tag{7}$$

for $\forall z \in Q$ and $\forall a \in C^{(\circ)}$.

(III). Recall that the inversion is a left semi-automorphism of right Bol loops, i.e., $(xy \cdot x)^{-1} = (x^{-1} \cdot y^{-1}) \cdot x^{-1}$. This fact was observed by D.A. Robinson. Note that it can be easily obtained if we denote $(xy \cdot x)^{-1}$ by z. In other words, if $e = z \cdot (xy \cdot x) = (zx \cdot y) \cdot x$. Then, applying three times the right inverse property, we obtain $(xy \cdot x)^{-1} = (x^{-1} \cdot y^{-1}) \cdot x^{-1}$.

Theorem 2.4. *The commutant of a middle Bol loop is a subloop.*

Proof. Let $(Q, \circ)$ be a middle Bol loop and let $(Q, \cdot)$ be the corresponding right Bol loop. If $a, b \in C^{(\circ)}$ then, using the equalities (6) and (5), the right Bol identity and the fact that $x \mapsto x^{-1}$ is a left semi-automorphism of $(Q, \cdot)$, we have:

$$\begin{aligned}(ba \cdot y)^{-1} \cdot a^{-1} &= [(ba \cdot y) \cdot a]^{-1} = [b \cdot (ay \cdot a)]^{-1} = b^{-1} \cdot (ay \cdot a)^{-1} \\ &= b^{-1} \cdot (a^{-1}y^{-1} \cdot a^{-1}) = (b^{-1}a^{-1} \cdot y^{-1}) \cdot a^{-1},\end{aligned}$$

so

$$(ba \cdot y)^{-1} = b^{-1}a^{-1} \cdot y^{-1} = (ba)^{-1} \cdot y^{-1},$$

for every $y \in Q$.

According to Lemma 2.2, the condition $(ba \cdot y)^{-1} = (ba)^{-1} \cdot y^{-1}$, $\forall y \in Q$, is equivalent to $b \cdot a \in C^{(\circ)}$. Thus, using (2) and Lemma 2.1, we can see that $a \circ b = (b \cdot ab^{-1}) \cdot b \in C^{(\circ)}$, which means that " $\circ$ " is an algebraic operation on $C^{(\circ)}$.

Moreover, using Lemma 2.1, (4) and (7), we get: $a, b \in C^{(\circ)} \Rightarrow a, b^{-1} \in C^{(\circ)} \Rightarrow b^{-1} \cdot a = a//b = b\backslash\backslash a \in C^{(\circ)}$, i.e., $y = b\backslash\backslash a = a//b \in C^{(\circ)}$, where y is the solution of the equations $b \circ y = y \circ b = a$. Hence $(C^{(\circ)}, \circ)$ is a subloop of $(Q, \circ)$. $\square$

Corollary 2.5. *The commutant of a middle Bol loop $(Q, \circ)$ is its AIP-subloop.*

Proof. Indeed, if $a \in C^{(\circ)}$ then $a^{-1} \in C^{(\circ)}$, so $(a \circ x)^{-1} = x^{-1} \circ a^{-1} = a^{-1} \circ x^{-1}$, $\forall x \in Q$. $\square$

Corollary 2.6. *If $(Q, \circ)$ is a middle Bol loop and $(Q, \cdot)$ is the corresponding right Bol loop, then $(C^{(\circ)}, \cdot)$ is an AIP-subloop of $(Q, \cdot)$.*

Proof. It was shown in the proof of Theorem 2.4 that $a \cdot b, a \circ b, a\backslash\backslash b \in C^{(\circ)}$ for $a, b \in C^{(\circ)}$. This means that " $\cdot$ " is an algebraic operation on $C^{(\circ)}$. So, if $a, b \in C^{(\circ)}$ then, using (3), (4) and Lemma 2.1, we have: $b\backslash a = a \circ b^{-1} \in C^{(\circ)}$ and $a/b = c \Leftrightarrow c \cdot b = a \Leftrightarrow b//c^{-1} = a \Leftrightarrow a \circ c^{-1} = b \Leftrightarrow a\backslash\backslash b = c^{-1} \Leftrightarrow (a\backslash\backslash b)^{-1} = c$, so $a/b = (a\backslash\backslash b)^{-1} \in C^{(\circ)}$, i.e., $(C^{(\circ)}, \cdot)$ is a subloop of $(Q, \cdot)$.

Moreover, according to (5), Lemma 2.2, $(a \cdot z)^{-1} = a^{-1} \cdot z^{-1}$, $\forall a \in C^{(\circ)}$ and $\forall z \in Q$, so $(C^{(\circ)}, \cdot)$ is an AIP-subloop of $(Q, \cdot)$. $\square$

3. A criterion for $C^{(\circ)} = C^{(\cdot)}$

If $(Q,\cdot)$ is a Moufang loop and $(Q,\circ)$ is the corresponding middle Bol loop, then "$\circ$" = "$\cdot$" and $C^{(\circ)} = C^{(\cdot)}$. The examples below show that both cases $C^{(\circ)} = C^{(\cdot)}$ and $C^{(\circ)} \neq C^{(\cdot)}$ are possible for an arbitrary middle Bol loop $(Q,\circ)$ and its corresponding right Bol loop $(Q,\cdot)$. The right Bol loops, used in these examples, can be found at http://www.uwyo.edu/moorhouse/pub/bol/mult8.txt (the loop 8.1.4.0 of order 8) and at http://www.uwyo.edu/moorhouse/pub/bol/mult12.txt (the loop 12.9.1.0 of order 12)

Example 3.1. Let $Q = \{1,2,3,4,5,6,7,8\}$. Consider the right Bol loop $(Q,\cdot)$ and the corresponding middle Bol loop $(Q,\circ)$, given by the tables:

$(\cdot)$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	8	6	1	7	3	5	4
3	3	7	8	6	1	4	2	5
4	4	1	7	8	6	5	3	2
5	5	6	1	7	8	2	4	3
6	6	3	4	5	2	8	1	7
7	7	5	2	3	4	1	8	6
8	8	4	5	2	3	7	6	1

.

$(\circ)$	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8
2	2	8	6	1	7	3	5	4
3	3	7	8	6	1	4	2	5
4	4	1	7	8	6	5	3	2
5	5	6	1	7	8	2	4	3
6	6	5	2	3	4	8	1	7
7	7	3	4	5	2	1	8	6
8	8	4	5	2	3	7	6	1

.

The commutants of the given loops are $C^{(\cdot)} = \{1,6,7,8\}$ and $C^{(\circ)} = \{1,8\}$, respectively, so $C^{(\circ)} \neq C^{(\cdot)}$.

Example 3.2. In this example $C^{(\circ)} = C^{(\cdot)} = \{1\}$, $(Q,\circ)$ is a right Bol loop and $(Q,\cdot)$ is the corresponding middle Bol loop.

$(\cdot)$	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	4	3	6	5	8	10	11	9	12	7
3	3	5	6	2	4	1	10	9	12	11	7	8
4	4	6	5	1	3	2	9	11	7	12	8	10
5	5	3	2	6	1	4	12	7	10	8	9	11
6	6	4	1	5	2	3	11	12	8	7	10	9
7	7	9	11	8	12	10	1	5	4	6	3	2
8	8	10	12	7	11	9	2	1	6	5	4	3
9	9	7	8	11	10	12	4	3	1	2	5	6
10	10	8	7	12	9	11	3	2	5	1	6	4
11	11	12	10	9	8	7	6	4	2	3	1	5
12	12	11	9	10	7	8	5	6	3	4	2	1

$(\circ)$	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12
2	2	1	5	6	3	4	12	7	10	8	9	11
3	3	4	6	5	2	1	11	12	8	7	10	9
4	4	3	2	1	6	5	9	11	7	12	8	10
5	5	6	4	3	1	2	8	10	11	9	12	7
6	6	5	1	2	4	3	10	9	12	11	7	8
7	7	12	10	9	8	11	1	4	2	3	6	5
8	8	7	9	11	10	12	4	1	3	2	5	6
9	9	10	12	7	11	8	2	6	1	5	4	3
10	10	8	11	12	9	7	6	2	5	1	3	4
11	11	9	7	8	12	10	3	5	4	6	1	2
12	12	11	8	10	7	9	5	3	6	4	2	1

The following theorem gives a necessary and sufficient condition for $C^{(\circ)} = C^{(\cdot)}$.

Theorem 3.3. *If $(Q, \circ)$ is a middle Bol loop and $(Q, \cdot)$ is the corresponding right Bol loop, then $C^{(\circ)} = C^{(\cdot)}$ if and only if the following conditions are satisfied:*

1. $x^{-1} \cdot xa = a$, $\forall x \in Q$, $\forall a \in C^{(\cdot)}$;

2. $x^{-1} \circ (x \circ b) = b$, $\forall x \in Q$, $\forall b \in C^{(\circ)}$.

Proof. Let $a \in C^{(\cdot)}$ and let $x^{-1} \cdot xa = a$, $\forall x \in Q$. Then, using (2) and the right inverse property of $(Q, \cdot)$, we obtain:

$$a \circ x = (x \cdot ax^{-1})x = (x \cdot x^{-1}a)x = a \cdot x = x \cdot a = (xa^{-1} \cdot a)a = (a \cdot xa^{-1})a = x \circ a,$$

for every $x \in Q$, i.e., $a \in C^{(\circ)}$. So, $C^{(\cdot)} \subseteq C^{(\circ)}$.

Conversely, let $C^{(\cdot)} \subseteq C^{(\circ)}$ and let $a \in C^{(\cdot)}$. Since $a \cdot x = x \cdot a$ and $a \circ x = x \circ a$, $\forall x \in Q$, we have:

$$\begin{aligned} x \cdot x^{-1}a = x \cdot ax^{-1} &= (x \cdot ax^{-1})x \cdot x^{-1} = (a \circ x) \cdot x^{-1} = (x \circ a) \cdot x^{-1} \\ &= (a \cdot xa^{-1})a \cdot x^{-1} = (xa^{-1} \cdot a)a \cdot x^{-1} = xa \cdot x^{-1} = ax \cdot x^{-1} = a, \end{aligned}$$

for every $x \in Q$, hence $x \cdot x^{-1}a = a$, $\forall x \in Q$.

Now, let $b \in C^{(\circ)}$. Then $b \in C^{(\cdot)}$ if and only if $b \cdot x = x \cdot b$, $\forall x \in Q$, which according to (4), is equivalent to $x//b^{-1} = b//x^{-1}$, $\forall x \in Q$, i.e., to $b = (x//b^{-1}) \circ x^{-1}$, $\forall x \in Q$, where "$//$" is the left division in $(Q, \circ)$. Making the substitution $x//b^{-1} \rightarrow y$ in the last equality and using the anti-automorphic inverse property of $(Q, \circ)$, we get:

$$b = y \circ (y \circ b^{-1})^{-1} = y \circ (b \circ y^{-1}) = y \circ (y^{-1} \circ b),$$

for every $y \in Q$. So, the second condition is equivalent to $C^{(\circ)} \subseteq C^{(\cdot)}$. $\square$

Corollary 3.4. *If $C^{(\circ)} = C^{(\cdot)}$, then $(C^{(\circ)}, \circ) = (C^{(\cdot)}, \cdot)$ is a commutative Moufang subloop.*

Proof. If $C^{(\circ)} = C^{(\cdot)}$ then, for $\forall x, y \in C^{(\circ)} = C^{(\cdot)}$, have:

$$x \circ y = (y \cdot xy^{-1}) \cdot y = (xy^{-1} \cdot y) \cdot y = x \cdot y,$$

hence, "$\circ$" = "$\cdot$" on the set $C^{(\circ)} = C^{(\cdot)}$. So, as $(C^{(\circ)}, \circ)$ is a commutative middle Bol IP-loop, it is a commutative Moufang loop. $\square$

4. When the commutant is a normal subloop?

In this section, for simplicity the operation of a middle Bol loop will be denoted by "$\cdot$".

Lemma 4.1. *If $(Q, \cdot)$ is a middle Bol loop and H is a subloop in $(Q, \cdot)$, then the following conditions are equivalent:*

1. *$L_{x,y}(H) = H$, $\forall x, y \in Q$;*

2. *$R_{x,y}(H) = H$, $\forall x, y \in Q$,*

where $L_{x,y} = L_{xy}^{-1} L_x L_y$ and $R_{x,y} = R_{xy}^{-1} R_y R_x$.

Proof. Let $L_{x,y}(H) = H$, $\forall x, y \in Q$. Then, for $x^{-1}, y^{-1} \in Q$ and $h^{-1} \in H$, there exists $h_1^{-1} \in H$, such that $L_{x^{-1},y^{-1}}(h^{-1}) = h_1^{-1}$. Hence $L_{x^{-1}y^{-1}}^{-1} L_{x^{-1}} L_{y^{-1}}(h^{-1}) = h_1^{-1}$, and consequently $x^{-1} \cdot y^{-1}h^{-1} = x^{-1}y^{-1} \cdot h_1^{-1}$.

Since the loop $(Q, \cdot)$ is power-associative and satisfies the anti-automorphic property, the last eqution implies $hy \cdot x = h_1 \cdot yx$, so $R_{yx}^{-1} R_x R_y(h) = h_1 \in H$, i.e., $R_{y,x}(H) \subseteq H$.

Analogously, for $h_1 \in H$ there exists $h^{-1} \in H$ such that $L_{x^{-1},y^{-1}}(h^{-1}) = h_1^{-1}$, which implies $R_{y,x}(h) = h_1$, so $H \subseteq R_{y,x}(H)$. In a similar way we can prove that the condition $R_{x,y}(H) = H$, $\forall x, y \in Q$ implies $L_{x,y}(H) = H$, $\forall x, y \in Q$. $\square$

Theorem 4.2. *The commutant $C^{(\cdot)}$ of a middle Bol loop $(Q, \cdot)$ is a normal subloop if and only if $L_{x,y}(C^{(\cdot)}) = C^{(\cdot)}$ (or, equivalently, if and only if $R_{x,y}(C^{(\cdot)}) = C^{(\cdot)}$), for every $x \in Q$.*

Proof. The subloop $C^{(\cdot)}$ is normal if and only if $L_{x,y}(C^{(\cdot)}) = C^{(\cdot)}$, $R_{x,y}(C^{(\cdot)}) = C^{(\cdot)}$, and $T_x(C^{(\cdot)}) = C^{(\cdot)}$, where $T_x = R_x^{-1} L_x$, $\forall x, y \in Q$. If $c \in C^{(\cdot)}$ then, denoting $T_x(c)$ by b, we have $b = T_x(c) = R_x^{-1} L_x(c)$. Thus $R_x(b) = L_x(c)$, i.e., $bx = xc$, and consequently, $bx = cx$. Therefore $b = c$, so $T_x(c) = c$, $\forall c \in C^{(\cdot)}$. $\square$

References

[1] **V. D. Belousov**, *Foundations of the theory of quasigroups and loops*, (Russian), Nauka, Moscow, 1967.

[2] **I. Grecu and P. Syrbu**, *On some isostrophy invariants of Bol loops*, Bull. Transilv. Univ. Braşov, Series III, **5(54)** (2012), 145 – 154.

[3] **A. A. Gvaramiya**, *A certain class of loops*, (Russian), Moscov. Gos. Ped. Inst. Učen. Zap. **375** (1971), 25 – 34.

[4] **M. K. Kinyon and J. D. Phillips**, *Commutants of Bol loops of odd order*, Proc. Amer. Math. Soc. **132** (2004), 617 – 619.

[5] **M. K. Kinyon and J. D. Phillips, P. Vojtechovsky**, *When is the commutant of a Bol loop a subloop*, Trans. Amer. Math. Soc. **360** (2008), 2393 – 2408.

[6] **P. Syrbu**, *On middle Bol loops*, ROMAI J. **6** (2010), 229 – 236.

Received March 24, 2014

Moldova State University, A. Mateevici str. 60, MD2009 Chisinau, Republic of Moldova
E-mails: grecui85@yahoo.com, syrbuviv@yahoo.com

Quasigroups and Related Systems **22** (2014), 89 − 96

Green's relations and the relation $\mathcal{N}$ in Γ-semigroups

Niovi Kehayopulu

Abstract. Let M be a Γ-semigroup. For a prime ideal I of M, let σ_I be the relation on M consisted of the pairs (x, y), where x and y are elements of M such that either both x and y are elements of I or both x and y are not elements of I. Let $\mathcal{N}$ be the semilattice congruence on M defined by $x\mathcal{N}y$ if and only if the filters of M generated by x and y coincide. Then the set $\mathcal{N}$ is the intersection of the relations σ_I, where I runs over the prime ideals of M. If $\mathcal{R}$, $\mathcal{L}$, $\mathcal{I}$, $\mathcal{H}$ are the Green's relations of M and $\mathcal{A}$ the set of right ideals, $\mathcal{B}$ the set of left ideals and $\mathcal{I}$ the set of ideals of M, then we have $\mathcal{H} \subseteq \mathcal{R} \subseteq \mathcal{I} \subseteq \mathcal{N}$, $\mathcal{H} \subseteq \mathcal{L} \subseteq \mathcal{I} \subseteq \mathcal{N}$ and $\mathcal{L} \circ \mathcal{R} \subseteq \mathcal{I}$, $\mathcal{R} = \bigcap\limits_{I \in \mathcal{A}} \sigma_I$, $\mathcal{L} = \bigcap\limits_{Ix \in \mathcal{B}} \sigma_I$, $\mathcal{I} = \bigcap\limits_{I \in \mathcal{M}} \sigma_I$. The relation $\mathcal{R} \circ \mathcal{L}$ $(= \mathcal{L} \circ \mathcal{R})$ is the least -with respect to the inclusion relation- equivalence relation on M containing both $\mathcal{R}$ and $\mathcal{L}$. Finally, we characterize the Γ-semigroups which have only one $\mathcal{L}$ (or $\mathcal{R}$)-class or only one $\mathcal{I}$-class.

1. Introduction and prerequisites

An ideal I of a semigroup S is called *completely prime* if for any $a, b \in I$, $ab \in I$ implies that either $a \in I$ or $b \in I$. Every semilattice congruence on a semigroup S is the intersection of congruences σ_I where I is a completely prime ideal and for all $x, y \in S$, we have $x\sigma_I y$ if and only if $x, y \in I$ or $x, y \notin I$ [6]. For semigroups, ordered semigroups or ordered Γ-semigroups, we always use the terminology weakly prime, prime (subset) instead of the terminology prime, completely prime given by Petrich. For Green's relations in semigroups we refer to [1, 6]. For Green's relations in ordered semigroups, we refer to [2]. In the present paper we mainly present the analogous results of [2] in case of Γ-semigroups.

The concept of a Γ-semigroup has been introduced by M.K. Sen in 1981 as follows: If S and Γ are two nonempty sets, S is called a Γ-*semigroup* if the following assertions are satisfied: (1) $a\alpha b \in S$ and $\alpha a \beta \in \Gamma$ and (2) $(a\alpha b)\beta c = a(\alpha b \beta)c = a\alpha(b\beta c)$ for all $a, b, c \in S$ and all $\alpha, \beta \in \Gamma$ [8]. In 1986, M.K. Sen and N.K. Saha changed that definition and gave the following definition of a Γ-semigroup: Given two nonempty sets M and Γ, M is called a Γ-semigroup if (1) $a\alpha b \in M$ and (2) $(a\alpha b)\beta c = a\alpha(b\beta c)$ for all $a, b, c \in M$ and all $\alpha, \beta \in \Gamma$ [9]. Later, in [7], Saha calls a nonempty set S a Γ-semigroup ($\Gamma \neq \emptyset$) if there is a mapping

2010 Mathematics Subject Classification: 20F99, 06F99; 20M10; 06F05
Keywords: Γ-semigroup; right (left) ideal; ideal; prime ideal; filter; semilattice congruence; Green's relations; left (right) simple; simple.

$S \times \Gamma \times S \to S \mid (a, \gamma, b) \to a\gamma b$ such that $(a\alpha b)\beta c = a\alpha(b\beta c)$ for all $a, b, c \in S$ and all $\alpha, \beta \in \Gamma$, and remarks that the most usual semigroup concepts, in particular regular and inverse Γ-semigroups have their analogous in Γ-semigroups. Although it was very convenient to work on the definition by Sen and Saha using binary relations [9], the uniqueness condition was missing from that definition. Which means that in an expression of the form, say $a\gamma b\mu c\xi d\rho e$ or $a\Gamma b\Gamma c\Gamma d\Gamma e$, it was not known where to put the parentheses. In that sense, the definition of a Γ-semigroup given by Saha in [7] was the right one. However, adding the uniqueness condition in the definition given by Sen and Saha in [9], we do not need to define it via mappings. The revised version of the definition by Sen and Saha in [9] has been introduced by Kehayopulu in [3] as follows:

For two nonempty sets M and Γ, define $M\Gamma M$ as the set of all elements of the form $m_1\gamma m_2$, where $m_1, m_2 \in M$, $\gamma \in \Gamma$. That is,

$$M\Gamma M := \{m_1\gamma m_2 \mid m_1, m_2 \in M, \gamma \in \Gamma\}.$$

Definition 1.1. Let M and Γ be two nonempty sets. The set M is called a Γ-*semigroup* if the following assertions are satisfied:

(1) $M\Gamma M \subseteq M$.

(2) If $m_1, m_2, m_3, m_4 \in M$, $\gamma_1, \gamma_2 \in \Gamma$ such that $m_1 = m_3$, $\gamma_1 = \gamma_2$ and $m_2 = m_4$, then $m_1\gamma_1 m_2 = m_3\gamma_2 m_4$.

(3) $(m_1\gamma_1 m_2)\gamma_2 m_3 = m_1\gamma_1(m_2\gamma_2 m_3)$ for all $m_1, m_2, m_3 \in M$ and $\gamma_1, \gamma_2 \in \Gamma$.

In other words, Γ is a set of binary operations on M such that:

$(m_1\gamma_1 m_2)\gamma_2 m_3 = m_1\gamma_1(m_2\gamma_2 m_3)$ for all $m_1, m_2, m_3 \in M$ and all $\gamma_1, \gamma_2 \in \Gamma$.

According to that "associativity" relation, each of the elements $(m_1\gamma_1 m_2)\gamma_2 m_3$, and $m_1\gamma_1(m_2\gamma_2 m_3)$ is denoted by $m_1\gamma_1 m_2\gamma_2 m_3$.

Using conditions (1) – (3) one can prove that for an element of M of the form

$$m_1\gamma_1 m_2\gamma_2 m_3\gamma_3 m_4 \ldots \gamma_{n-1} m_n\gamma_n m_{n+1},$$

or a subset of M of the form

$$m_1\Gamma_1 m_2\Gamma_2 m_3\Gamma_3 m_4 \ldots \Gamma_{n-1} m_n\Gamma_n m_{n+1},$$

one can put a parenthesis in any expression beginning with some m_i and ending in some m_j [3, 4, 5].

The example below based on Definition 1.1 shows what a Γ-semigroup is.

Example 1.2. [4] Consider the two-elements set $M := \{a, b\}$, and let $\Gamma = \{\gamma, \mu\}$ be the set of two binary operations on M defined in the tables below:

γ	a	b
a	a	b
b	b	a

μ	a	b
a	b	a
b	a	b

One can check that $(x\rho y)\omega z = x\rho(y\omega z)$ for all $x, y, z \in M$ and all $\rho, \omega \in \Gamma$. So, M is a Γ-semigroup.

Example 1.3. [5] Consider the set $M := \{a, b, c, d, e\}$, and let $\Gamma = \{\gamma, \mu\}$ be the set of two binary operations on M defined in the tables below:

γ	a	b	c	d	e
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c
e	e	a	b	c	d

μ	a	b	c	d	e
a	b	c	d	e	a
b	c	d	e	a	b
c	d	e	a	b	c
d	e	a	b	c	d
e	a	b	c	d	e

Since $(x\rho y)\omega z = x\rho(y\omega z)$ for all $x, y, z \in M$ and all $\rho, \omega \in \Gamma$, M is a Γ-semigroup.

Let now M be a Γ-semigroup. A nonempty subset A of M is called a *subsemigroup* of M if $A\Gamma A \subseteq A$, that is, if $a\gamma b \in A$ for every $a, b \in A$ and every $\gamma \in \Gamma$. A nonempty subset A of M is called a *left ideal* of M if $M\Gamma A \subseteq A$, that is, if $m \in M$, $\gamma \in \Gamma$ and $a \in A$, implies $m\gamma a \in A$. It is called a *right ideal* of M if $A\Gamma M \subseteq A$, that is, if $a \in A$, $\gamma \in \Gamma$ and $m \in M$, implies $a\gamma m \in A$. A is called an *ideal* of M if it is both a left and a right ideal of M. For an element a of M, we denote by $R(a)$, $L(a)$, $I(a)$, the right ideal, left ideal and the ideal of M, respectively, generated by a, and we have $R(a) = a \cup a\Gamma M$, $L(a) = a \cup M\Gamma a$, $I(a) = a \cup a\Gamma M \cup M\Gamma a \cup M\Gamma a\Gamma M$. An ideal A of M is called a *prime ideal* of M if $a, b \in M$ and $\gamma \in \Gamma$ such that $a\gamma b \in A$, then $a \in A$ or $b \in A$. Equivalently, if B and C are subsets of M such that $B \neq \emptyset$ (or $C \neq \emptyset$), $\gamma \in \Gamma$ and $B\gamma C \subseteq A$, then $B \subseteq A$ or $C \subseteq A$. A subsemigroup F of M is called a *filter* of M if $a, b \in M$ and $\gamma \in \Gamma$ such that $a\gamma b \in F$, implies $a \in F$ and $b \in F$. For an element a of M, we denote by $N(a)$ the filter of M generated by a and by $\mathcal{N}$ the equivalence relation on M defined by $\mathcal{N} := \{(x, y) \mid N(x) = N(y)\}$. An ideal A of M is a prime ideal of M if and only if $M \backslash A = \emptyset$ or $M \backslash A$ is a subsemigroup of M. A nonempty subset F of M is a filter of M if and only if $M \backslash F = \emptyset$ or $M \backslash F$ is a prime ideal of M. An equivalence relation σ on M is called a *left congruence* on M if $(a, b) \in \sigma$ implies $(c\gamma a, c\gamma b) \in \sigma$ for every $c \in M$ and every $\gamma \in \Gamma$. It is called a *right congruence* on M if $(a, b) \in \sigma$ implies $(a\gamma c, b\gamma c) \in \sigma$ for every $c \in M$ and every $\gamma \in \Gamma$. It is called a *congruence* on M if it is both a left and a right congruence on M. A *semilattice congruence* σ is a congruence on M such that

(1) $(a\gamma a, a) \in \sigma$ for every $a \in M$ and every $\gamma \in \Gamma$ and

(2) $(a\gamma b, b\gamma a) \in \sigma$ for every $a, b \in M$ and every $\gamma \in \Gamma$.

The relation $\mathcal{N}$ defined above is a semilattice congruence on M.

2. Main results

For a Γ-semigroup M, the Green's relations $\mathcal{R}$, $\mathcal{L}$, $\mathcal{I}$, $\mathcal{H}$ are the equivalence relations on M defined by:

$\mathcal{R} = \{(x, y) \mid R(x) = R(y)\}$, $\quad \mathcal{L} = \{(x, y) \mid L(x) = L(y)\}$,

$$\mathcal{I} = \{(x,y) \mid I(x) = I(y)\}, \qquad \mathcal{H} = \mathcal{R} \cap \mathcal{L}.$$

The relation $\mathcal{R}$ is a left congruence and the relation $\mathcal{L}$ is a right congruence on M. Let now M be a Γ-semigroup. For a subset I of M we denote by σ_I the relation on M defined by

$$\sigma_I = \{(x,y) \mid x,y \in I \text{ or } x,y \notin I\}.$$

Exactly as in case of semigroups, for a Γ- semigroup the following holds:

Lemma 2.1. *Let M be a Γ-semigroup. If F is a filter of M, then*

($\star$) *$M \backslash F = \emptyset$ or $M \backslash F$ is a prime ideal of M.*

In particular, any nonempty subset F of M satisfying ($\star$) is a filter of M. □

Proposition 2.2. *Let M be a Γ-semigroup and I a prime ideal of M. Then the set σ_I is a semilattice congruence on M.*

Proof. Clearly σ_I is a relation on M which is reflexive and symmetric. Let $(a,b) \in \sigma_I$ and $(b,c) \in \sigma_I$. Then $a,b \in I$ or $a,b \notin I$ and $b,c \in I$ or $b,c \notin I$. If $a,b \in I$ and $b,c \in I$, then $a,c \in I$, so $(a,c) \in \sigma_I$. The case $a,b \in I$ and $b,c \notin I$ is impossible and so is the case $a,b \notin I$ and $b,c \in I$. If $a,b \notin I$ and $b,c \notin I$, then $a,c \notin I$, then $(a,c) \in \sigma_I$, and σ_I is transitive. Let $(a,b) \in \sigma_I$, $c \in M$ and $\gamma \in \Gamma$. Then $(a\gamma c, b\gamma c) \in \sigma_I$. Indeed: If $a,b \in I$ then, since I is an ideal of M, we have $a\gamma c$, $b\gamma c \in I$, so $(a\gamma c, b\gamma c) \in \sigma_I$. Let $a,b \notin I$. If $c \in I$ then, since I is an ideal of M, we have $a\gamma c$, $b\gamma c \in I$, so $(a\gamma c, b\gamma c) \in \sigma_I$. If $c \notin I$, then $a\gamma c, b\gamma c \notin I$. This is because if $a\gamma b \in I$ then, since I is a prime ideal of M, we have $a \in I$ or $c \in I$ which is impossible. For $b\gamma c \in I$, we also get a contradiction. Thus we obtain $(a\gamma c, b\gamma c) \in \sigma_I$, and σ_I is a right congruence on M. Similarly σ_I is a left congruence on M, so σ_I is a congruence on M.

σ_I is a semilattice congruence on M. In fact: Let $a \in M$ and $\gamma \in \Gamma$. Then $(a\gamma a, a) \in \sigma_I$. Indeed: If $a \notin I$, then $a\gamma a \notin I$. This is because if $a\gamma a \in I$ then, since I is a prime ideal of M, we have $a \in I$ which is impossible. Since $a, a\gamma a \notin I$, we have $(a, a\gamma a) \in \sigma_I$. If $a \in I$ then, since I is an ideal of M, we have $a\gamma a \in I$, so $(a, a\gamma a) \in \sigma_I$. Let now $a,b \in M$ and $\gamma \in \Gamma$. Then $(a\gamma b, b\gamma a) \in \sigma_I$. In fact: If $a\gamma b \in I$ then, since I is a prime ideal of M, we have $a \in I$ or $b \in I$. Then, since I is an ideal of M, we have $b\gamma a \in I$. Since $a\gamma b, b\gamma a \in I$, we have $(a\gamma b, b\gamma a) \in \sigma_I$. If $a\gamma b \notin I$, then $b\gamma a \notin I$. This is because if $b\gamma a \in I$ then, since I is a prime ideal of M, we have $b \in I$ or $a \in I$. Since I is an ideal of M, we have $a\gamma b \in I$ which is impossible. Since $a\gamma b, b\gamma a \notin I$, we have $(a\gamma b, b\gamma a) \in \sigma_I$. □

Theorem 2.3. *Let M be a Γ-semigroup and $\mathcal{P}(M)$ the set of prime ideals of M. Then*

$$\mathcal{N} = \bigcap_{I \in \mathcal{P}(M)} \sigma_I.$$

Proof. $\mathcal{N} \subseteq \sigma_I$ for every $I \in \mathcal{P}(M)$. In fact: Let $(a,b) \in \mathcal{N}$ and $I \in \mathcal{P}(M)$. Then $(a,b) \in \sigma_I$. Indeed: Let $(a,b) \notin \sigma_I$. Then $a \in I$ and $b \notin I$ or $a \notin I$ and $b \in I$. Let $a \in I$ and $b \notin I$. Since $b \in M \backslash I$, we have $\emptyset \neq M \backslash I \subseteq M$. Since

$M\backslash(M\backslash I)=I$ and I is a prime ideal of M, the set $M\backslash(M\backslash I)$ is a prime ideal of M. By Lemma 2.1, $M\backslash I$ is a filter of M. Since $b\in M\backslash I$, we have $N(b)\subseteq M\backslash I$. Since $N(a)=N(b)$, we have $a\in M\backslash I$ which is impossible. If $a\notin I$ and $b\in I$, we also get a contradiction.

Let now $(a,b)\in\sigma_I$ for every $I\in\mathcal{P}(M)$. Then $(a,b)\in\mathcal{N}$. In fact: Let $(a,b)\notin\mathcal{N}$. Then $N(a)\neq N(b)$, from which $a\notin N(b)$ or $b\notin N(a)$ (This is because if $a\in N(b)$ and $b\in N(a)$, then $N(a)\subseteq N(b)\subseteq N(a)$, so $N(a)=N(b)$). Let $a\notin N(b)$. Then $a\in M\backslash N(b)$. Since $b\in N(b)$, $b\notin M\backslash N(b)$. Since $a\in M\backslash N(b)$ and $b\notin M\backslash N(b)$, we have $(a,b)\notin\sigma_{M\backslash N(b)}$. Since $N(b)$ is a filter of M and $M\backslash N(b)\neq\emptyset$, by Lemma 2.1, $M\backslash N(b)\in\mathcal{P}(M)$. We have $M\backslash N(b)\in\mathcal{P}(M)$ and $(a,b)\notin\sigma_{M\backslash N(b)}$ which is impossible. If $b\notin N(a)$, by symmetry we get a contradiction. $\square$

For two relations ρ and σ on a set X, their composition $\rho\circ\sigma$ is defined by

$$\rho\circ\sigma=\{(a,b)\mid\exists\, x\in X:(a,x)\in\rho \text{ and } (x,b)\in\sigma\}.$$

If $\mathcal{B}_X$ is the set of relations on X, then the composition " $\circ$ " is an associative operation on $\mathcal{B}_X$, and so $(\mathcal{B}_X,\circ)$ is a semigroup.

Theorem 2.4. *Let M be a Γ-semigroup, $\mathcal{A}$ the set of right ideals, $\mathcal{B}$ the set of left ideals and $\mathcal{M}$ the set of ideals of M. Then we have*

(1) $\mathcal{R}=\bigcap\limits_{I\in\mathcal{A}}\sigma_I,\quad \mathcal{L}=\bigcap\limits_{I\in\mathcal{B}}\sigma_I,\quad \mathcal{I}=\bigcap\limits_{I\in\mathcal{M}}\sigma_I.$

(2) $\mathcal{H}\subseteq\mathcal{R}\subseteq\mathcal{I}\subseteq\mathcal{N},\quad \mathcal{H}\subseteq\mathcal{L}\subseteq\mathcal{I}\,(\subseteq\mathcal{N})$ *and* $\mathcal{L}\circ\mathcal{R}\subseteq\mathcal{I}$.

(3) *In particular, if M is commutative, then* $\mathcal{L}=\mathcal{R}=\mathcal{H}=\mathcal{I}=\mathcal{L}\circ\mathcal{R}$.

Proof. (1). Let $(x,y)\in\mathcal{R}$ and $I\in\mathcal{A}$. If $x\in I$, then

$$y\in R(y)=R(x)=x\cup x\Gamma M\subseteq I\cup I\Gamma M=I,$$

so $y\in I$. Then $x,y\in I$, and $(x,y)\in\sigma_I$. If $x\notin I$, then $y\notin I$. This is because $y\in I$ implies $x\in I$ which is impossible. Since $x,y\notin I$, we have $(x,y)\in\sigma_I$. Let now $(x,y)\in\sigma_I$ for every $I\in\mathcal{A}$. Since $x\in R(x)$ and $(x,y)\in\sigma_{R(x)}$, we have $y\in R(x)$, then $R(y)\subseteq R(x)$. Since $y\in R(y)$ and $(x,y)\in\sigma_{R(y)}$, we have $x\in R(y)$, so $R(x)\subseteq R(y)$. Then $R(x)=R(y)$, and $(x,y)\in\mathcal{R}$. The rest of the proof is similar.

(2). Let $(x,y)\in\mathcal{R}$. Then $R(x)=R(y)$, so $x\cup x\Gamma M=y\cup y\Gamma M$. Then

$$M\Gamma(x\cup x\Gamma M)=M\Gamma(y\cup y\Gamma M),$$

and $M\Gamma x\cup M\Gamma x\Gamma M=M\Gamma y\cup M\Gamma y\Gamma M$. Then we have

$$I(x)=x\cup x\Gamma M\cup M\Gamma x\cup M\Gamma x\Gamma M=y\cup y\Gamma M\cup M\Gamma y\cup M\Gamma y\Gamma M=I(y),$$

and $(x,y)\in\mathcal{I}$. Moreover, $\mathcal{I}\subseteq\mathcal{N}$. Indeed: By Theorem 2.3, $\mathcal{N}=\bigcap\limits_{I\in\mathcal{P}(S)}\sigma_I$, where $\mathcal{P}(S)$ is the set of prime ideals of M. Since $\mathcal{P}(M)\subseteq\mathcal{M}$, by (1), we have

$$\mathcal{I} = \bigcap_{I \in \mathcal{M}} \sigma_I \subseteq \bigcap_{I \in \mathcal{P}(S)} \sigma_I = \mathcal{N}.$$

$\mathcal{L} \circ \mathcal{R} \subseteq \mathcal{I}$. In fact: If $(a,b) \in \mathcal{L} \circ \mathcal{R}$, then there exists $c \in M$ such that $(a,c) \in \mathcal{L}$ and $(c,b) \in \mathcal{R}$. Then $L(a) = L(c)$ and $R(c) = R(b)$, $a \in c \cup M\Gamma c$ and $c \in b \cup b\Gamma M$. Then we get $a \in b \cup b\Gamma M \cup M\Gamma(b \cup b\Gamma M) = b \cup b\Gamma M \cup M\Gamma b \cup M\Gamma b\Gamma M = I(b)$, and so $I(a) \subseteq I(b)$. Since $(b,c) \in \mathcal{R}$ and $(c,a) \in \mathcal{L}$, we have

$$b \in c \cup c\Gamma M \subseteq a \cup M\Gamma a \cup (a \cup M\Gamma a)\Gamma M = a \cup M\Gamma a \cup a\Gamma M \cup M\Gamma a\Gamma M = I(a),$$

and $I(b) \subseteq I(a)$. Then $I(a) = I(b)$, and $(a,b) \in \mathcal{I}$.

(3). Let now M be commutative. Then we have

$$\begin{aligned} (a,b) \in \mathcal{L} &\Longleftrightarrow L(a) = L(b) \Longleftrightarrow a \cup M\Gamma a = b \cup M\Gamma b \\ &\Longleftrightarrow a \cup a\Gamma M = b \cup b\Gamma M \Longleftrightarrow (a,b) \in \mathcal{R}. \end{aligned}$$

$\mathcal{I} \subseteq \mathcal{H}$. Indeed:

$$\begin{aligned} (a,b) \in I &\Longrightarrow I(a) = I(b) \\ &\Longrightarrow a \cup M\Gamma a \cup a\Gamma M \cup M\Gamma a\Gamma M = b \cup M\Gamma b \cup b\Gamma M \cup M\Gamma b\Gamma M \\ &\Longrightarrow a \cup M\Gamma a \cup M\Gamma M\Gamma a = b \cup M\Gamma b \cup M\Gamma M\Gamma b \\ &\Longrightarrow a \cup M\Gamma a = b \cup M\Gamma b \Longrightarrow L(a) = L(b) \Longrightarrow (a,b) \in \mathcal{L} = \mathcal{R} = \mathcal{H}. \end{aligned}$$

Since $\mathcal{I} \subseteq \mathcal{H}$ and $\mathcal{H} \subseteq \mathcal{I}$ (by (2)), we have $\mathcal{H} = \mathcal{I}$.

$\mathcal{I} \subseteq \mathcal{L} \circ \mathcal{R}$. Indeed: If $(a,b) \in \mathcal{I}$, then $\mathcal{I} = \mathcal{L} = \mathcal{R}$. Since $(a,b) \in \mathcal{L}$ and $(a,b) \in \mathcal{R}$, we have $(a,b) \in \mathcal{L} \circ \mathcal{R}$. Besides, by (2), $\mathcal{L} \circ \mathcal{R} \subseteq \mathcal{I}$. Thus we get $\mathcal{I} = \mathcal{L} \circ \mathcal{R}$. □

Corollary 2.5. *Let M be a Γ-semigroup, A a right ideal, B a left ideal and I an ideal of M. Then*

$$A = \bigcup_{x \in A} (x)_{\mathcal{R}},\ B = \bigcup_{x \in B} (x)_{\mathcal{L}},\ I = \bigcup_{x \in I} (x)_{\mathcal{I}}.$$

Proof. Let A be a right ideal of M. If $t \in A$, then $t \in (t)_{\mathcal{R}} \subseteq \bigcup_{x \in A} (x)_{\mathcal{R}}$. Let $t \in (x)_{\mathcal{R}}$ for every $x \in A$. Then, by Theorem 2.4, we have $(t,x) \in \mathcal{R} = \bigcap_{I \in \mathcal{A}} \sigma_I$. Since $(t,x) \in \sigma_A$ and $x \in A$, we have $t \in A$. The proof of the rest is similar. □

Finally, we prove that the relation $\mathcal{R} \circ \mathcal{L}$, which is equal to $\mathcal{L} \circ \mathcal{R}$, is the least – with respect to the inclusion relation – equivalence relation on M containing both $\mathcal{R}$ and $\mathcal{L}$.

For a set X, denote by $E(X)$ the set of equivalence relations on X and by $\sup_{E(X)}\{\rho, \sigma\}$ the supremum of ρ and σ in $E(X)$.

Lemma 2.6. *If ρ and σ are equivalence relations on a set X such that $\rho \circ \sigma = \sigma \circ \rho$, then $\rho \circ \sigma$ is also an equivalence relation on X and $\rho \circ \sigma = \sup_{E(X)}\{\rho, \sigma\}$.* □

Lemma 2.7. *If ρ and σ are symmetric relations on a set X such that $\rho \circ \sigma \subseteq \sigma \circ \rho$, then $\rho \circ \sigma = \sigma \circ \rho$.* □

Theorem 2.8. *If M is a Γ-semigroup, then $\mathcal{R} \circ \mathcal{L} = sup_{E(M)}\{\mathcal{R}, \mathcal{L}\}$.*

Proof. We prove that $\mathcal{R} \circ \mathcal{L} = \mathcal{L} \circ \mathcal{R}$, then the rest of the proof is a consequence of Lemma 2.6. According to Lemma 2.7, it is enough to prove that $\mathcal{R} \circ \mathcal{L} \subseteq \mathcal{L} \circ \mathcal{R}$. Let $(a, b) \in \mathcal{R} \circ \mathcal{L}$. Then there exists $c \in M$ such that $(a, c) \in \mathcal{R}$ and $(c, b) \in \mathcal{L}$. Since $R(a) = R(c)$ and $L(c) = L(b)$, we have $a \in c \cup c\Gamma M$ and $b \in c \cup M\Gamma c$. Then $a = c$ or $a = c\gamma x$ and $b = c$ or $b = y\mu c$ for some $x, y \in M$, $\gamma, \mu \in \Gamma$.

We consider the cases:

(A) Let $a = c$ and $b = c$. Then $(a, b) = (c, c)$. Since $c \in M$, $(c, c) \in \mathcal{L}$ and $(c, c) \in \mathcal{R}$, we have $(c, c) \in \mathcal{L} \circ \mathcal{R}$. So $(a, b) \in \mathcal{L} \circ \mathcal{R}$.

(B) Let $a = c$ and $b = y\mu c$ for some $y \in M$, $\mu \in \Gamma$. Then $(a, b) = (c, y\mu c)$. Since $(b, b) \in \mathcal{R}$, we have $(b, y\mu c) \in \mathcal{R}$. Since $c \in M$, $(c, b) \in \mathcal{L}$ and $(b, y\mu c) \in \mathcal{R}$, we have $(c, y\mu c) \in \mathcal{L} \circ \mathcal{R}$, so $(a, b) \in \mathcal{L} \circ \mathcal{R}$.

(C) Let $a = c\gamma x$ for some $\gamma \in \Gamma$, $x \in M$ and $b = c$. Then $(a, b) = (c\gamma x, c)$. Since $(a, a) \in \mathcal{L}$, we have $(c\gamma x, a) \in \mathcal{L}$. Since $a \in M$, $(c\gamma x, a) \in \mathcal{L}$ and $(a, c) \in \mathcal{R}$, we have $(c\gamma x, c) \in \mathcal{L} \circ \mathcal{R}$, so $(a, b) \in \mathcal{L} \circ \mathcal{R}$.

(D) Let $a = c\gamma x$ and $b = y\mu c$ for some $x, y \in M$, $\gamma, \mu \in \Gamma$. Then $(a, b) = (c\gamma x, y\mu c) \in \mathcal{L} \circ \mathcal{R}$. Indeed: We have $b\gamma x = y\mu c\gamma x = y\mu a$. Since $(c, b) \in \mathcal{L}$ and $\mathcal{L}$ is a right congruence on M, we have $(c\gamma x, b\gamma x) \in \mathcal{L}$. Since $(a, c) \in \mathcal{R}$ and $\mathcal{R}$ is a left congruence on M, we have $(y\mu a, y\mu c) \in \mathcal{R}$, so $(b\gamma x, y\mu c) \in \mathcal{R}$. Since $b\gamma x \in M$, $(c\gamma x, b\gamma x) \in \mathcal{L}$ and $(b\gamma x, y\mu c) \in \mathcal{R}$, we have $(c\gamma x, y\mu c) \in \mathcal{L} \circ \mathcal{R}$. $\square$

Each Γ-semigroup M has an $\mathcal{L}$-class, an $\mathcal{R}$-class, and an $\mathcal{I}$-class. The set M is nonempty and, for each $x \in M$, $(x)_{\mathcal{L}}$ is a nonempty $\mathcal{L}$-class of M, $(x)_{\mathcal{R}}$ is a nonempty $\mathcal{R}$-class of M and $(x)_{\mathcal{I}}$ is a nonempty $\mathcal{I}$-class of M.

Definition 2.9. A Γ-semigroup M is called *left* (resp. *right*) *simple* if M has only one $\mathcal{L}$ (resp. $\mathcal{R}$)-class. M called *simple* if M has only one $\mathcal{I}$-class.

A right ideal, left ideal or ideal A of a Γ-semigroup M is called *proper* if $A \neq M$.

By Theorem 2.4, we have the following:

Corollary 2.10. *A Γ-semigroup M is left* (*resp. right*) *simple if and only if M does not contain proper left* (*resp. right*) *ideals. M is simple if and only if does not contain proper ideals.*

Proof. ($\Rightarrow$) Let M be left simple, A a left ideal of M and $x \in M$. Then $x \in A$. Indeed: Suppose $x \notin A$. Take an element $a \in A\,(A \neq \emptyset)$. Since $(x, a) \notin \sigma_A$, by Theorem 2.4(1), we have $(x, a) \notin \mathcal{L}$. Then $x \neq a$ and $(x)_{\mathcal{L}} \neq (a)_{\mathcal{L}}$ which is impossible.

($\Leftarrow$) Suppose M does not contain proper left ideals. Let $x \in M$ ($M \neq \emptyset$). Then, for each $t \in M$ such that $t \neq x$, we have $(t)_{\mathcal{L}} = (x)_{\mathcal{L}}$. In fact: Let $t \in M$, $t \neq x$. By the assumption, we have $L(x) = M$ and $L(t) = M$, then $(x, t) \in \mathcal{L}$, so $(t)_{\mathcal{L}} = (x)_{\mathcal{L}}$. Then $(x)_{\mathcal{L}}$ is the only $\mathcal{L}$-class of M, and M is left simple. The other cases are proved in a similar way. $\square$

Corollary 2.11. *Let M be a Γ-semigroup. Then M is left* (*resp. right*) *simple if and only if $M\Gamma a = M$* (*resp. $a\Gamma M = M$*) *for every $a \in M$. M is simple if and only if $M\Gamma a\Gamma M = M$ for every $A \subseteq M$.*

Proof. Let M be left simple and $a \in M$. Since $M\Gamma a$ is a left ideal of M, by Corollary 2.10, we have $M\Gamma a = M$. Conversely, let $M\Gamma a = M$ for every $a \in M$ and A a left ideal of M. Take an element $x \in A$ $(A \neq \emptyset)$. Then $M = M\Gamma x \subseteq M\Gamma A \subseteq A$, so $A = M$. By Corollary 2.10, M is left simple. $\square$

Remark 2.12. If M is a Γ-semigroup, then we have $M\Gamma a = M$ for every $a \in M$ if and only if $M\Gamma A = M$ for every nonempty subset A of M. We have $a\Gamma M = M$ for every $a \in M$ if and only if $A\Gamma M = M$ for every nonempty subset A of M. Also $M\Gamma a\Gamma M = M$ for every $a \in M$ if and only if $M\Gamma A\Gamma M = M$ for every nonempty subset A of M. Let us prove the third one: $\Rightarrow$. Let $a \in M$. Since $\{a\} \subseteq M$, by hypothesis, we have $M\Gamma\{a\}\Gamma M = M$, so $M\Gamma a\Gamma M = M$. $\Leftarrow$. Let $\emptyset \neq A \subseteq M$. Take an element $a \in A$. By hypothesis, we have $M = M\Gamma a\Gamma M \subseteq M\Gamma A\Gamma M \subseteq (M\Gamma M)\Gamma M \subseteq M\Gamma M \subseteq M$, so $M\Gamma A\Gamma M = M$.

Conclusion. In this paper we mainly gave the analogous results of [3] in case of Γ-semigroups. Analogous results of [3] for ordered Γ-semigroups can be also obtained. If we want to get a result on a Γ-semigroup or an ordered Γ semigroup, then we have to prove it first on a semigroup or on an ordered semigroup, respectively. We never work directly in Γ-semigroups or in ordered Γ-semigroups. The paper serves as an example to show the way we pass from semigroups to Γ-semigroups (also from ordered semigroups to ordered Γ-semigroups).

References

[1] **A.H. Clifford, G.B. Preston**, *The Algebraic Theory of Semigroups*, Vol. **I**, Amer. Math. Soc., Math. Surveys no. 7, Providence, Rh. Island 1961.

[2] **N. Kehayopulu**, *Note on Green's relations in ordered semigroups*, Math. Japon. **36** (1991), 211 – 214.

[3] **N. Kehayopulu**, *On prime, weakly prime ideals in po-Γ-semigroups*, Lobachevskii J. Math. **30** (2009), 257 – 262.

[4] **N. Kehayopulu**, *On ordered Γ-semigroups*, Sci. Math. Jpn. **71** (2010), 179 – 185.

[5] **N. Kehayopulu**, *On regular duo po-Γ-semigroups*, Math. Slovaca **61** (2011), 871 – 884.

[6] **M. Petrich**, *Introduction to Semigroups*, Merrill Research and Lecture Series, Charles E. Merrill Publishing Co., Columbus, Ohio 1973.

[7] **N.K. Saha**, *The maximum idempotent separating congruence on an inverse Γ-semigroup*, Kyungpook Math. Soc. J. **34** (1964), 59 – 66.

[8] **M.K. Sen**, *On Γ-semigroups*, Algebra and its applications, New Delhi, 1981, p. 301; Lecture Notes in Pure and Appl. Math., Dekker, New York, Vol. **91**, 1984.

[9] **M.K. Sen, N.K. Saha**, *On Γ-semigroup* I, Bull. Calcutta Math. Soc. **78** (1986), 180 – 186.

Received November 29, 2013

University of Athens, Department of Mathematics, 15784 Panepistimiopolis, Athens, Greece
E-mail: nkehayop@math.uoa.gr

Quasigroups and Related Systems **22** (2014), 97 − 132

Structure and representations of finite dimensional Malcev algebras

E. N. Kuzmin

Abstract. The paper [6] is devoted to the study of the basic structure theory of finite dimensional Malcev algebras. Similarly to the structure of finite dimensional Lie algebras, this theory has attracted a lot of attention and stimulated further research in this area. However, for the sake of brevity, detailed proofs of some results were omitted. Some authors experienced some difficulty owing to the lack of detailed proofs (see, for example [14]). The present work mostly follows the outline of [6] and fills the gaps in the literature.

Editors' Preface

This is an English translation of *Structure and representations of finite dimensional Malcev algebras* by E. N. Kuzmin, originally published in *Akademiya Nauk SSSR, Sibirskoe Otdelenie, Trudy Instituta Matematiki* (*Novosibirsk*), *Issledovaniya po Teorii Kolets i Algebr* 16 (1989), 75–101. The translation by Marina Tvalavadze was edited by Murray Bremner and Sara Madariaga. A brief survey of recent developments is included at the end of the paper.

1. Representations of nilpotent Malcev algebras. Cartan subalgebras

1.1. Malcev algebras were first introduced in [10] as Moufang-Lie algebras. They are defined by the identities,

$$x^2 = 0, \tag{1}$$

$$J(x, y, xz) = J(x, y, z)x, \tag{2}$$

where $J(x, y, z)$ is the so-called *Jacobian* of x, y, z:

$$J(x, y, z) = (xy)z + (yz)x + (zx)y.$$

In any anticommutative algebra, the Jacobian $J(x, y, z)$ is a skew-symmetric function of its arguments. Expanding the Jacobian, the Malcev identity (2) can be

2010 Mathematics Subject Classification: Primary 17D10. Secondary 17A36, 17A60, 17A65, 17B60, 17D05.

Keywords: Malcev algebras, Cartan subalgebras, nilpotent algebras, representation theory, solvable algebras, semisimple algebras, classification of simple algebras in characteristic 0, conjugacy theorem for Cartan subalgebras.

rewritten as follows,

$$xyzx + yzxx + zxxy = (xy)(xz), \tag{3}$$

where, for convenience, we omit parentheses in left-normed products: $((xy)z)x$.

Following [11] let us establish some basic identities which hold in all Malcev algebras. If A is a Malcev algebra, $x \in A$ and $R_x\colon a \mapsto ax$ is the operator of right multiplication by the element x, then the associative algebra A^* generated by $\{R_x \mid x \in A\}$ is called the *multiplication algebra* of A. Identity (3) implies that the following identities hold in A^*:

$$R_y R_x^2 = R_x^2 R_y + R_{yx} R_x + R_x R_{yx}, \tag{4}$$

$$R_x R_z R_x = R_z R_x^2 - R_x R_{zx} - R_{zxx}. \tag{5}$$

Linearizing identity (2) in x we obtain

$$J(x, y, uz) + J(u, y, xz) = J(x, y, z)u + J(u, y, z)x. \tag{6}$$

Hence the following identity holds in A^*:

$$R_{xyz} + R_{yzx} = R_y R_z R_x - R_z R_x R_y - R_{yz} R_x - R_{zx} R_y + R_y R_{zx} + R_z R_{xy}. \tag{7}$$

Adding the three identities obtained by cyclic permutations of the variables in (7), and assuming we work in characteristic different from 2, we obtain

$$R_{J(x,y,z)} = [R_y, R_{zx}] + [R_z, R_{xy}] + [R_x, R_{yz}], \tag{8}$$

where the square brackets denote the commutator of two operators:

$$[X, Y] = XY - YX.$$

Subtracting (7) from (8) we obtain

$$R_{zxy} = R_z R_x R_y - R_y R_z R_x + R_x R_{yz} - R_{xy} R_z,$$

or equivalently,

$$R_{xyz} = R_x R_y R_z - R_z R_x R_y + R_y R_{zx} - R_{yz} R_y. \tag{9}$$

Identity (9) implies that the following identity holds in A:

$$xyzt + yztx + ztxy + txyz = (xz)(yt); \tag{10}$$

this becomes identity (3) when setting $t = x$. If the characteristic of the field is other than 2 then identity (10) (also known as the Sagle identity) is equivalent to identity (3). Identity (10) presents some advantages: it is linear in each variable and invariant under cyclic permutations of the variables. Therefore, it is reasonable to use it (together with the anticommutative identity $x^2 = 0$) as the definition of the class of Malcev algebras in characteristic 2.

It is easy to check that Lie algebras in particular satisfy identity (10). On the other hand, it is easy to show that any Malcev algebra is binary-Lie: if u, v, w are arbitrary nonassociative words in two variables then, using induction on the length of u, v, w and identities (1), (2) and (6), it can be shown that $J(u, v, w) = 0$ when substituting for the variables any two elements of A. Therefore, the class of Malcev algebras can be regarded as an intermediate class between Lie algebras and binary-Lie algebras.

If we set $\Delta(x, y) = [R_x, R_y] - R_{xy}$ then $z\Delta(x, y) = J(z, x, y)$. From (8) we obtain

$$\begin{aligned}\Delta(y, zx) + \Delta(z, xy) + \Delta(x, yz) &= [R_y, R_{zx}] + [R_z, R_{xy}] + [R_x, R_{yz}] + R_{J(x,y,z)} \\ &= 2R_{J(x,y,z)},\end{aligned}$$

which can be written in the form

$$2wJ(x, y, z) = J(w, y, zx) + J(w, z, xy) + J(w, x, yz). \tag{11}$$

Define $D(x, y) = R_{xy} + [R_x, R_y]$. Since (9) is symmetric in x and y we obtain

$$2R_{xyz} = [[R_x, R_y], R_z] + [R_y, R_{zx}] + [R_x, R_{yz}]. \tag{12}$$

Subtracting (12) from (8) we obtain

$$R_{yzx+zxy-xyz} = R_{zD(x,y)} = [R_z, R_{xy}] + [R_z, [R_x, R_y]] = [R_z, D(x, y)],$$

which can be written in the form

$$(tz)D(x, y) = (tD(x, y))\, z + t\,(zD(x, y))\,. \tag{13}$$

This means that $D(x, y)$ is a derivation of A. If we set $R(x, y) = 2R_{xy} + [R_x, R_y]$ then it follows from (12) that

$$[R(x, y), R_z] = 2[R_{xy}, R_z] + 2R_{xyz} - [R_y, R_{zx}] - [R_x, R_{yz}]. \tag{14}$$

Adding (14) to (12) multiplied by 2 we obtain

$$[R(x, y), R_z] + 2R_{yzx} + 2R_{zxy} = [R_y, R_{zx}] + [R_x, R_{yz}],$$

which can be written in the form

$$[R(x, y), R_z] = R(xz, y) + R(x, yz). \tag{15}$$

Note that the identity

$$R_xR_yR_x = R_x^2R_y + R_{yx}R_x - R_{yxx}, \tag{16}$$

is a consequence of (4) and (5). A more general identity follows from (16) using induction on n:

$$R_x^n R_y R_x = R_x^{n+1} R_y + R_x^n R_{yx} - R_x R_{yx^n} - R_{yx^{n+1}} + R_{yx^n} R_x. \qquad (17)$$

To perform the inductive step it suffices to multiply both sides of (17) by R_x on the left and then substitute the term $R_x R_{yx^n} R_x$ using (16).

1.2. Let A be a Malcev algebra over a field F. According to [1], by a representation of A on a vector space V over F we understand a linear map $\rho\colon A \to \mathrm{End}(V)$ which provides the direct sum of vector spaces $V \oplus A$ with the structure of a Malcev algebra by setting

$$(v_1 + x)(v_2 + y) = v_1\rho(y) - v_2\rho(x) + xy \qquad (v_1, v_2 \in V,\ x, y \in A).$$

The algebra defined this way is called the *semidirect* or *split extension* of A by V, in which V (resp. A) appears as an abelian ideal (resp. Malcev subalgebra) of $V \oplus A$. The identities satisfied by ρ are similar to (9):

$$\rho(xyz) = \rho(x)\rho(y)\rho(z) - \rho(z)\rho(x)\rho(y) + \rho(y)\rho(zx) - \rho(yz)\rho(x).$$

A vector space V on which a representation is defined is called *Malcev A-module*. There is a special representation of the form $x \mapsto R_x$ (the regular representation). We will denote an arbitrary representation by R_x instead of $\rho(x)$. This will not lead to any confusion because it should be clear from the context which representation we mean†. It is easy to check that identities (12), (15)–(17) hold not only for the regular representation but also for arbitrary representations of a Malcev algebra A.

If a linear representation $\rho\colon A \to \mathrm{End}(V)$ satisfies

$$R_{xy} = [R_x, R_y], \qquad (18)$$

for any $x, y \in A$ then (9) follows from (18). Therefore, ρ is a representation of A (a homomorphism from A to the Lie algebra of endomorphisms of V). Representations of this type play a special role in the theory of Lie algebras. However, in the theory of Malcev algebras they are not very significant.

Generally speaking, the kernel $\mathrm{Ker}\rho$ of a representation ρ of a Malcev algebra A is not necessarily an ideal of A. Obviously, there exists a maximal ideal of A contained in $\mathrm{Ker}\rho$: the sum of all ideals of A contained in $\mathrm{Ker}\rho$. This ideal will be called the *quasi-kernel* of the representation ρ and it will be denoted by $\widetilde{\mathrm{Ker}\rho} = I$. For every representation ρ of a Malcev algebra A with quasi-kernel $\widetilde{\mathrm{Ker}\rho} = I$ there exists an induced nearly faithful representation of the quotient algebra A/I in the same vector space. Sometimes it can be useful to consider an arbitrary associative

† Translator's note: The author denotes the representation map by ρ and the image of an element x of the Malcev algebra under ρ by R_x.

algebra with identity E instead of $\mathrm{End}(V)$, where the right regular representation of E is isomorphic to[†] the algebra of endomorphisms of E.

Furthermore, we will restrict our attention to finite dimensional Malcev algebras, so we also assume that their representations are finite dimensional. We will denote by A_ρ^* the associative enveloping algebra of the representation ρ, i.e., the associative algebra generated by $\{R_x \mid x \in A\}$.

1.3. It is well-known that Engel's theorem plays an important role in the theory of finite dimensional Lie algebras. An analogue of this theorem holds for binary-Lie algebras [4]. The following theorems for the regular representation are found in [16].

Theorem 1.1. *Let ρ be a representation of a Malcev algebra A by nilpotent operators. Then A_ρ^* is nilpotent, and if ρ is a nearly faithful representation then A is also nilpotent.*

Proof. Let us first prove that A_ρ^* is nilpotent. To a subalgebra $B \subseteq A$ we assign the subalgebra $B^* \subseteq A_\rho^*$ generated by $\{R_x \mid x \in B\}$. Let B be a maximal subalgebra of A for which B^* is nilpotent and assume that $B \neq A$. Let $x \notin B$. Then for some natural number n we have $x_n = xb_1b_2 \cdots b_n \in B$ for any $b_i \in B$. Indeed, using (9), R_{x_n} can be written as a linear combination of "R-words" from A_ρ^*, each of them having sufficiently many operators R_b $(b \in B)$ if n is large enough. By our assumption, B^* is nilpotent, hence for some n we have $R_{x_n} = 0$ and $R_{x_n b} = 0$ $(b \in B)$. If now $x_n \notin B$ then B is a proper subalgebra of B_1 generated by $\{x_n, B\}$ and $B_1^* = B^*$. Therefore, B_1^* is nilpotent, which contradicts the maximality of B. Hence we can choose u from the sequence $\{x_k \mid k \geq 0\}$ such that $u \notin B$, $uB \subseteq B$. We write $C = (u) + B$ and show that C is nilpotent, which contradicts the maximality of B. For this we consider "long" R-words depending on R_u, R_{b_i} $(b_i \in B)$. It follows from the nilpotency of R_u that such words are either trivially equal to 0 in A_ρ^* or have many operators R_b $(b \in B)$. For definiteness we assume that $R_u^m = 0$, $(B^*)^n = 0$. Then, nontrivial words of R-length $N \geq mt$ contain at least t operators R_{b_i}. We apply the following transformations to these words:

(a) Transformations of subwords of the form $R_{b_i}R_u^2$, $R_uR_{b_i}R_u$ using identities (4) and (16) in which $x = u$ and $y = b_i$. Operators R_u either shift to the left or disappear and the total number t of operators R_{b_i} remains invariant.

(b) If we run out of transformations of the first type then we consider the rightmost operator R_u and assume that R_{b_1}, R_{b_2} precede it. By setting $x = b_1$, $y = b_2$, $z = u$ in (9) we transform $R_{b_1}R_{b_2}R_u$. Then the operator R_u either shifts to the left or disappears and the total number of operators R_{b_i} decreases by 1 only in the term $R_{b_1b_2u}$. At the same time, the rightmost operator R_u disappears.

[†] Translator's note: In other words, the right regular representation $x \mapsto R_x$ is an isomorphism between E and $\mathrm{End}(E)$.

If we write $N \geq 2mn$ then $t \geq 2n$. Using transformations of the first and second types (note that if both transformations are possible then transformations of the first type will be applied) we obtain a linear combination of words and at the right side of each of them will be at least n operators R_{b_i}. However, such words are equal to 0 because the nilpotency index of B^* is n. Hence nilpotency of C is proved and therefore A_ρ^* is nilpotent. Let $(A_\rho^*)^n = 0$. In the same way as when we chose the element u, we have to ensure that $A^N \subseteq \mathrm{Ker}\rho$ when $N \geq 2n$. However, A^N is an ideal of A so if the representation R is nearly faithful then $A^N = 0$, i.e., A is nilpotent. □

The following is a useful generalization of Theorem 1.1.

Theorem 1.2. *Let B be an ideal of a Malcev algebra A, let ρ be a nearly faithful representation of A, and for every $x \in B$ assume that the operator R_x is nilpotent. Then the ideal B is nilpotent and the algebra B^* generated by $\{R_x \mid x \in B\}$ lies in the radical of A_ρ^*.*

Proof. By Theorem 1.1, B^* is nilpotent of index n. To every R-word from A_ρ^* that has at least $2n$ operators R_{b_i} ($b_i \in B$) we can apply a transformation similar to transformations (a) and (b) from Theorem 1.1. Using (9) we change subwords $R_b R_{a_1} R_{a_2}$ and $R_{a_1} R_b R_{a_2}$ ($b \in B$) shifting R_b to the right and keeping the total number of them unchanged in each term. If we run out of transformations of this type then we consider the rightmost operator R_a where $a \notin B$. Let R_{b_1} and R_{b_2} precede it. Using (9) we transform $R_{b_1} R_{b_2} R_a$ so that R_{b_i} shifts to the right and the total number of them remains invariant. In the term with a factor $R_{b_1 b_2 a}$ the total number of operators R_{b_i} decreases by 1 and a factor R_a disappears. As a result all terms can be reduced to 0 and B^* generates a nilpotent ideal of A_ρ^* with nilpotency index less than or equal to $2n$, i.e., $B^* \subseteq \mathrm{Rad}\, A_\rho^*$. The subalgebra B^{4n} generates the ideal B_0 of A, whose elements are represented by zero operators. However, $\mathrm{Ker}\rho$ contains nonzero ideals $B^{4n} = 0$, so the theorem is proved. □

It follows from the proof above that the sum of nilpotent ideals in an arbitrary (not necessarily finite dimensional) Malcev algebra is a nilpotent ideal and any finite dimensional Malcev algebra contains the largest nilpotent ideal $N(A)$ which is called the *nil-radical* of the algebra A [16].

1.4. In the general case, operators of a representation of a Malcev algebra are not necessarily nilpotent. The theory of such representations is based on lemmas which are analogues to some well-known lemmas from the theory of Lie algebras [3].

Lemma 1.3. *Let ρ be a representation of a Malcev algebra A in the vector space V, let $x, y \in A$ and let $yx^m = 0$ for some $m > 0$. Then the Fitting components V_0 and V_1 of V with respect to R_x are invariant with respect to R_y.*

Proof. First note that V_0 and V_1 coincide with the kernel and image of R_x^n respectively, for sufficiently large n, for example $n \geq \dim V$. For convenience, we use induction on m. If $m = 1$ then the lemma follows from identity (4). If $m > 1$ then we can use identity (4) and we also note that the operators R_x and R_{yx} leave V_0 and V_1 invariant. To the decomposition of the characteristic polynomial $f(\lambda)$ of the operator R_x into irreducible factors $\pi(\lambda)$ corresponds a decomposition of V into the direct sum of primary components V_π annihilated by certain powers of the operator $\pi(R_x)$. □

Lemma 1.4. *Under the hypotheses of Lemma 1.3, let V be decomposed into its primary components V_π with respect to the operator R_x. Then the subspaces V_π are invariant with respect to R_y.*

Proof. By Lemma 1.3 it suffices to consider subspaces V_π on which R_x acts as a non-singular transformation. Let us again use induction on m. If $m = 1$ then for any polynomial $P(\lambda)$ we use identity (16),

$$V_\pi R_y P(R_x) = V_\pi R_x R_y P(R_x) = V_\pi R_x P(R_x) R_y = V_\pi P(R_x) R_y,$$

which proves our lemma. If $m > 1$ then using (16) we note that the operators R_x, R_{yx} and R_{yxx} leave the subspace V_π invariant. □

Proposition 1.5. *Let A be a nilpotent Malcev algebra, let ρ be a representation of A in a vector space V, let V_0^x and V_1^x be the Fitting components of V with respect to R_x, and let $x \in A$. Then $V = V_0 + V_1$, where*

$$V_0 = \bigcap_{x\in A} V_0^x, \qquad V_1 = \sum_{x\in A} V_1^x = \sum_{k=1}^{\infty} V(A_\rho^*)^k.$$

Proof. The proof is standard: we only need to note that if $V = V_0^x$ for all $x \in A$, i.e., ρ is a representation of A by nilpotent transformations of V, then A_R^* is nilpotent, so $(A_R^*)^k = 0$ for some $k > 0$ (by Theorem 1.1 this fact is even true without the assumption that A is nilpotent). If $V_1^x \neq 0$ for some $x \in A$ then V can be decomposed into the direct sum of A-submodules $V_0^x + V_1^x$. Moreover, $V_1^x \subseteq V_1$, $\dim V_0^x < \dim V$, and then we use induction on the dimension of V_0^x. □

Proposition 1.6. *Under the same hypotheses of Proposition 1.5, V can be decomposed into a direct sum of A-submodules V_i. Moreover, the minimal polynomial of a transformation induced by any operator R_x on V_i is some power of an irreducible polynomial.*

Proof. The proof trivially follows from Lemma 1.4 and it uses induction on the dimension of V. Here we remark that every subspace V_i can be constructed as an intersection of primary components for a finite number of operators R_x ($x \in A$) and the decomposition of Proposition 1.6 is uniquely determined. □

A representation ρ is called *split* if the characteristic roots of each operator R_x belong to the base field F. The next theorem follows from Proposition 1.6.

Theorem 1.7. *Let ρ be a split representation of a nilpotent Malcev algebra A. Then the representation space V can be decomposed into the direct sum of subspaces V_α characterized by the following conditions:*

1) V_α is invariant with respect to A_ρ^* (it is an A-submodule of V).

2) Each operator R_x has a unique characteristic root $\alpha(x)$.

3) If $\alpha \neq \beta$ then there exists an element $x \in A$ such that $\alpha(x) \neq \beta(x)$.

As we did in the proof of Proposition 1.6, we remark that each subspace V_α coincides with the intersection of root subspaces of V with respect to operators R_x for some finite number of elements $x \in A$. A map $\alpha\colon A \to F$ is called a *weight* of the algebra A with respect to the given representation ρ, and the corresponding subspaces V_α are called *weight spaces.*

In the case where H is a nilpotent subalgebra of a Malcev algebra A, and the given representation of H in A is split and induced by the regular representation of A, the subspaces A_α are said to be *root spaces* and the map $\alpha\colon H \to F$ is called a *root* of H in A. Below we will see that split representations of nilpotent Malcev algebras over fields of characteristic 0 can be completely described. In particular the weights are linear maps.

1.5. Let H be a nilpotent subalgebra of a Malcev algebra A whose regular representation on A is split. We now want to study relations between the root spaces A_α. The technique used to obtain these relations is similar to that used in [11] where they were derived for the case $\dim H = 1$. Using the results of the previous section we offer a simpler proof for a more general case. We will identify operators of scalar multiplication with elements of the base field F of arbitrary characteristic.

Let h be an arbitrary nonzero element of H and let $A = A_0^h + A_\alpha^h + \cdots$ be the decomposition of A into root spaces with respect to the operator R_h. Then Lemma 1.4 implies that $A_0^h A_\alpha^h \subseteq A_\alpha^h$. In particular A_0^h is a subalgebra of A. By setting $x = h$, $y = x_\alpha \in A_\alpha^h$ in (2) we obtain

$$J(h, x_\alpha, hx_\beta) = J(h, x_\alpha, x_\beta)h, \text{ or } J(h, x_\alpha, x_\beta(\beta - R_h)) = J(h, x_\alpha, x_\beta)(\beta + R_h).$$

By induction,

$$J(h, x_\alpha, x_\beta(\beta - R_h)^n) = J(h, x_\alpha, x_\beta)(\beta + R_h)^n,$$

and so $J(h, x_\alpha, x_\beta) \in A_{-\beta}^h$. Similarly, $J(h, x_\alpha, x_\beta) \in A_{-\alpha}^h$. Thus

$$J(h, x_\alpha, x_\beta) = 0 \quad (\alpha \neq \beta). \tag{19}$$

Substituting $u = x_0 \in A_0^h$ in (6) we obtain

$$J(x_0, x_\alpha, hx_\beta) + J(h, x_\alpha, x_0 x_\beta) = J(x_0, x_\alpha, x_\beta)h + J(h, x_\alpha, x_\beta)x_0,$$
$$J(x_0, x_\alpha, hx_\beta) = J(x_0, x_\alpha, x_\beta)h.$$

Therefore, similarly to (19) we get

$$J(A_0^h, A_\alpha^h, A_\beta^h) = 0 \ \ (\alpha \neq \beta). \tag{20}$$

If α, β are different roots of H in A, and A_α, A_β are the corresponding root spaces, then there exists an element $h \in H$ such that $\alpha(h) \neq \beta(h)$. Then

$$A_\alpha \subseteq A^h_{\alpha(h)}, \qquad A_\beta \subseteq A^h_{\beta(h)}, \qquad A_0 \subseteq A^h_0,$$

and it follows from (20) that

$$J(A_0, A_\alpha, A_\beta) = 0 \ (\alpha \neq \beta). \tag{21}$$

In particular, $J(H, A_\alpha, A_\beta) = 0$ $(\alpha \neq \beta)$ or

$$(x_\alpha x_\beta)h = (x_\alpha h)x_\beta + x_\alpha(x_\beta h) \ \ (\alpha \neq \beta), \tag{22}$$

for any $x_\alpha \in A_\alpha$, $x_\beta \in A_\beta$, $h \in H$. Identity (22) shows that each operator R_h $(h \in H)$ is a derivation of the linear space $A_\alpha A_\beta$. Thus

$$A_\alpha A_\beta \subseteq A_{\alpha+\beta} \ (\alpha \neq \beta). \tag{23}$$

Here $\alpha + \beta$ is not necessarily a root. If $\gamma\colon H \to F$ is not a root of H in A then we can assume that $A_\gamma = 0$. Reasoning in the same way when $\alpha = \beta$ we obtain

$$J(h, A_\alpha^h, A_\alpha^h) \subseteq A^h_{-\alpha}, \qquad J(A_0^h, A_\alpha^h, A_\alpha^h) \subseteq A^h_{-\alpha},$$

and in particular $J(A_0, A_\alpha, A_\alpha) \subseteq A^h_{-\alpha(h)}$. Any vector from $J(A_0, A_\alpha, A_\alpha)$ appears as a root vector for the operator R_h $(h \in H)$ with eigenvalue $-\alpha(h)$. Therefore,

$$J(A_0, A_\alpha, A_\alpha) \subseteq A_{-\alpha}. \tag{24}$$

In particular, for any $h \in H$ the following identity holds:

$$(x_\alpha y_\alpha)h = (x_\alpha h)y_\alpha + x_\alpha(y_\alpha h) + z_{-\alpha}. \tag{25}$$

Decomposing $x_\alpha y_\alpha$ into a sum of components from different root spaces of A gives

$$x_\alpha y_\alpha = u_{2\alpha} + u_\beta + \cdots . \tag{26}$$

Then for any $\beta \neq 2\alpha$ there exists an element $h \in H$ such that $\beta(h) \neq 2\alpha(h)$. If we apply the operator $(R_h - 2\alpha(h))^n$, where n is sufficiently large, to (26) then we obtain on one side an element of $A_{-\alpha}$ by (25) and on the other side an element $u_\beta(R_h - 2\alpha(h))^n + \cdots$. Moreover, the component $u'_\beta = u_\beta(R_h - 2\alpha(h))^n \in A_\beta$ is nonzero if $u_\beta \neq 0$, and the restriction of $(R_h - 2\alpha(h))$ to A_β has as its only characteristic root $\beta(h) - 2\alpha(h) \neq 0$, and it acts on A_β as a nonsingular map. Therefore the only nonzero component u_β in (26) except for $u_{2\alpha}$ is $u_{-\alpha}$:

$$x_\alpha y_\alpha \in A_{2\alpha} + A_{-\alpha}. \tag{27}$$

In particular, $A_0^2 \subseteq A_0$, which is clear since A_0 is the intersection of subspaces A_0^h, each of which is a subalgebra of A, and an intersection of subalgebras is itself a subalgebra.

Let α, β, γ be pairwise distinct weights of H in A. We show that $J(A_\alpha, A_\beta, A_\gamma) = 0$. If one of the weights α, β, γ is 0 then this follows from (21). Thus it is enough to consider the case $\alpha\beta\gamma \neq 0$. We first assume that $\alpha + \beta \neq \gamma$, $\alpha + \gamma \neq \beta$. Then it follows from (6), (21) and (23) that $J(x_\alpha, x_\beta, hx_\gamma) = J(x_\alpha, x_\beta, x_\gamma)h$, which implies $J(x_\alpha, x_\beta, x_\gamma) \in A_{-\gamma}$. Interchanging β and γ we obtain $J(x_\alpha, x_\beta, x_\gamma) \in A_{-\beta}$, which implies $J(x_\alpha, x_\beta, x_\gamma) = 0$. Further let $\alpha + \beta = \gamma$ and $\mathrm{char}F \neq 2$. Then $\gamma + \alpha \neq \beta$, $\gamma + \beta \neq \alpha$, and we go back to the previous case if we interchange α and γ. Finally let $\alpha + \beta = \gamma$ and $\mathrm{char}F = 2$. Then $\beta + \gamma = \alpha$ is symmetric in α, β and γ. It follows from (6), (21), (23) and (24) that

$$J(x_\alpha, x_\beta, hx_\gamma) = J(x_\alpha, x_\beta, x_\gamma)h + z_\beta, \tag{28}$$

where $z_\beta = J(h, x_\beta, x_\alpha x_\gamma) \in A_\beta$. Similar to (27), (28) implies that $J(x_\alpha, x_\beta, x_\gamma) \in A_\gamma + A_\beta$. By symmetry,

$$J(x_\alpha, x_\beta, x_\gamma) \in A_\alpha + A_\beta, \quad J(x_\alpha, x_\beta, x_\gamma) \in A_\alpha + A_\gamma,$$

which implies that $J(x_\alpha, x_\beta, x_\gamma) = 0$. Thus the proof is complete.

We now consider the Jacobian $J(x_\alpha, y_\alpha, x_\beta)$ where $\alpha, \beta \neq 0$. We first assume that $\beta \neq \alpha, -\alpha, 2\alpha$. Using (6) repeatedly and also (21), (23) and (27) we obtain $J(x_\alpha, x_\beta, hy_\alpha) = J(x_\alpha, x_\beta, y_\alpha)h$. Therefore, $J(x_\alpha, y_\alpha, x_\beta) \in A_{-\alpha}$. On the other hand, $J(x_\alpha, y_\alpha, hx_\beta) = J(x_\alpha, y_\alpha, x_\beta)h$. Therefore, $J(x_\alpha, y_\alpha, x_\beta) \in A_{-\beta}$. Therefore, $J(x_\alpha, y_\alpha, x_\beta) \in A_{-\beta}$ and thus $J(x_\alpha, y_\alpha, x_\beta) = 0$. Let $\beta = 2\alpha$ and $2\alpha \neq 0, \alpha, -\alpha$ (in particular, this implies that $\mathrm{char}F \neq 2, 3$). The identity $J(x_\alpha, y_\alpha, hx_{2\alpha}) = J(x_\alpha, y_\alpha, x_{2\alpha})h$ implies that $u = J(x_\alpha, y_\alpha, x_{2\alpha}) \in A_{-2\alpha}$. On the other hand,

$$J(x_{2\alpha}, x_\alpha, hy_\alpha) = J(x_{2\alpha}, x_\alpha, y_\alpha)h + z_\alpha,$$

where $z_\alpha = J(h, x_\alpha, y_\alpha)x_{2\alpha} \in A_\alpha$. Consequently, $u \in A_\alpha + A_{-\alpha}$. Taking into account that $-2\alpha \neq \alpha, -\alpha$, we conclude that $u = 0$.

Assume that $\mathrm{char}F \neq 2$. It follows from

$$J(x_\alpha, y_\alpha, hx_{-\alpha}) = J(x_\alpha, y_\alpha, x_{-\alpha})h,$$

for any $x_\alpha, y_\alpha \in A_\alpha$, $x_{-\alpha} \in A_{-\alpha}$ ($\alpha \neq 0$), $h \in H$, that $J(x_\alpha, y_\alpha, x_{-\alpha}) \in A_\alpha$. Moreover, $J(x_\alpha, y_\alpha, hz_\alpha) = J(x_\alpha, y_\alpha, z_\alpha)h + u_0$, where $u_0 = J(h, y_\alpha, z_\alpha)x_\alpha \in A_{-\alpha}A_\alpha \subseteq A_0$. Therefore $J(x_\alpha, y_\alpha, z_\alpha) \in A_{-\alpha} + A_0$. On the other hand, expanding the Jacobian $J(x_\alpha, y_\alpha, z_\alpha)$ and taking into account formulas (23) and (27) for multiplication of root spaces we note that $J(x_\alpha, y_\alpha, z_\alpha) \in A_{3\alpha} + A_0$. Since $3\alpha \neq \alpha$, $J(x_\alpha, y_\alpha, z_\alpha) \in A_0$.

To sum up, we state the above results in the following lemma:

Lemma 1.8. *Let H be a nilpotent subalgebra of a Malcev algebra A over a field F. Assume that the regular representation of H in A is split and $A = A_0 + A_1 + \dots$ is the corresponding decomposition of A into root spaces. Then*

$$A_\alpha A_\beta \subseteq A_{\alpha+\beta} \ (\alpha \neq \beta), \qquad A_\alpha^2 \subseteq A_{2\alpha} + A_{-\alpha}, \tag{29}$$
$$J(A_\alpha, A_\beta, A_\gamma) = 0 \ (\alpha \neq \beta \neq \gamma \neq \alpha), \tag{30}$$
$$J(A_\alpha, A_\alpha, A_\beta) = 0 \ (\beta \neq 0, \alpha, -\alpha), \tag{31}$$
$$J(A_\alpha, A_\alpha, A_0) \subseteq A_{-\alpha}. \tag{32}$$

If $\mathrm{char} F \neq 2$ *then*

$$J(A_\alpha, A_\alpha, A_{-\alpha}) \subseteq A_\alpha, \tag{33}$$
$$J(A_\alpha, A_\alpha, A_\alpha) \subseteq A_0. \tag{34}$$

1.6. Let us introduce the important notion of a Cartan subalgebra of Malcev algebra.

Definition 1.9. A subalgebra H of a Malcev algebra A is said to be a *Cartan subalgebra* if it is nilpotent and coincides with the Fitting component A_0 of A with respect to H.

The definition above is similar to the usual definition of Cartan subalgebra of a Lie algebra. Any Cartan subalgebra of A is obviously a maximal nilpotent subalgebra of A. If Ω is an extension of the base field F, then $A_\Omega = A_F \otimes \Omega$ is the corresponding tensor extension of A, and if H is a Cartan subalgebra of A then $H_\Omega = H_F \otimes \Omega$ is a Cartan subalgebra of A_Ω (to prove this it suffices to note that $H = A_0$ coincides with the intersection of root subspaces A_0^h for a finite number of $h \in H$).

The *normalizer* $N(H)$ of a subalgebra $H \subseteq A$ is the set of elements $x \in A$ such that $xH \subseteq H$.

Proposition 1.10. *A subalgebra H of a Malcev algebra A is a Cartan subalgebra of A if and only if it is nilpotent and coincides with its normalizer.*

Proof. For any nilpotent subalgebra H of A we have $H \subseteq N(H) \subseteq A_0$. If H is a Cartan subalgebra then these inclusions become equalities. To prove the other implication, let $H \subset A_0$. Since the regular representation of H in A_0 is nilpotent, by Theorem 1.1 we have H has an induced nilpotent representation in A_0/H. Therefore there exists an element $\xi \neq 0$ in A_0/H annihilated by all operators R_h $(h \in H)$. The preimage x of ξ in A_0 is an element of $N(H)$. Moreover, $x \in H$. $\square$

As for Lie algebras, there exists a simple way of constructing a Cartan subalgebra of a Malcev algebra A if the base field F is sufficiently large, say $|F| \geq \mathrm{dim} A$.

Definition 1.11. An element $x \in A$ is said to be *regular* if the dimension of the Fitting 0 component of A with respect to the operator R_x is minimal.

Proposition 1.12. *If A is a finite dimensional Malcev algebra over a field F with $\dim A \leq |F|$ and x is a regular element of A, then the Fitting 0 component A_0^x of A with respect to R_x is a Cartan subalgebra. Conversely, if H is a Cartan subalgebra of A that contains a regular element h then $H = A_0^h$.*

This can be proved in the same way as in the case of Lie algebras [3]. Note that in the case of binary Lie algebras the proposition does not make sense because A_0^x is not a subalgebra of A. In [13] the definition of a Cartan subalgebra of a binary Lie algebra is more restrictive than that given in Definition 1.9. However, it is not very good because it requires too many conditions to hold; following this definition, Cartan subalgebras might not even exist for Malcev algebras or binary Lie algebras.

2. Generalization of Lie's theorem. Criteria for solvability and semisimplicity of Malcev algebras

2.1. In this section, unless otherwise stated, we assume that the base field F has characteristic 0.

To every representation ρ of a Malcev algebra A we associate the bilinear trace form $(x, y) = \operatorname{tr}(R_x R_y)$. It is clear that (x, y) is symmetric, that is $(x, y) = (y, x)$. It follows from (4) after canceling the 2s that $(yx, x) = 0$. Linearizing this expression in x gives $(yx, z) + (yz, x) = 0$ or

$$(xy, z) = (x, yz), \tag{35}$$

for any $x, y, z \in A$. We call a bilinear form (x, y) satisfying this condition *invariant*. The bilinear form (x, y) associated to the regular representation of a Malcev algebra is called the Killing form. Using the trace technique we can obtain a number of results about Malcev algebras over fields of characteristic 0. The following lemma generalizes Jacobson's well-known lemma [3] about nilpotent elements of a Lie algebra of linear transformations.

Lemma 2.1. *Let A be a Malcev algebra over a field of characteristic 0 such that for some $c \in A$ this relation holds:*

$$c = \sum_{i=1}^{r} a_i b_i, \quad c a_i = 0 \quad (i = 1, \ldots, r).$$

Then the operator R_c is nilpotent in any representation $\rho\colon x \mapsto R_x$ in A.

Proof. Let us show that $ac = 0$ for some $a, c \in A$ implies $\operatorname{tr} R_c^k R_{ab} = 0$ for some $k \geq 1$ and for all $b \in A$. Setting $a = a_i$, $b = b_i$ and summing over i we obtain $\operatorname{tr} R_c^{k+1} = 0$ $(k \geq 1)$, which implies nilpotency of R_c.

Note that by (12), $\operatorname{tr} R_{xyz} = 0$ for all $x, y, z \in A$. Taking this into account and comparing traces of operators on both sides of (17) we obtain $\operatorname{tr} R_x^n R_{yx} = 0$ $(n \geq 1)$. In particular,

$$\operatorname{tr} R_c^n R_{bac} = 0 \quad (n \geq 0). \tag{36}$$

It follows from (9) that $R_{bac} = R_b R_a R_c - R_c R_b R_a + R_a R_{cb}$. Substituting this into (36) we obtain

$$\operatorname{tr} R_c^n R_a R_{cb} = 0 \quad (n \geq 0). \tag{37}$$

On the other hand,

$$0 = R_{cab} = R_c R_a R_b - R_b R_c R_a + R_a R_{bc} - R_{ab} R_c.$$

Multiplying this relation by R_c^n on the left and taking into account (37) we obtain

$$\begin{aligned} \operatorname{tr} R_c^n R_{ab} R_c &= \operatorname{tr}(R_c^{n+1} R_a R_b - R_c^n R_b R_c R_a) \\ &= \operatorname{tr}(R_c^{n+1} R_a - R_c R_a R_c^n) R_b \quad (n \geq 0). \end{aligned}$$

This remains to show that $R_c^{n+1} R_a - R_c R_a R_c^n = 0$ when $n \geq 0$. It follows easily from (16) so the proof is complete. $\square$

In the case of Malcev algebras, the notion of solvability defined for arbitrary nonassociative algebras admits a useful modification. We remark that it follows from (10) that if $I \lhd A$ then $L(I) = I^2 + I^2 \cdot A \lhd A$. For an arbitrary ideal I of a Malcev algebra A we define the chain of ideals $I_k = L_k(I)$, $k \geq 0$, by setting $I_0 = I$ and $I_k = L(I_{k-1})$, $k \geq 1$. We also define the derived series $I^{(k)}$ by $I^{(0)} = I$ and $I^{(k)} = I^{(k-1)} \cdot I^{(k-1)}$, $k \geq 1$. The ideal I is said to be *solvable* (resp. *L-solvable*) if $I^{(k)} = 0$ (resp. $I_k = 0$) for some $k \geq 0$. Since $I_k \supseteq I^{(k)}$ for any k, it follows that any L-solvable ideal of a Malcev algebra A is solvable. The converse is also true.

Proposition 2.2. *[5] Every solvable ideal of a Malcev algebra A is also L-solvable.*

Proof. Yamaguti [15] gives a similar definition of solvability for Malcev algebras. However he did not note that this definition is equivalent to the usual definition of solvability. For the sake of completeness we prove Proposition 2.2. Let $I \lhd A$. Let us show that $I_2 \subseteq I^{(1)} = I^2$. Since $I_1 \subseteq I$, it suffices to show that $I_1^2 \cdot A \subseteq I^2$ or $(I^2 + I^2 A)^2 A \subseteq I^2$, which can be reduced to the proof of $(I^2 \cdot I)A \subseteq I^2$ and $((I^2 A)I)A \subseteq I^2$. Obviously, the first inclusion follows from (10). If $c_1 \in I^2$, $c_2 \in I$, $a_1, a_2 \in A$ then

$$c_1 a_1 c_2 a_2 + a_1 c_2 a_2 c_1 + c_2 a_2 c_1 a_1 + a_2 c_1 a_1 c_2 = (c_1 c_2)(a_1 a_2).$$

Moreover, $a_1 c_2 a_2 c_1, a_2 c_1 a_1 c_2 \in I^2$ and $c_2 a_2 c_1 a_1, c_1 c_2 \cdot a_1 a_2 \in I^3 \cdot A$. Note that we have already seen that $I^3 \cdot A \subseteq I^2$. Suppose that $I_{2k} \subseteq I^{(k)}$ for some $k \geq 1$. Then $I_{2k+2} = L_2(I_{2k}) \subseteq I_{2k}^2 \subseteq I^{(k+1)}$. Consequently, $I^{(n)} = 0$ implies $I_{2n} = 0$, i.e., we have L-solvability of the ideal I. $\square$

Since all elements of the sequence $\{I_k \mid k \geq 0\}$ are ideals of A, it follows from Proposition 2.2 that:

Corollary 2.3. *In any nonzero solvable ideal of a Malcev algebra there exists a nonzero abelian ideal of the algebra.*

A maximal solvable ideal $S(A)$ of an algebra A is said to be the *radical* of the algebra A. If $S(A) = 0$ then A is called *semisimple.* According to the previous remarks, semisimple Malcev algebras can be equivalently defined as Malcev algebras without nontrivial abelian ideals.

In some sense, *reductive Lie algebras*, i.e., Lie algebras whose regular representation is completely reducible, are close to semisimple Lie algebras. More generally, they are defined as algebras with a faithful completely reducible representation. Theorem 8 in [4] gives a description of such algebras. Results about them are similar to results about Lie algebras.

Theorem 2.4. *Let A be a Malcev algebra which has a nearly faithful representation ρ with semisimple enveloping algebra A^*_ρ. Then $A = A_1 + C$ where A_1 is a semisimple subalgebra and C is the center (annihilator) of the algebra A.*

Proof. Let S be the radical of the algebra A. We show that S coincides with the center of A. Otherwise, $S_1 = S \cdot A \subseteq S$ is a nonzero solvable ideal of A. Let S_2 be a nonzero abelian ideal in S_1 (which exists by Corollary 2.3) and set $S_3 = S_2 \cdot A \subseteq S_2$. By Lemma 2.1 each element of the ideal S_3 can be represented by a nilpotent operator, and by Theorem 1.2, S^*_3 is in the radical of A^*_ρ, so $S^*_3 = 0$. Then $S_3 \subseteq \ker\rho$ and thus, since ρ is nearly faithful, $S_3 = 0$. Hence S_2 lies in the center of A. Also $S_2 \subseteq S \cdot A$. Using again Lemma 2.1 and repeating the reasoning we can show that $S_2 = 0$. This contradicts the assumption that S_2 is nonzero and thus $S \cdot A = 0$. For the same reason $S \cap A^2 = 0$ and therefore $A = S + A_1$ where A_1 is a complementary subspace of S containing A^2. Since $A_1 \supseteq A^2$ we immediately have $A_1 \lhd A$. Moreover, $A_1 \cong A/S$ so A_1 is semisimple. □

Definition 2.5. The Lie algebra generated by the operators R_x, $x \in A$ is said to be the *Lie enveloping algebra $L_\rho(A)$ of a representation ρ.*

Identity (12) shows that $L_\rho(A)$ and $\rho(A) + [\rho(A), \rho(A)]$ coincide as vector spaces. If the algebra A is abelian then $L_\rho(A)$ is at least metabelian. The associative enveloping algebra of $L_\rho(A)$ coincides with A^*_ρ.

Corollary 2.6. *Under the hypothesis of Theorem 2.4, if A is a solvable Malcev algebra then A is abelian and the algebra A^*_ρ is commutative. More generally, if ρ is a nearly faithful representation of a solvable Malcev algebra A, and R is the radical of A^*_ρ, then the quotient algebra A^*_ρ/R is commutative.*

Proof. The algebra A is abelian by Theorem 2.4, so $L_\rho(A)$ is at least metabelian. However, since the associative enveloping algebra A^*_ρ of $L_\rho(A)$ is semisimple, then

$L_\rho(A)$ is indeed abelian. Therefore A_ρ^* is commutative. To prove the second claim by analogy with Lie algebras [3] we consider the sequence

$$A \to A_\rho^* \to A_\rho^*/R,$$

which is a representation of a solvable Malcev algebra, so its associative enveloping algebra is the semisimple algebra A_ρ^*/R. □

The following theorem based on Theorem 2.4 and Corollary 2.6 has an important application.

Theorem 2.7. *Let ρ be a nearly faithful representation of a Malcev algebra A in a vector space V, let S be the radical of A, let R be the radical of A_ρ^*, and let $\bar\rho$ be the induced representation $A \to A_\rho^*/R$ with $I = \widetilde{\ker}\bar\rho$. Then I is a nilpotent ideal of A which coincides with the set S_0 consisting of all the elements of S which are nilpotent with respect to ρ. Moreover, $S \cdot A \subseteq S_0$.*

Proof. Let R_0 be the radical of the subalgebra $S^* \leq A_\rho^*$. Then by Corollary 2.6, S^*/R_0 is semisimple and commutative. The set S_0 coincides with the kernel of the representation $S \to S^*/R_0$, so S_0 is a subspace of S. Consider the representation $\bar\rho$; its enveloping algebra is the semisimple algebra A_ρ^*/R. Elements of the ideal I are represented by nilpotent operators with respect to ρ. Then by Theorem 1.2, I is a nilpotent ideal in A, i.e., $I \subseteq S$ and by definition of S_0, $I \subseteq S_0$. The radical of the algebra $\bar A = A/I$ equals S/I and the induced representation $\bar A \to A_\rho^*/R$ is nearly faithful. By Theorem 2.4, the radical of $\bar A$ coincides with its center, so $S \cdot A \subseteq I \subseteq S_0$, where S_0 is an ideal of A. Again by Theorem 1.2 we have $S_0^* \subseteq R$ and therefore $S_0 \subseteq \widetilde{\ker}\bar\rho = I$. The other inclusion was already proved. □

Corollary 2.8. *If S is the radical and N is the nil-radical of an algebra A then $S \cdot A \subseteq N$. In particular, if A is solvable then A^2 is nilpotent.*

Lemma 2.9. *Let ρ be a split representation of a solvable algebra A and let V be irreducible. Then V is one-dimensional.*

Proof. The algebra A_ρ^* is semisimple and owing to solvability of A it is also commutative. The rest of the proof is obvious. □

Theorem 2.10. *Let ρ be a split representation of a Malcev algebra A. Then all matrices R_x can be simultaneously reduced to triangular form. In other words, in the vector space V there exists an A-invariant flag of subspaces.*

The same is true for split representations of nilpotent Malcev algebras. However, in this case the subspace of a representation is a direct sum of weight spaces by Theorem 1.7 and therefore the matrices R_x have a more specific form, as in the case of Lie algebras.

Theorem 2.11. *Let ρ be a representation of a nilpotent Malcev algebra A in a vector space V. Then V can be decomposed into the direct sum of weight spaces V_α, and all matrices corresponding to the restriction of R_x to V_α can be simultaneously reduced to triangular form with $\alpha(x)$ on the main diagonal.*

Corollary 2.12. *Under the hypothesis of Theorem 2.11 the weights $\alpha\colon A \to F$ are linear maps that are 0 on A^2.*

This last corollary implies that elements from A^2 are represented by nilpotent operators. Moreover, this is true even in the case of a solvable algebra A. Indeed, by Theorem 2.7 we have $S \cdot A = A^2 \subseteq S_0$.

2.2. The following is the proof of solvability and semisimplicity criteria for Malcev algebras over fields of characteristic 0, which is similar to the well-known Cartan criteria for Lie algebras [3].

Let F be an algebraically closed field, let H be a Cartan subalgebra of the Malcev algebra A over F, and let ρ be a representation of A in V. Then V can be decomposed into the sum of weight spaces V_α with respect to the representation of H in V induced by ρ. On the other hand, A has a decomposition into the sum of subspaces A_β with respect to the subalgebra H ($A_0 = H$). Let us show that

$$V_\alpha A_\beta \subseteq V_{\alpha+\beta}\ (\alpha \neq \beta), \quad V_\alpha A_\alpha \subseteq V_{2\alpha} + V_{-\alpha}, \tag{38}$$

where as usual we assume that $V_\alpha = 0$ if α is not a weight of H in V. Consider the semidirect extension $E = V + A$ of A given by ρ and the regular representation of H in E. Since H is a nilpotent subalgebra of E, we can decompose E into the sum of root spaces with respect to H. These subspaces are of the form $V_\alpha + A_\alpha$ where one of the terms can be absent (for example V_α, if a root α of H in A is not a weight of H in V). Indeed, a system of such spaces satisfies the conditions of Theorem 1.7. By Lemma 1.8 we have

$$V_\alpha A_\beta \subseteq E_{\alpha+\beta} \cap V = (V_{\alpha+\beta} + A_{\alpha+\beta}) \cap V = V_{\alpha+\beta}.$$

The second formula of (38) can be proved in a similar way.

Lemma 2.13. *If α, β, γ are pairwise distinct weights then the identity $v_\alpha(x_\beta x_\gamma) = (v_\alpha x_\beta)x_\gamma$ holds for any $v_\alpha \in V_\alpha$, $x_\beta \in A_\beta$ and $x_\gamma \in A_\gamma$. The same is true if $\alpha \neq 0$, $\beta = \gamma = 0$.*

Proof. The proof is similar to that of (38). For the algebra $E = V + A$ this lemma claims that $J(V_\alpha, A_\beta, A_\gamma) = 0$, $J(V_\alpha, A_0, A_0) = 0$. It suffices to apply Lemma 1.8. □

Note that $A^2 = \sum A_\alpha A_\beta$. Formulas for multiplication of root spaces show that

$$H \cap A^2 = \sum_\alpha A_\alpha A_{-\alpha}.$$

Lemma 2.14. *Let A be a Malcev algebra over an algebraically closed field F of characteristic 0, let H be a Cartan subalgebra of A, and let ρ be a representation of A in a vector space V. Suppose that $\alpha, -\alpha$ are roots of H, $e_\alpha \in A_\alpha$, $e_{-\alpha} \in A_{-\alpha}$ and $h_\alpha = e_\alpha \cdot e_{-\alpha}$. Then for any weight φ of H in V the value of $\varphi(h_\alpha)$ is a rational multiple of $\alpha(h_\alpha)$.*

Proof. If φ is an integer multiple of α then the claim is obviously true for any $h \in H$, in particular, for any h_α. Let φ be a non-multiple of α. Consider the direct sum U of subspaces of the form $V_{\varphi+k\alpha}$, where k runs over the set of integers (of course, we assume that this sum has a finite number of nonzero terms). The subspace U is invariant with respect to e_α and $e_{-\alpha}$. The hypothesis of Lemma 2.13 holds for the weights $\varphi + k\alpha$, α and $-\alpha$, hence R_{h_α} restricted to U equals $[R_{e_\alpha}, R_{e_{-\alpha}}]$, and therefore the trace of R_{h_α} restricted to U equals 0. The rest of the proof is similar to that of Lemma 1.3 in [3]. □

Note that if $n_\alpha = \dim V_\alpha$ then

$$0 = \mathrm{tr}_U R_{h_\alpha} = \sum_k n_{\varphi+k\alpha} \cdot (\varphi + k\alpha)(h_\alpha),$$

$$\varphi(h_\alpha) = r_{\varphi,\alpha} \cdot \alpha(h_\alpha),$$

$$\text{where } r_{\varphi,\alpha} = -\sum_k k n_{\varphi+k\alpha} \Big/ \sum_k n_{\varphi+k\alpha}.$$

Theorem 2.15. *Let A be a Malcev algebra over a field of characteristic 0, and let ρ be a nearly faithful representation of A such that the bilinear form on $A' = A^2$ associated to ρ is trivial. Then A is solvable.*

Proof. Replacing the base field F by an algebraic extension if necessary, we use induction on the dimension of A. As in [3], it can be shown that A' is strictly contained in A. If $A = A^2$ then $H = \sum_\alpha A_\alpha \cdot A_{-\alpha}$ and by Lemma 2.14 the condition $\mathrm{tr}\, R^2_{h_\alpha} = 0$ implies $\varphi(h_\alpha) = 0$ for any weight φ of H in V. It follows from linearity of weights that $\varphi = 0$ is the only weight of H, that is, $V = V_0$. Then $VA_\alpha = 0$ for any $\alpha \neq 0$, and the representation ρ of A can be reduced to a representation of H with weight 0, i.e., ρ is a representation of A by nilpotent operators. By Theorem 1.1 A is nilpotent, but this contradicts $A = A^2$. Let ρ' be the restriction of ρ to A', $I = \widetilde{\ker \rho'} \subseteq \ker \rho$. Then A'/I satisfies the induction hypothesis and is solvable. By Proposition 2.2 it is also L-solvable, i.e., $L_m(A') \subseteq I \subseteq \ker \rho$ for some $m \geq 0$. Since $L_m(A') \lhd A$ and the representation of ρ is nearly faithful, $L_m(A') = 0$ and it follows that A is solvable. □

Corollary 2.16. *A Malcev algebra A over a field of characteristic 0 is solvable if and only if $\mathrm{tr}\, R_x^2 = 0$ for all $x \in A^2$ (here R_x is the operator of right multiplication by $x \in A$).*

To prove the necessary condition it suffices to note that in the regular representation of a Malcev algebra A the operators R_x, for $x \in A^2 \subseteq N$, are nilpotent.

Theorem 2.17. *Let ρ be a nearly faithful representation of a semisimple Malcev algebra A. Then the form associated with ρ is non-degenerate. If the Killing form of an algebra A is non-degenerate then A is semisimple.*

Proof. The proof of the first claim, like the proof of Theorem 2.15, uses L-solvability specifically. It follows from invariance of the form associated to the representation ρ that its kernel B is an ideal of A. Assume that $B \neq 0$ and let ρ' be the restriction of ρ to B and let $I = \widetilde{\ker}\rho'$. Then B/I satisfies the hypothesis of Theorem 2.15 and thus it is solvable; therefore, it is L-solvable: $L_m(B) \subseteq I \subseteq \ker\rho$. However, $L_m(B) \lhd A$ so $L_m(B) = 0$ and B is a solvable ideal of A, a contradiction.

The second claim of the theorem was proved by Sagle [11] and it is clearly a consequence of Dieudonné's theorem [3] (it follows from this theorem that a nonassociative algebra with non-degenerate invariant Killing form can be decomposed into the direct sum of simple ideals; therefore, this algebra is semisimple). However, taking into account Corollary 2.6, it is possible to prove this second claim by repeating the arguments from the Lie algebra case: if A is not semisimple then A contains a nonzero abelian ideal and such an ideal is contained in the kernel of the Killing form. □

Corollary 2.18. *Any nearly faithful representation of a semisimple Malcev algebra is faithful.*

Since the non-degeneracy of the Killing form does not depend on extensions of the base field, the following holds:

Corollary 2.19. *A Malcev algebra A over a field F of characteristic 0 is semisimple if and only if A_Ω is semisimple over any extension Ω of the field F.*

Below are a few more facts whose proofs are standard.

Structure Theorem. If A is a finite dimensional semisimple Malcev algebra over a field of characteristic 0 then A can be decomposed into the direct sum of ideals which are simple algebras.

Corollary 2.20. *If A is a semisimple algebra then any ideal of A is a semisimple subalgebra.*

Corollary 2.21. *If A is semisimple then $A = A^2$.*

Corollary 2.22. *If S is the radical of an algebra A and $B \lhd A$ then $B \cap S$ is the radical of B.*

Proposition 2.23. *If N is the nil-radical of an algebra A and $B \lhd A$ then $B \cap N$ is the nil-radical of B.*

Proof. If N_1 is the nil-radical of B and S_1 is the radical of B then $N_1 \subseteq S_1 \subseteq S$ and $N_1 A \subseteq S \cdot A \cap B \subseteq N \cap B \subseteq N_1$. Therefore N_1 is a nilpotent ideal of A and $N_1 \subseteq N \cap B$. □

Proposition 2.24. *The radical S of a Malcev algebra A coincides with the orthogonal complement in A of the subalgebra A^2 with respect to the Killing form of A.*

Corollary 2.25. *Any solvable (resp. nilpotent) subinvariant subalgebra of an algebra A lies in the radical (resp. nilradical) of A.*

Remark 1. The solvability and semisimplicity criteria for Malcev algebras are similar to the Cartan criteria. (Theorems 2.15 and 2.17 were first obtained only for the regular representation in [9] by using the connection between Malcev algebras and Lie triple systems (LTS) and their embeddings into Lie algebras.)

In §§4 and 5 we will return to the study of Malcev algebras of characteristic 0.

3. Simple Malcev algebras over a field of arbitrary characteristic

In this section we assume that the base field F has either characteristic 0 or $p > 3$. We consider the classification of non-Lie simple Malcev algebras over F.

3.1. Let A be a non-Lie simple Malcev algebra, let H be a Cartan subalgebra of A, and assume that the regular representation of H in A is split. (If such a subalgebra exists, then it is called a *split Cartan subalgebra* and A is called *split*. Proposition 1.12 shows that in order for Cartan subalgebras to exist the base field F must be infinite; if F is algebraically closed then any Lie subalgebra is split.) Note that there exist nonzero roots α of H in A. Indeed, otherwise we would have $A = A_0 = H$ and A would be nilpotent, which is not possible. Identity (11) shows that the subspace $J(A, A, A)$ is an ideal of A. Thus

$$A = J(A, A, A). \tag{39}$$

Lemma 3.1. *[12] If for some $x, y \in A$ we have*

$$J(x, y, A) = 0, \tag{40}$$

then $xy = 0$.

Proof. Equation (40) can be written as $R_{xy} = [R_x, R_y]$. Then $D(x, y) = 2R_{xy}$ and the identity $R_{xD(x,y)} = [R_z, D(x, y)]$ implies that either $R_{z(xy)} = [R_z, R_{xy}]$ for any $z \in A$ or

$$J(xy, A, A) = 0. \tag{41}$$

This argument shows, in particular, that the set of elements $x \in A$ such that $J(x, A, A) = 0$ (the so-called *center* of A) is a Lie ideal in A. In a simple algebra A this ideal must be equal to 0 and, in particular, $xy = 0$. □

Lemma 3.2. *[12] For any nonzero root α of a subalgebra H in A we have $A_\alpha^2 \subseteq A_{-\alpha}$. Moreover, $A = A_0 + A_\alpha + A_{-\alpha}$ and $A_0 = A_\alpha A_{-\alpha}$.*

Proof. Let $x_\alpha y_\alpha = z_{2\alpha} + z_{-\alpha}$; see (27). Then by (21) we have $J(h, x_\beta, z_{2\alpha}) = 0$ for all $\beta \neq 2\alpha$. If $\beta = 2\alpha$, then by Lemma 1.8 we have

$$\begin{aligned} J(h, x_{2\alpha}, z_{2\alpha}) &= J(h, x_{2\alpha}, x_\alpha y_\alpha) \\ &= -J(x_\alpha, x_{2\alpha}, hy_\alpha) + J(h, x_{2\alpha}, y_\alpha)x_\alpha + J(x_\alpha, x_{2\alpha}, y_\alpha)h = 0. \end{aligned}$$

Therefore $J(h, z_{2\alpha}, A) = 0$ and $hz_{2\alpha} = 0$, and since $h \in H$ was chosen arbitrarily, we have $z_{2\alpha} = 0$. Using what was just proved, the subspace

$$B = A_\alpha A_{-\alpha} + A_\alpha + A_{-\alpha} \subseteq A_0 + A_\alpha + A_{-\alpha},$$

is invariant under multiplications by A_α and $A_{-\alpha}$. Invariance of $A_\alpha A_{-\alpha}$ with respect to multiplication by A_0 follows from the relation $J(A_0, A_\alpha, A_{-\alpha}) = 0$. Thus B is a subalgebra. Let us show that B is an ideal of A. By (30) and (31), for any $\beta \neq 0, \alpha, -\alpha$ we have $J(A, A_\alpha, A_\beta) = 0$ and $A_\alpha A_\beta = 0$. Similarly, $A_{-\alpha} A_\beta = 0$. It follows from $J(A_\alpha, A_{-\alpha}, A_\beta) = 0$ that $(A_\alpha A_{-\alpha})A_\beta = 0$. Hence $BA \subseteq B$ and $B \lhd A$. Therefore $B = A$ and, in particular, $A_0 = A_\alpha A_{-\alpha}$. □

Lemma 3.2 shows that the system of roots of A has a very simple structure.

Lemma 3.3. *The subalgebra $H = A_0$ is abelian. A root $\alpha\colon A \to F$ is a linear map.*

Proof. Using for example (11) we can show that the subspace $J(A_0, A_0, A_0)$ is invariant under multiplications by A_0, A_α and $A_{-\alpha}$, i.e., it is an ideal of A. Therefore

$$J(A_0, A_0, A_0) = 0, \quad J(A_0, A_0, A) = 0, \quad A_0^2 = 0. \tag{42}$$

By (42), for any $x, y \in H$ we have $R_{xy} = R_x R_y - R_y R_x = 0$. Therefore, the operators R_x and R_y have a common eigenvector e_α in A_α: $e_\alpha(x+y) = [\alpha(x), \alpha(y)]e_\alpha$. However, the operator R_{x+y} has the unique eigenvalue $\alpha(x+y)$. Thus $\alpha(x+y) = \alpha(x) + \alpha(y)$ and the lemma is proved. □

Let us choose an element $h_0 \in H$ such that $\alpha(h_0) = 1$. Then any element $h \in H$ can be represented in the form $h = \alpha(h)h_0 + h_1$ where $\alpha(h_1) = 0$. For any $x \in A_\alpha$, $y \in A_{-\alpha}$, $h \in H$ we have

$$\begin{aligned} &0 = J(h, x, y) = hx \cdot y + yh \cdot x, \qquad xh \cdot y = -x \cdot yh, \\ &x[\alpha(h) - R_h] \cdot y = x \cdot y[\alpha(h) + R_h]. \end{aligned} \tag{43}$$

Lemma 3.4. *Let $h \in H$, $h \neq 0$ and let U be any cyclic subspace of A_α (or $A_{-\alpha}$) with respect to R_h. Then for any $u_1, u_2 \in U$ we have $u_1 u_2 = 0$.*

Proof. Let us choose any element u of maximal height in U. For all $h' \in H$ we have $J(h', h, u) = 0$, i.e., the triple of elements $\{h', h, u\}$ is Lie. By [10] it generates a Lie subalgebra $B \leq A$. In particular, $J(U, U, h') = 0$. Therefore, the operator $R_{h'}$ is a derivation of the linear subspace $U \cdot U$ and, since $h' \in H$ was arbitrary, $U \cdot U \subseteq A_{2\alpha}$. However, 2α is not a root, so $U \cdot U = 0$. □

Formula (39) shows that

$$A_{-\alpha} = J(A_0, A_\alpha, A_\alpha) + J(A_{-\alpha}, A_{-\alpha}, A_\alpha). \tag{44}$$

Using identity (11) and the known relations for root subspaces we can show that

$$\begin{aligned} &A_0 J(A_0, A_\alpha, A_\alpha) \subseteq J(A_0, A_\alpha, A_\alpha), \\ &A_0 J(A_{-\alpha}, A_{-\alpha}, A_\alpha) = J(A_0, A_\alpha, A_{-\alpha}^2) \subseteq J(A_0, A_\alpha, A_\alpha). \end{aligned}$$

Multiplying both sides of (44) on the left by A_0 we obtain $A_{-\alpha} \subseteq J(A_0, A_\alpha, A_\alpha)$. Since the converse inclusion also holds we have

$$A_{-\alpha} = J(A_0, A_\alpha, A_\alpha) \subseteq A_\alpha^2 + A_\alpha^2 \cdot A_0.$$

Similarly $A_\alpha = J(A_0, A_{-\alpha}, A_{-\alpha})$. In particular, $A_\alpha^2 \neq 0$ and $A_{-\alpha}^2 \neq 0$.

Lemma 3.5. *For all $x, y \in A_\alpha$, $h \in A_0$ we have*

$$yx \cdot x = 0, \quad hx \cdot x = 0. \tag{45}$$

Proof. Set $y = J(a_0, a_{-\alpha}, b_{-\alpha})$. Then by (6)

$$\begin{aligned} yx &= J(b_{-\alpha}, a_0, a_{-\alpha})x \\ &= -J(x, a_0, a_{-\alpha})b_{-\alpha} + J(b_{-\alpha}, a_0, xa_{-\alpha}) + J(x, a_0, b_{-\alpha}a_{-\alpha}) \\ &= J(x, a_0, b_{-\alpha}a_{-\alpha}) = J(x, a_0, c_\alpha), \\ yx \cdot x &= J(x, a_0, xc_\alpha) \in J(A_0, A_\alpha, A_{-\alpha}) = 0. \end{aligned}$$

The second claim follows from Lemma 3.4. □

Let us denote the system of roots of H in A by Δ; then $\Delta = \{0, \alpha, -\alpha\}$. We denote by (x, y) the symmetric bilinear form on A given by

$$(x, y) = \begin{cases} 0 & x \in A_\beta;\ y \in A_\gamma;\ \beta, \gamma \in \Delta;\ \beta + \gamma \neq 0; \\ \alpha(x)\alpha(y) & x, y \in A_0; \\ \alpha(x \cdot y_1) & x \in A_\alpha;\ y_1 \in A_{-\alpha};\ y = y_1 h_0. \end{cases} \tag{46}$$

Since the restriction of R_{h_0} to $A_{-\alpha}$ is non-degenerate, the form (46) is well-defined. In all previous lemmas the expressions were symmetric in α and $-\alpha$; however, in the definition of the form (46) this symmetry is lost. Let us show that this apparent asymmetry does not in fact hold. We change α to $\alpha' = -\alpha$ and h_0

to $h_0' = -h_0$ so that $\alpha'(h_0') = 1$. Then for $x, y \in A_0$ we have $(x, y) = \alpha(x)\alpha(y) = \alpha'(x)\alpha'(y)$. For $x \in A_\alpha$, $y \in A_{-\alpha}$ the definition of the form (46) can be written as $(xh_0, yh_0) = \alpha(xh_0 \cdot y)$. Let us check that $(yh_0', xh_0') = \alpha'(yh_0' \cdot x)$. Indeed,

$$\begin{aligned}(yh_0', xh_0') &= (yh_0, xh_0) = (xh_0, yh_0) = \alpha(xh_0 \cdot y) = \alpha(-x \cdot yh_0) = \alpha(yh_0 \cdot x)\\ &= \alpha'(yh_0' \cdot x).\end{aligned}$$

Lemma 3.6. *The form* (46) *is invariant; i.e., for all $x, y \in A$* (35) *holds.*

Proof. Taking into account the linearity of (35) in x, y, z, it suffices to consider the cases when x, y, z are in the root subspaces. Omitting the trivial relations, we need to check that $(xh, y) = (x, hy)$ and $(xy, h) = (x, yh)$ only when $x \in A_\alpha$, $y \in A_{-\alpha}$, $h \in H$, and the cases $x, y, z \in A_\alpha$ and $x, y, z \in A_{-\alpha}$.

(a) Let $x \in A_\alpha$, $y \in A_{-\alpha}$. Setting $y = y_1 h_0$ ($y_1 \in A_{-\alpha}$) we obtain by definition $(xh, y) = \alpha(xh \cdot y_1)$ and $(x, hy) = (x, hy_1 \cdot h_0) = \alpha(x \cdot hy_1)$; then the equality $(xh, y) = (x, hy)$ follows from $xh \cdot y_1 = x \cdot hy_1$.

(b) For the same x, y, h, y_1 we have $(xy, h) = \alpha(xy)\alpha(h) = \alpha(x \cdot y_1 h_0)\alpha(h)$ and $(x, yh) = \alpha(x \cdot y_1 h)$. Let us show that the following identity holds:

$$\alpha(x \cdot yh_0)\alpha(h) = \alpha(x \cdot yh),\ x \in A_\alpha, y \in A_{-\alpha}. \tag{47}$$

Note that (47) is linear in h; if $h = h_0$ then it is trivial. It remains to consider the case $\alpha(h) = 0$. Write $x \cdot yh = h_1$. Since $\alpha(h) = 0$, the operator R_h is nilpotent. Let $xR_h^{m-1} = x_1 \neq 0$, $x_1 h = 0$ ($m \geq 1$). It follows from $J(x, y, h) = 0$ that x, y, h, x_1 belong to the same Lie subalgebra of A. In particular,

$$0 = J(x, x_1, yh) = xx_1 \cdot yh + (x_1 \cdot yh)x + x_1 h_1 = x_1 h_1,$$

since $xx_1 = 0$ by Lemma 3.4, and $x_1 \cdot yh = -x_1 h \cdot y = 0$ since $x_1 h = 0$. It follows from $x_1 h_1 = 0$ that $\alpha(h_1) = 0$.

(c) Let $x, y, z \in A_\alpha$. We rewrite identity (35) in the form $(yx, z) + (yz, x) = 0$, so it suffices to prove that $(yx, x) = 0$ ($x, y \in A_\alpha$) and then linearize in x. Setting $x = x_1 h_0$ ($x_1 \in A_\alpha$) and using the previous arguments we get $(yx, x) = (yx \cdot x_1, h_0) = \alpha(yx \cdot x_1)$. Let us prove that $yx \cdot x_1 = 0$. Linearizing the second identity in (45) we obtain $yx = y \cdot x_1 h_0 = -x_1 \cdot yh_0 = yh_0 \cdot x_1$. Using the first relation in (45) we have $yx \cdot x_1 = (hy_0 \cdot x_1)x_1 = 0$ as desired. The case $x, y, z \in A_{-\alpha}$ is immediate owing to the symmetry of the roots α and $-\alpha$, so the lemma is proved. □

The form (x, y) is non-trivial since, for example $(h_0, h_0) = 1$. It follows from its invariance and the simplicity of A that the form is non-degenerate. If $\alpha(h) = 0$ for some $h \in H$ then by (46) we have $(h, A) = 0$ and therefore $h = 0$. Consequently the subalgebra H is one-dimensional: $H = (h_0)$. The subspaces A_α and $A_{-\alpha}$ are dual to each other with respect to (x, y); in particular, $\dim A_\alpha = \dim A_{-\alpha}$. If $x \in A_\alpha$ and $y \in A_{-\alpha}$ then $xy = \lambda h_0$ where $\lambda = (xy, h_0) = (x, yh_0)$. Hereafter we will denote the element h_0 simply by h.

Lemma 3.7. *All cyclic subspaces with respect to R_h in A_α (and $A_{-\alpha}$) are one-dimensional.*

Proof. Let U be a cyclic subspace in A_α with $\dim U = n > 0$, let $x_1, \dots x_n$ be a cyclic basis of U (here x_k is a vector of height k), and let y be an eigenvector (with respect to R_h) from $A_{-\alpha}$. Then it follows from (43) that $xy = 0$ for any vector $x \in U$ of height less than n; in particular, $x_1 \cdot y = 0$. Let V be an arbitrary cyclic subspace of $A_{-\alpha}$. Let us show that $x_1 \cdot V = 0$. If $\dim V = 1$ then this is already known, so let $\dim V = m > 1$ and let $y_1, \dots, y_m$ be a cyclic basis of V. Then $x_1 y_i = 0$ for $i = 1, \dots, m-1$. If $x_1 y_m \neq 0$ then, without loss of generality, $x_1 y_m = h$. Since A is binary Lie, the elements x_1 and y_m generate a Lie subalgebra in A with basis $x_1, y_1, \dots, y_m, h$. Then $0 = J(x_1, y_m, y_1) = x_1 y_m \cdot y_1 = y_1$, which is impossible. Consequently, $x_1 A_{-\alpha} = 0$ and $(x_1, A_{-\alpha}) = 0$, which contradicts the non-degeneracy of (x, y). The lemma is then proved. □

Lemma 3.7 shows that the operator R_h acts diagonally on A_α and $A_{-\alpha}$. Its restriction to A_α is the identity operator 1 and its restriction to $A_{-\alpha}$ is -1. In particular, for all $x \in A_\alpha$, $y \in A_{-\alpha}$ we have $xy = -(x, y)h$.

Further arguments can be made as in the case of characteristic 0 [16]. For all $x, y, z \in A_\alpha$ we have $xy \cdot z = yz \cdot x = zx \cdot y = (xy, z)h$; furthermore, $J(x, y, h) = -3xy$. If $x, y \in A_\alpha$, $z' \in A_{-\alpha}$ then

$$J(x, y, z'h) + J(z', y, xh) = J(x, y, h)z' = -3xy \cdot z'. \tag{48}$$

Also, the left side of (48) equals $-2J(x, y, z')$; therefore, $3xy \cdot z' = 2J(x, y, z')$ or

$$xy \cdot z' = 2(yz' \cdot x + z'x \cdot y). \tag{49}$$

According to (49), for any elements $x, y, z, t \in A_\alpha$ we have

$$xz \cdot yt = 2\left[(z \cdot yt)x + (yt \cdot x)z\right] = 2yztx + 2txyz.$$

Comparing this identity with (10) we obtain

$$xyzt = yztx - ztxy + txyz. \tag{50}$$

We now have enough identities to construct a basis and a multiplication table for A. Taking into account that $A_\alpha^2 \neq 0$, we choose two arbitrary elements $x, y \in A_\alpha$ for which $xy = z' \neq 0$. Then $xz' = yz' = 0$. If $z \in A_\alpha$ such that $zz' = \frac{1}{2}h$ then x, y, z are linearly independent and (50) shows that any element $t \in A_\alpha$ is a linear combination of x, y, z. Therefore, $\dim A_\alpha = \dim A_{-\alpha} = 3$. Write $yz = x'$ and $zx = y'$. Then $xx' = yy' = zz' = \frac{1}{2}h$, and it follows from the orthogonality of elements $\{x, y, z\}$ and $\{x', y', z'\}$ that $\{x', y', z'\}$ is a basis of $A_{-\alpha}$. In order to find the multiplication formulas for A_α we use identity (49):

$$x'y' = yz \cdot zx = 2\left[(z \cdot zx)y + (zx \cdot y)z\right] = 2(zx \cdot y)z = 2y'y \cdot z = -hz = z.$$

Similarly $y'z' = x$ and $z'x' = y$. Thus the multiplication table for A is complete. Note that $\dim A = 7$. We can find an explicit automorphism of order 2 which interchanges A_α and $A_{-\alpha}$. This automorphism sends x to x', y to y', z to z' and $h = 2xx'$ to $2x'x = -h$.

There is a close relation between A and a split Cayley-Dickson algebra C over F. Recall that C is a simple alternative algebra whose elements are matrices

$$\begin{pmatrix} \alpha & a \\ b & \beta \end{pmatrix},$$

where $\alpha, \beta \in F$ and a, b are arbitrary vectors of a 3-dimensional vector space over F. If $a \times b$ is the ordinary vector product and (a, b) is the dot product with the identity matrix as the Gram matrix for the chosen basis, then the product of two elements of C is given by the formula

$$\begin{pmatrix} \alpha & a \\ b & \beta \end{pmatrix}\begin{pmatrix} \gamma & c \\ d & \delta \end{pmatrix} = \begin{pmatrix} \alpha\gamma - (a, d) & \alpha c + \delta a + b \times d \\ \gamma b + \beta d + a \times c & \beta\delta - (b, c) \end{pmatrix}.$$

We define a new multiplication in C by $x * y = \frac{1}{2}[x, y]$, slightly different from the commutator; C becomes a Malcev algebra $C^{(-)}$ with respect to this operation. Elements of the form $\operatorname{diag}(\alpha, \alpha)$ form the 1-dimensional center of $C^{(-)}$. The complementary subspace for the center consists of the matrices of trace 0. In fact, this subspace is a subalgebra denoted by $C^{(-)}/F$. Multiplication in $C^{(-)}/F$ is given by

$$\begin{pmatrix} \alpha & a \\ b & -\alpha \end{pmatrix} * \begin{pmatrix} \beta & c \\ d & -\beta \end{pmatrix} = \begin{pmatrix} \frac{1}{2}[(b, c) - (a, d)] & \alpha c - \beta a + b \times d \\ \beta b - \alpha d + a \times c & \frac{1}{2}[(a, d) - (b, c)] \end{pmatrix}. \tag{51}$$

Comparing (51) with the known multiplication table of the algebra A shows that A is isomorphic to $C^{(-)}/F$. To the element h corresponds the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$

and to the element $\alpha_1 x + \alpha_2 y + \alpha_3 z + \beta_1 y' + \beta_2 y' + \beta_3 z'$ corresponds the matrix

$$\begin{pmatrix} 0 & b \\ a & 0 \end{pmatrix}, \ a = (\alpha_1, \alpha_2, \alpha_3), b = (\beta_1, \beta_2, \beta_3).$$

This correspondence is the isomorphism $A \to C^{(-)}/F$.

Theorem 3.8. *If F is an arbitrary field of characteristic not 2 or 3, then there exists a unique non-Lie split simple Malcev algebra A over F. This algebra is isomorphic to the algebra $C^{(-)}/F$ obtained from the Cayley-Dickson algebra C over F using the operation $x * y = \frac{1}{2}(xy - yx)$ and factoring out the center.*

The following proposition clarifies the meaning of the bilinear form (46) on A.

Proposition 3.9. *For all $x, y \in A$ we have*

$$xy \cdot y = (y,y)x - (x,y)y. \tag{52}$$

Proof. The proof is based on the multiplication table for A. Using the isomorphism $A \cong C^{(-)}/F$, computations can be performed using the matrix form. It should be noted that if

$$x \rightsquigarrow \begin{pmatrix} \alpha & a \\ b & -\alpha \end{pmatrix}, \qquad y \rightsquigarrow \begin{pmatrix} \beta & c \\ d & -\beta \end{pmatrix},$$

then by the above isomorphism we have $(x,y) = \alpha\beta - \frac{1}{2}\left[(a,d) + (b,c)\right]$. □

Identity (52) shows that the bilinear form (46) on A can be defined independently of the choice of the Cartan subalgebra H. Moreover, it follows from (52) that for all $x, y \in A$ the subspace spanned by x, y, xy is a subalgebra, i.e., any two elements $x, y \in A$ generate a subalgebra which is at most 3-dimensional.

Lemma 3.10. *We have*

$$(xy, xy) = (x,y)^2 - (x,x)(y,y). \tag{53}$$

Proof. This claim is trivial if $x = 0$, so let $x \neq 0$. Replacing y by xy in (52) we get $(x \cdot xy)(xy) = (xy, xy)x$. On the other hand,

$$(x \cdot xy)(xy) = \left[(x,x)y - (x,y)x\right](xy) = \left[(x,y)^2 - (x,x)(y,y)\right]x,$$

hence the assertion follows. □

Linearizing (53) on y we obtain

$$(xy, xz) = (x,y)(x,z) - (x,x)(y,z). \tag{54}$$

It is well known that the problem of the classification of finite dimensional simple algebras over the field F can be reduced to the description of central simple algebras over F and over finite extensions of F. Let us describe central simple non-Lie Malcev algebras over a field F of characteristic not 2 or 3. Let A be an algebra as above. If F is algebraically closed then A is split and its structure is well known. In general, let $\bar{F}$ be the algebraic closure of F and $\bar{A} = A_F \otimes \bar{F}$ be the corresponding extension of A. Then $\bar{A}$ is a central simple Malcev algebra over $\bar{F}$ and $\dim_F A = \dim_{\bar{F}} \bar{A} = 7$. Let (x,y) be the bilinear form (46) defined on $\bar{A}$. Identity (52) shows that the restriction of this form to A is defined over F, and it is a non-singular bilinear form, which we also denote by (x,y). We construct a basis $\{e_1, \ldots, e_7\}$ of the algebra A as follows. We choose e_1, e_2 to be two arbitrary non-isotropic elements of A which are orthogonal with respect to (x,y) and write $(e_1,e_1) = -\alpha$, $(e_2,e_2) = -\beta$, $e_1e_2 = e_3$. Then e_1, e_2, e_3 are pairwise orthogonal and it follows from (52) and (53) that $e_2e_3 = \beta e_1$, $e_3e_1 = \alpha e_2$ and $(e_3,e_3) = -\alpha\beta \neq 0$. The subspace (e_1, e_2, e_3) is non-singular. Its orthogonal complement $(e_1, e_2, e_3)^\perp$ has the same property. We choose as e_4 any non-isotropic element of $(e_1, e_2, e_3)^\perp$ and write $(e_4, e_4) = -\gamma$, $e_1e_4 = e_5$, $e_2e_4 = e_6$, $e_3e_4 = e_7$. Then by (54) for any $i, j = 1, 2, 3$ we have $(e_i, e_je_4) = (e_ie_j, e_4) = 0$ and $(e_ie_4, e_je_4) = -(e_4, e_4)(e_i, e_j)$, which implies that e_5, e_6e_7 are non-isotropic and $e_1, \ldots, e_7$ are mutually orthogonal. Therefore e_i $(i = 1, \ldots, 7)$ form a basis of A. Using the linearization of (52) we obtain for $i, j = 1, 2, 3$ that

$$e_ie_4 \cdot e_j + e_ie_j \cdot e_4 = -(e_i, e_j)e_4, \qquad e_4e_i \cdot e_4e_j + (e_4 \cdot e_4e_j)e_i = 0.$$

As a result, the multiplication table of A in the chosen basis is as follows, where $i, j = 1, 2, 3$ $(i \neq j)$:

$$\begin{array}{lll} e_1e_2 = e_3, & e_2e_3 = \beta e_1, & e_3e_1 = \alpha e_2, \\ e_ie_4 = e_{i+4}, & e_ie_{i+4} = (e_i, e_i)e_4, & e_4e_{i+4} = \gamma e_i, \\ e_{i+4}e_j = -e_ie_j \cdot e_4, & e_{i+4}e_{j+4} = -\gamma e_ie_j; & \end{array} \tag{55}$$

we write $(e_1, e_1) = -\alpha$, $(e_2, e_2) = -\beta$ and $(e_3, e_3) = -\alpha\beta$.

We denote by $M(\alpha, \beta, \gamma)$ any anticommutative algebra with multiplication table (55). It can be defined over a field of arbitrary characteristic and it is a Malcev algebra (i.e., it satisfies the identity (10)) for any $\alpha, \beta, \gamma \in F$. If $\mathrm{char}F \neq 3$ then $M(\alpha, \beta, \gamma)$ is a non-Lie algebra. If $\alpha\beta\gamma \neq 0$ then it is central simple. Hence we have proved the following theorem.

Theorem 3.11. *The class of non-Lie central simple Malcev algebras over an arbitrary field F of characteristic not 2 or 3 coincides with the class $M(\alpha, \beta, \gamma)$ for any $\alpha, \beta, \gamma \neq 0 \in F$.*

If, for example, A is the split simple Malcev algebra with basis h, x, y, z, x', y', z' constructed above, then we can set

$$\begin{array}{llll} e_1 = h, & e_2 = x + x', & e_3 = e_1e_2 = x' - x, & e_4 = y + y', \\ e_5 = e_1e_4 = y' - y, & e_6 = e_2e_4 = z + z', & e_7 = e_3e_4 = z - z'. & \end{array}$$

The parameters α, β and γ take the following values: $\alpha = -1$, $\beta = 1$ and $\gamma = 1$, i.e., $A = M(-1, 1, 1)$.

Isomorphic algebras $M(\alpha, \beta, \gamma)$ may correspond to different values $\alpha, \beta, \gamma \in F$ $(\alpha\beta\gamma \neq 0)$. The solution to the isomorphism problem for $M(\alpha, \beta, \gamma)$ follows from the method of constructing the basis described above and the Witt theorem on extension of partial isometries of bilinear metric spaces.

Theorem 3.12. *Two algebras of type $M(\alpha, \beta, \gamma)$ $(\alpha\beta\gamma \neq 0)$ over the same field F of characteristic not 2 are isomorphic if and only if their corresponding quadratic forms $f(x) = (x, x)$ are equivalent.*

Note that if $x = \sum_i t_ie_i$ $(t_i \in F)$ then

$$(x, x) = -\alpha t_1^2 - \beta t_2^2 - \alpha\beta t_3^2 - \gamma t_4^2 - \alpha\gamma t_5^2 - \beta\gamma t_6^2 - \alpha\beta\gamma t_7^2. \tag{56}$$

To every $M(\alpha,\beta,\gamma)$ over F we can associate $C(\alpha,\beta,\gamma) = F + M(\alpha,\beta,\gamma)$, whose multiplication is given by

$$(\alpha + x)\cdot(\beta + y) = \alpha\beta + \alpha y + \beta x + x \cdot y,$$

for any $\alpha,\beta \in F$ and $x, y \in M(\alpha,\beta,\gamma)$ where $x \cdot y = (x, y) + xy$. If $\alpha\beta\gamma \neq 0$ and char$F \neq 2$ then $C(\alpha,\beta,\gamma)$ is a simple alternative algebra (Cayley-Dickson algebra) which is related to $M(\alpha,\beta,\gamma)$ in the same way as $C^{(-)}/F$ is related to the split Cayley-Dickson algebra $M(-1,1,1)$. Clearly, two algebras $M(\alpha,\beta,\gamma)$ and $M(\alpha',\beta',\gamma')$ are isomorphic if and only if the corresponding alternative algebras $C(\alpha,\beta,\gamma)$ and $C(\alpha',\beta',\gamma')$ are isomorphic.

Let us discuss the question of Cartan subalgebras of a central simple Malcev algebra $A = M(\alpha,\beta,\gamma)$. Let y be an arbitrary nonzero element in A. If $(y, y) \neq 0$ then the subspace $V = (y)^{\perp}$ is invariant with respect to R_y and identity (52) shows that for all $x \in V$ we have

$$xy \cdot y = (y, y)x, \tag{57}$$

that is, R_y restricted to V is non-degenerate, $A_0^y = (y)$ and y is a regular element in the sense of Definition 1.11. If $(y, y) = 0$ then it follows from (52) that $R_y^3 = 0$ and $A_0^y = A$. Therefore, an element $y \in A$ is regular if and only if $(y, y) \neq 0$, and hence any Cartan subalgebra H of A coincides with the intersection of subspaces A_0^y $(y \in H)$; then H contains a regular element y and therefore coincides with the 1-dimensional subalgebra generated by y. Conversely, any regular element in A generates a (1-dimensional) Cartan subalgebra of A, independently of the cardinality of the field F.

It follows from (57) that nonzero characteristic roots of R_y coincide with quadratic roots of (y, y), and that a Cartan subalgebra $H = (y)$ is split if and only if (y, y) is the square of a nonzero element of F. Therefore, the following holds.

Proposition 3.13. *An algebra $M(\alpha,\beta,\gamma)$ is split, thus isomorphic to $M(-1,1,1)$, if and only if the quadratic form* (56) *represents the identity in F.*

Theorem 3.12 shows that the classification of central simple Malcev algebras over F is related to the theory of quadratic forms over F. For example, let F be the field $\mathbb{Q}$ of rational numbers. If not all α,β,γ are positive then (56) is undefined. Since an indefinite (or positive definite) quadratic form of rank $n \geq 4$ over $\mathbb{Q}$ represents 1, the form $-(x, x)$ is also positive definite, and using the above properties of quadratic forms over $\mathbb{Q}$ we have $M(\alpha,\beta,\gamma) \equiv M(1,1,1)$. Therefore, there are only two distinct non-Lie central simple Malcev algebras over $\mathbb{Q}$. The same is true if $F = \mathbb{R}$, the field of the real numbers. If the base field F is the field of p-adic numbers $\mathbb{Q}_p$ then any algebra of the form $M(\alpha,\beta,\gamma)$ over F is split, as in the case of an algebraically closed field, although $\mathbb{Q}_p$ is not algebraically closed.

4. Conjugacy of Cartan subalgebras of Malcev algebras

If A is an arbitrary (nonassociative) algebra over a field of characteristic 0, and D is a nilpotent derivation of A, then $\exp D$ is an automorphism of A. A derivation D is said to be *inner* if it belongs to the algebra A^* of multiplications of A, where A^* is generated by the operators of left and right multiplication. Consider the group Φ of all automorphisms of A generated by all $\exp D$ where D is an inner nilpotent derivation. Elements of Φ will be called *special automorphisms of A*.

4.1. Let F be an algebraically closed field of characteristic 0, let A be a Malcev algebra over F, let H be a Cartan subalgebra of A, and let $\alpha_1, \dots, \alpha_n$ be the nonzero roots of H in A. To each pair of elements $x, y \in A$ we associate the inner derivation $D(x, y) = R_{xy} + [R_x, R_y]$; see equation (13). Let us show that any element $e_\alpha \in A_\alpha$ ($\alpha \neq 0$) and any element $h \in H$ define a nilpotent derivation $D(e_\alpha, h)$. Indeed, if $e_\beta \in A_\beta$ and $\beta \neq k\alpha$ for any integer k, then for every $k > 0$ we have $e_\beta D^h(e_\alpha, h) = 0$ for k sufficiently large. The same is true for $\beta = k\alpha$ for $k \geq 2$. The case $\beta = -\alpha$ is of special interest; then $J(h, e_\alpha, e_{-\alpha}) = 0$. It follows that the elements $h, e_\alpha, e_{-\alpha}$ generate a Lie subalgebra in A. The restriction of $D(e_\alpha, h)$ to this subalgebra coincides with $R_{e'_\alpha}$, where $e'_\alpha = 2e_\alpha h \in A_\alpha$. Thus

$$e_{-\alpha} D^{k+1}(e_\alpha, h) = [(e_{-\alpha} \underbrace{e'_\alpha) \cdots]\, e'_\alpha}_{k+1}. \tag{58}$$

For any $h_1 \in H$ the elements $e_\alpha, e_{-\alpha}, h_1$ form a Lie triple, i.e., $J(e_\alpha, e_{-\alpha}, h_1) = 0$. Therefore, the right side of (58) belongs to $A_{k\alpha}$ for any $k \geq 0$, and since $\alpha \neq 0$ we conclude that $e_{-\alpha} D^h(e_\alpha, h) = 0$ for $k > 0$ sufficiently large. By (29) the remaining cases can be reduced to the cases considered above.

We choose a basis $\{h_1, \dots, h_s, e_{s+1}, \dots, e_m\}$ of A in such a way that the elements $\{h_1, \dots, h_s\}$ form a basis of H and $\{e_{s+1}, \dots, e_m\}$ lie in root spaces A_α, $\alpha \neq 0$. We choose an element $h_0 \in H$ such that $\alpha_i(h_0) \neq 0$ for all $i = 1, \dots, n$. This can be done owing to the linearity of the roots: the product $\alpha_1 \alpha_2 \dots \alpha_n$ is a polynomial function $H \to F$ which is not identically 0. Let $\lambda_1, \dots, \lambda_m$ be independent variables and let

$$x = \lambda_1 h_1 + \cdots + \lambda_s h_s + \lambda_{s+1} e_{s+1} + \cdots + \lambda_m e_m,$$

be an element of A. Then the element

$$xP = \left(\sum_{i=1}^{s} \lambda_i h_i \right) \exp D(\lambda_{s+1} e_{s+1}, h_0) \cdots \exp D(\lambda_m e_m, h_0),$$

defines a polynomial map P of the algebra A into itself (the coordinates of xP are polynomial functions of the coordinates of x). Let us compute the differential

$d_{h_0}P$ of this map at the point h_0. Set

$$x = h + e, \qquad h \in H, \qquad e \in \sum_{\alpha \neq 0} A_\alpha.$$

Then

$$\begin{aligned}(h_0 + tx)P = [(h_0 + th) + te]\, P &\equiv (h_0 + th)\, [1 + tD(e, h_0)] \pmod{t^2} \\ &\equiv h_0 + t\, [h + h_0 D(e, h_0)] \pmod{t^2},\end{aligned}$$

which implies that $d_{h_0}P$ is a map

$$h + e \mapsto h + h_0 D(e, h_0) = h - 2(eh_0)h_0.$$

Since $h \mapsto h$ and $e \mapsto -2(eh_0)h_0$ are non-degenerate, we see that $d_{h_0}P$ is an epimorphism. Arguing in the same way as [3] we can show the following:

Theorem 4.1. *If H_1 and H_2 are Cartan subalgebras of a finite dimensional Malcev algebra A over an algebraically closed field of characteristic 0 then there exists a special automorphism η of A such that $H_1^\eta = H_2$.*

In the proof it is shown that a Zariski open set consisting of regular elements of A is the image of the regular elements from an arbitrary Cartan subalgebra $H \leq A$ with respect to a special automorphism. In particular, all Cartan subalgebras of A have the same dimension and contain regular elements. When extending the base field $F \subset \Omega$, the Fitting 0 component A_0^x of A with respect to R_x for any $x \in A$ becomes the Fitting 0 component $A_0^x \otimes \Omega$ of $A_\Omega = A \otimes \Omega$ with respect to the same operator, and a Cartan subalgebra $H \leq A$ becomes a Cartan subalgebra $H_\omega = H \otimes \Omega$ of A_Ω. Therefore, the following holds:

Corollary 4.2. *If A is a finite dimensional Malcev algebra over an arbitrary field of characteristic 0 then all Cartan subalgebras of A have the same dimension. Moreover, each Cartan subalgebra contains a regular element.*

Proof. We only need to prove the second claim. Let $x = \lambda_1 h_1 + \cdots + \lambda_s h_s$ be an element of a Cartan subalgebra H, and let $f(\lambda, x) = \det(\lambda - R_x)$ be the characteristic polynomial of R_x. If the multiplicity of 0 as eigenvalue of R_x (i.e., the dimension of A_0^x) is greater than $\dim H = s$ for any specialization of $\lambda_1, \ldots, \lambda_s$ in the base field F then $f(\lambda, x)$ has the form

$$f(\lambda, x) = \lambda^m - \tau_1(x)\lambda^{m-1} + \cdots + (-1)^{m-1}\tau_{m-1}(x)\lambda^\ell,$$

where $\ell > s$. However, the same is true for any extension Ω of F; this contradicts the existence of a regular element in $H_\Omega = H \otimes \Omega$ when Ω is algebraically closed. $\square$

5. Representations of semisimple Malcev algebras of characteristic 0

The results of this section are based on the connection between Malcev algebras and Lie triple systems pointed out by Loos [9]. The main result is the theorem about complete reducibility of representations of semisimple Malcev algebras (Theorem 5.5) which is similar to Weyl's theorem for Lie algebras.

5.1. We recall the definition and basic properties of Lie triple systems (LTS) [8, 2]. A vector space T over a field F is called an LTS if a ternary operation $[xyz]$ defined on it is linear in each variable and satisfies the following identities:

$$\begin{aligned}
&[aab] = 0,\\
&[abc] + [bca] + [cab] = 0,\\
&[ab[xyz]] = [[abx]yz] + [x[aby]z] + [xy[abz]].
\end{aligned}$$

The last identity shows that the map $D_{a,b}\colon x \mapsto [abx]$ is a derivation of T. Such derivations are called *inner* and they generate a Lie algebra $D_0(T)$ which is called the *algebra of inner derivations.* Any Lie algebra L with triple product $[xyz] = xy\cdot z$ (or any subspace of L closed under the iterated product) is an example of an LTS. On the other hand, any LTS can be realized as a subspace of a Lie algebra with the iterated product; in this case we say that the LTS is embedded into the Lie algebra. If an LTS T is embedded into a Lie algebra L then the subalgebra of L generated by T is called the *enveloping Lie algebra of the embedding.* For an arbitrary LTS we can define the notions of ideal, solvability, radical, and semisimplicity. If an LTS T is semisimple then its enveloping Lie algebra is also semisimple for any embedding $T \to L$. Among all embeddings of an LTS into a Lie algebra there are two special ones: the standard and the universal. The underlying vector space of the standard enveloping algebra $L_s(T)$ has the form $T + D_0(T)$ and the multiplication in $L_s(T)$ is defined in the obvious way. In particular, if $a, b \in T$ then $ab = D_{a,b}$. The universal Lie enveloping algebra $L_u(T)$ is characterized by the property that any homomorphism $T \to L$, where L is an arbitrary Lie algebra, can be uniquely extended to a homomorphism $L_u(T) \to L$. If an LTS T is semisimple then its standard and universal enveloping algebra coincide.

We now assume that the characteristic of the base field F is 0. If A is a semisimple algebra then T_A is also semisimple[†]; in general, the radical of A coincides with the radical of T_A [9]. The set of inner derivations of T_A is generated by the operators of the form $R(x, y) = 2R_{xy} + [R_x, R_y]$. Identities (15) show that each operator R_x is a derivation of the LTS T_A. Therefore, the Lie enveloping algebra $L(A)$ of the regular representation of A is a subalgebra of the algebra $D(T_A)$ for all derivations of $T(A)$:

$$D_0(T_A) \subseteq L(A) \subseteq D(T_A). \tag{59}$$

[†] Translator's note: T_A is the Lie triple system associated to the Malcev algebra A as in the paper by Loos [9].

Since all derivations of a semisimple LTS are inner [8], for any semisimple Malcev algebra the inclusions in (59) become equalities [9].

Proposition 5.1. *If A is a simple (respectively semisimple) Malcev algebra then the Lie enveloping algebra $L(A)$ of its regular representation is also simple (respectively semisimple).*

Proof. To the decomposition of A into a direct sum of ideals A_i corresponds a decomposition of $L(A)$ into a direct sum of ideals isomorphic to $L(A_i)$. If A_i is a simple Lie algebra then $L(A_i)$ is also a simple Lie algebra isomorphic to A_i. Let A be a simple non-Lie Malcev algebra; we show that $L(A)$ is again a simple Lie algebra. It suffices to consider the case when A is a central simple algebra. Indeed, if A is not central then A can be regarded as a central simple algebra A_Γ over its centroid $\Gamma \supset F$ [3]. Since all operators R_x $(x \in A)$ are Γ-linear and $R_{\gamma a} = \gamma R_a$ for $a \in A$, $\gamma \in \Gamma$, we see that the Lie algebra $L(A)$ can be regarded as an algebra (of smaller dimension) over the field Γ, which, obviously, coincides with $L(A_\Gamma)$. If we prove that $L(A_\Gamma)$ is a central simple algebra (over Γ), it would imply that $L(A)$ is also simple and its centroid is isomorphic to Γ. Using the same arguments we can restrict our attention to the case of an algebraically closed field F. In the case that the algebra has dimension 7 its structure is known (see §3). Inner derivations $D(x,y) = R_{xy} + [R_x, R_y]$ generate a subalgebra L_0 of dimension 14 in $L(A)$ which is a simple Lie algebra of type G_2 [2]. The underlying vector space of $L(A)$ can be decomposed into the sum of the subspaces L_0 and $R(A)$, where $R(A)$ is the subspace generated by the operators R_x; the sum is direct since R_x is a derivation of A if and only if x lies in the Lie center of A, which is 0 in a simple non-Lie Malcev algebra (compare Lemma 3.1). Therefore, $\dim L(A) = 21$. The Killing form on A is non-degenerate and each operator R_x $(x \in A)$ is skew-symmetric with respect to this form. Therefore, $L(A)$ is a subalgebra of a simple Lie algebra of type B_3 (the orthogonal algebra of a 7-dimensional vector space). Comparing the dimensions of $L(A)$ and B_3 we see that $L(A) = B_3$. The proof is complete. □

Corollary 5.2. *If A is a simple (respectively semisimple) Malcev algebra over a field of characteristic 0 then the algebra $D(T_A)$ of derivations of the Lie triple system T_A is also simple (respectively semisimple). In particular, if $A = C^{(-)}/F$ then $D(T_A) = L(A) = B_3$.*

Theorem 5.3. *Let A be a Malcev algebra over a field of characteristic 0, let S be its radical and N its nil-radical. Then every derivation D of A maps S to N.*

Proof. As shown in [9], S coincides with the radical of T_A. However, for any LTS T, the radical of $L_s(T)$ is generated as an ideal by the radical of T; if R is the radical of T then the radical of $L_s(T)$ equals $R + [R,T]$ [8]. In particular, S lies in the radical of $L_s(T_A)$. A derivation D of the algebra A is also a derivation of the LTS T_A, i.e., D can be regarded as an element of the algebra $D(T_A)$. Since $L_s(T_A)$ is an ideal of the Lie algebra $T_A + D(T_A)$, $(S)D$ lies in the nil-radical of $L_s = L_s(T_A)$. In order to distinguish the operators of right multiplication by x $(x \in A)$ in L_s

from the operators R_x in A, we will denote them by $\operatorname{ad} x$. Thus, for any $x \in (S)D$, $\operatorname{ad} x$ is a nilpotent operator. Furthermore, $(\operatorname{ad} x)^2$ leaves the subspace $T_A \subset L_s$ invariant, and since $[[ax]x] = [axx] = 3(ax)x$ for any $a \in A$, $(\operatorname{ad} x)^2$ coincides with $3R_x^2$ in T_A. Therefore, R_x is a nilpotent operator. However, it follows from Theorem 2.7 that the nil-radical of A coincides with the set of all elements from S which are nilpotent with respect to the regular representation. Hence $x \in N$. (We assume that it is known that the radical S is closed under all derivations of A. Any solvable radical of a finite dimensional algebra of characteristic 0 has this property.) □

The following theorem gives important information about the structure of the representations of semisimple Malcev algebras.

Theorem 5.4. *Let A be a semisimple Malcev algebra of characteristic 0, let ρ be a representation of A in a vector space V, and let $L_\rho(A)$ be the enveloping algebra of the representation ρ. Then $L_\rho(A)$ is a semisimple algebra.*

Proof. Let $E = V + A$ be the semidirect extension of A by means of V defined by ρ. If $\tilde\rho$ is the regular representation of A in E, and $\tilde L(A)$ is the enveloping algebra of $\tilde\rho$, then V is invariant under the action of $\tilde L(A)$ ($V \lhd E$); the restriction of ρ to V induces an epimorphism $\pi\colon \tilde L(A) \to L_\rho(A)$. Consider the LTS T_A and T_E; there exists a unique embedding $\iota\colon T_A \to T_E \subset L_s(T_E)$. Since the LTS T_A is semisimple, the standard embedding for T_A coincides with the universal embedding; therefore ι can be extended to a homomorphism $\iota^*\colon L_s(T_A) \to L_s(T_E)$. The operators $\tilde R(x,y) = 2\tilde R_{xy} + [\tilde R_x, \tilde R_y] \in \tilde L(A)$ are the images of the elements $[x,y] = R(x,y) \in D_0(T_A)$ under ι^*. The restriction of ι^* to $D_0(T_A) = D(T_A)$ defines a homomorphism $\iota'\colon D(T_A) \to \tilde L(A)$ and the composition of ι' and π defines a homomorphism from $D(T_A)$ onto the subalgebra $I \subseteq L_\rho(A)$ generated by the operators $\rho(x,y) = 2\rho(xy) + [\rho(x), \rho(y)]$, $x, y \in A$. Identity (15), which is true for arbitrary representations, shows that I is an ideal of $L_\rho(A)$. By Corollary 5.2, $D(T_A)$ is a semisimple algebra, therefore its homomorphic image I is also semisimple. Consider the quotient algebra $\bar L = L_\rho(A)/I$, and denote by $\bar\rho(x)$ the image of $\rho(x) \in L_\rho(A)$ under the canonical homomorphism $L_\rho(A) \to \bar L$. The underlying vector space of $\bar L$ is generated by the elements $\bar\rho(x)$ and they satisfy

$$\text{either}\quad 2\bar\rho(xy) + [\bar\rho(x), \bar\rho(y)] = 0, \quad\text{or}\quad -\frac{1}{2}\bar\rho(xy) = [-\tfrac12\bar\rho(x), -\tfrac12\bar\rho(y)].$$

Then the map $x \mapsto -\frac12\rho(x) \mapsto -\frac12\bar\rho(x)$ is a homomorphism of A onto $\bar L$. Since A is a semisimple algebra, it follows from the structural theorem (§2) that $\bar L$ is semisimple (or trivial). Then $L_\rho(A)$ is also a semisimple Lie algebra because the extension of a semisimple Lie algebra by a semisimple algebra is also semisimple. The proof is complete. □

Since each representation ρ of a semisimple algebra A in a vector space V can be regarded as the natural representation of the Lie algebra $L_\rho(A)$ in the same vector space, the next theorem follows directly from Theorem 5.4.

Theorem 5.5. *Any representation of a semisimple Malcev algebra of characteristic 0 is completely reducible.*

Corollary 5.6. *If the radical of a Malcev algebra A coincides with its center C then $A = A_1 + C$, where A_1 is a semisimple subalgebra which coincides with A^2.*

Proof. It suffices to consider the regular representation of A and note that it induces a completely reducible representation of A/C in A. An invariant subspace A_1 complementary to C is the desired subalgebra (even ideal). □

References

[1] **S. Eilenberg**, *Extensions of general algebras*, Ann. Soc. Polon. Math. **21** (1948), 125 – 134.

[2] **B. Harris**, *Cohomology of Lie triple systems and Lie algebras with involution*, Trans. Amer. Math. Soc. **98** (1961), 148 – 162.

[3] **N. Jacobson**, *Lie Algebras*, Interscience Tracts in Pure and Applied Mathematics, No. 10. Interscience Publishers (a division of John Wiley & Sons), New York-London, 1962.

[4] **E. N. Kuzmin**, *Anticommutative algebras satisfying Engel's condition*, Sibirsk. Mat. Zh. **8** (1967), 1026 – 1034.

[5] **E. N. Kuzmin**, *A locally nilpotent radical of Malcev algebras satisfying the n-th Engel condition*, Dokl. Akad. Nauk SSSR **177** (1967), 508 – 510.

[6] **E. N. Kuzmin**, *Malcev algebras and their representations*, Algebra i Logika **7** (1968), 48 – 69.

[7] **E. N. Kuzmin**, *Malcev Algebras*, Doctor of Science Thesis, Novosibirsk, 1969.

[8] **W. G. Lister**, *A structure theory of Lie triple systems*, Trans. Amer. Math. Soc. **72** (1952), 217 – 242.

[9] **O. Loos**, *Über eine Beziehung zwischen Malcev-Algebren und Lie-Tripelsystemen*, Pacific J. Math. **18** (1966), 553 – 562.

[10] **A. I. Malcev**, *Analytic loops*, Mat. Sb. N. S. **36(78)** (1955), 569 – 576.

[11] **A. A. Sagle**, *Malcev algebras*, Trans. Amer. Math. Soc. **101** (1961), 426–458.

[12] **A. A. Sagle**, *Simple Malcev algebras over fields of characteristic zero*, Pacific J. Math. **12** (1962), 1057 – 1078.

[13] **A. A. Sagle**, *On simple extended Lie algebras over fields of characteristic zero*, Pacific J. Math. **15** (1965), 621 – 648.

[14] **E. L. Stitzinger**, *Supersolvable Malcev algebras*, J. Algebra **103** (1986), 69–79.

[15] **K. Yamaguti**, *On the theory of Malcev algebras*, Kumamoto J. Sci. Ser. A. **6** (1963), 9 – 45.

[16] **K. A. Zhevlakov**, *Nil-radical of a Malcev algebra*, Algebra i Logika Sem. **4** (1965), 67 – 78.

Sobolev Institute of Mathematics
Siberian Branch, Academy of Sciences of the USSR
Novosibirsk, Russia

Editors' Comments on Recent Developments

In this section we briefly summarize research on Malcev algebras since the publication of Kuzmin's paper [6] in 1968 which contained the first statement (in some cases without detailed proofs) of the results in the present English translation.

Kuzmin's papers provide a complete theory for finite-dimensional semisimple Malcev algebras and their finite-dimensional representations over a field $\mathbb{F}$ of characteristic 0; in particular, such representations are completely reducible. With these assumptions, a simple Malcev algebra is either a Lie algebra or a 7-dimensional non-Lie Malcev algebra. Gavrilov [G] has recently given a detailed proof of the classification by Kuzmin [K] of 5-dimensional Malcev algebras.

If we regard a simple Lie algebra L as a Malcev algebra, then Carlsson [C1] showed that every Malcev module for L is a Lie module, with one exception: there is an irreducible 2-dimensional non-Lie Malcev module for $\mathfrak{sl}(2, \mathbb{F})$. The same author gave a different proof [C2] of the Wedderburn decomposition of a Malcev algebra into a semisimple subalgebra and the solvable radical. She also showed [C3] that in every characteristic any finite-dimensional Malcev module over a 7-dimensional central simple non-Lie Malcev algebra is completely reducible.

Elduque [E1] classified the maximal subalgebras of central simple non-Lie Malcev algebras over a field of characteristic not 2. The same author studied [E2] the lattice of subalgebras of a Malcev algebra, and showed that two semisimple Malcev algebras over an algebraically closed field are isomorphic if and only if their lattices are isomorphic. He also extended Carlsson's result on Malcev modules to characteristic not 2 or 3, and obtained a new 4-dimensional irreducible non-Lie Malcev module over a nonsplit simple 3-dimensional Lie algebra. The classification of non-Lie Malcev modules was completed by Elduque and Shestakov [ES] in the more general setting of Malcev superalgebras with no restriction on the dimension of the modules and only the condition that $\frac{1}{6} \in \mathbb{F}$.

In 2004, an important breakthrough was made by Pérez-Izquierdo and Shestakov [PS], who constructed universal nonassociative enveloping algebras for Malcev algebras. For any Malcev algebra M over a field $\mathbb{F}$ of characteristic not 2 or 3, there exists a nonassociative algebra $U(M)$ and an injective map from M to $U(M)$ such that the image of M lies in the generalized alternative nucleus of $U(M)$, and $U(M)$ is universal with respect to such maps. The algebra $U(M)$ has a basis of Poincaré-Birkhoff-Witt type, so $U(M)$ is linearly isomorphic to the polynomial algebra $P(M)$; moreover, $U(M)$ has a natural (nonassociative) Hopf algebra structure, and the image of M can be characterized as the primitive elements of $U(M)$ with respect to the diagonal homomorphism

$\Delta\colon U(M) \to U(M) \otimes U(M)$. The paper [PS] also proved an analogue of the Ado-Iwasawa theorem: every finite-dimensional Malcev algebra is isomorphic to a subalgebra of the generalized alternative nucleus of a finite-dimensional unital nonassociative algebra. Zhelyabin and Shestakov [ZS] established analogues for Malcev algebras of the Chevalley and Kostant theorems on centers of universal enveloping algebras of Lie algebras. The nonassociative bialgebra structure of the enveloping algebras $U(M)$ has been studied by Zhelyabin [Z]; see also [M]. Structure constants for $U(M)$ when $\dim M \leq 5$ have been obtained by various authors; see [B1,B2,TB] and the survey [B3].

The theory of free Malcev algebras has been developed primarily by Filippov, who showed (over a field of characteristic not 2 or 3) that free Malcev algebras have zero-divisors [F1]; that free Malcev algebras with 5 or more generators are not semiprime [F3], have nonzero annihilator, and are not separated [F4]; and that the base rank of the variety of Malcev algebras is infinite [F4]. Shestakov and Kornev [SK] showed that the prime radical of a free Malcev algebra on two or more generators coincides with the set of all its universally Engelian elements.

Simple Malcev superalgebras have been studied by Shestakov [S1], who showed that a prime Malcev superalgebra of characteristic not 2 or 3 with a nontrivial odd part is a Lie superalgebra. The same author in collaboration with Zhukavets has developed the theory of free Malcev superalgebras; see [S3,SZ1,SZ2].

The speciality problem for Malcev algebras asks whether every Malcev algebra is "special"; that is, isomorphic to a subalgebra of the commutator algebra of some alternative algebra. Filippov [F2] proved that over a field containing $\frac{1}{2}$ every semiprime Malcev algebra is special. Sverchkov [Sv] proved that every Malcev algebra in the variety generated by the 7-dimensional simple non-Lie Malcev algebra is special. Recent progress on this problem, and the corresponding problem for Malcev superalgebras, is primarily the work of Shestakov and Zhukavets. There is a close relation between this problem and the deformation theory of algebras [S2]. It has been shown that the free Malcev superalgebra on one odd generator is special [SZ3]; more generally, this holds for any Malcev superalgebra generated by one odd element.

For a generalization of Malcev algebras to the setting of dialgebras; see [B4,Sa].

[B1] M. R. Bremner, I. R. Hentzel, L. A. Peresi, H. Usefi, *Universal enveloping algebras of the four-dimensional Malcev algebra*, Algebras, Representations and Applications, pp. 73 – 89. Contemp. Math., 483, Amer. Math. Soc., Providence, 2009.

[B2] M. R. Bremner, H. Usefi, *Enveloping algebras of the nilpotent Malcev algebra of dimension five*, Algebr. Represent. Theory 13 (2010), 407 – 425.

[B3] M. R. Bremner, I. R. Hentzel, L. A. Peresi, M. Tvalavadze, H. Usefi, *Enveloping algebras of Malcev algebras*, Comment. Math. Univ. Carolin. 51 (2010), 157 – 174.

[B4] M. R. Bremner, L. A. Peresi, J. Sánchez-Ortega, *Malcev dialgebras*, Linear Multilinear Algebra 60 (2012), 1125 – 1141.

[C1] R. Carlsson, *Malcev-Moduln*, J. Reine Angew. Math. 281 (1976), 199 – 210.

[C2] R. Carlsson, *The first Whitehead lemma for Malcev algebras*, Proc. Amer. Math. Soc. 58 (1976), 79 – 84.

[C3] R. Carlsson, *On the exceptional central simple non-Lie Malcev algebras*, Trans. Amer. Math. Soc. 244 (1978), 173 – 184.

[E1] A. Elduquem, *On maximal subalgebras of central simple Malcev algebras*, J. Algebra 103 (1986), 216 – 227.

[E2] A. Elduque, *Lattice isomorphisms of Malcev algebras*, Proc. Roy. Soc. Edinburgh Sect. A 109 (1988), 37 – 50.

[ES] A. Elduque, I. P. Shestakov, *Irreducible non-Lie modules for Malcev superalgebras*, J. Algebra 173 (1995), 622 – 637.

[F1] V. T. Filippov, *Zero-divisors and nil-elements in Malcev algebras*, Algebra i Logika 14 (1975), 204 – 214.

[F2] V. T. Filippov, *On the theory of Malcev algebras*, Algebra i Logika 16 (1977), 101 – 108.

[F3] V. T. Filippov, *Nilpotent ideals in Malcev algebras*, Algebra i Logika 18 (1979), 599 – 613.

[F4] V. T. Filippov, *On the theory of finitely generated Malcev algebras*, Algebra i Logika 19 (1980), 480 – 499.

[G] A. V. Gavrilov, *Malcev extensions*, Southeast Asian Bull. Math. 34 (2010), 417 – 424.

[K] E. N. Kuzmin, *Malcev algebras of dimension five over a field of characteristic zero*, Algebra i Logika 9 (1970), 691 – 700.

[M] S. Madariaga, J. M. Pérez-Izquierdo, *Non-existence of coassociative quantized universal enveloping algebras of the traceless octonions*, Comm. Algebra 40 (2012), 1009 – 1018.

[PS] J. M. Pérez-Izquierdo, I. P. Shestakov, *An envelope for Malcev algebras*, J. Algebra 272 (2004), 379 – 393.

[Sa] J. Sánchez-Ortega, *On the definitions of nucleus for dialgebras*, J. Algebra 392 (2013), 244 – 264.

[S1] I. P. Shestakov, *Simple Malcev superalgebras*, Mat. Sb. 182 (1991), 1357 – 1366.

[S2] I. P. Shestakov, *Speciality problem for Malcev algebras and Poisson Malcev algebras*, Nonassociative Algebra and Its Applications (São Paulo, 1998), 365 – 371. Lecture Notes in Pure and Appl. Math., 211, Dekker, New York, 2000.

[S3] I. P. Shestakov, *Free Malcev superalgebra on one odd generator*, J. Algebra Appl. 2 (2003), 451 – 461.

[SK] I. P. Shestakov, A. I. Kornev, *On the radical of a free Malcev algebra*, Proc. Amer. Math. Soc. 140 (2012), 3049 – 3054.

[SZ1] I. P. Shestakov, N. Zhukavets, *The universal multiplicative envelope of the free Malcev superalgebra on one odd generator*, Comm. Algebra 34 (2006), 1319 – 1344.

[SZ2] I. P. Shestakov, N. Zhukavets, *The Malcev Poisson superalgebra of the free Malcev superalgebra on one odd generator*, J. Algebra Appl. 5 (2006), 521 – 535.

[SZ3] I. P. Shestakov, N. Zhukavets, *Speciality of Malcev superalgebras on one odd generator*, J. Algebra 301 (2006), 587 – 600.

[Sv] S. Sverchkov, *Varieties of special algebras*, Comm. Algebra 16 (1988), 1877 – 1919.

[TB] M. Tvalavadze, M. R. Bremner, *Enveloping algebras of solvable Malcev algebras of dimension five*, Comm. Algebra 39 (2011), 2816 – 2837.

[Z] V. N. Zhelyabin, *Universal envelopes of Malcev algebras: pointed Moufang bialgebras*, Sibirsk. Mat. Zh. 50 (2009), 1285 – 1304.

[ZS] V. N. Zhelyabin, I. P. Shestakov, *Chevalley and Kostant theorems for Malcev algebras*, Algebra Logika 46 (2007), 560 – 584.

Quasigroups and Related Systems **22** (2014), 133 − 140

Group signature protocol based on masking public keys

Nikolay A. Moldovyan and Alexander A. Moldovyan

Abstract. There is proposed and discussed the group signature protocol characterized in using the collective signature scheme and masking the public keys of the signers. The masking is performed depending on parameters computed depending on both the public keys and the hash function from document to be signed.

1. Introduction

Digital signature protocols are widely used in the information technologies to solve a variety of different problems. For practical application there are proposed the following types of the signature protocols: usual (individual) signature [6, 11]; blind signature [3, 4]; aggregate signature [10]; group signature [1]; collective signature [8] et. al. The last three protocols relates to the concept of multisignatures introduced in papers [2, 9]. The multisignature concept was generalized to the threshold group signatures in paper [5] when each t of k signers are able to sign a document. The group signature and the collective signature protocols are different in the following. The group signature to an electronic message is the signature on behalf of some set of of k signers (members of the group) headed by a person called dealer. The group signature is generated by a subset of t ($t \leqslant k$) signers. Any one can verify validity of the group signature. The group signature verification procedure does not provide possibility to open the signature, i.e. to identify the members of the group that created the signature. In the case of disputes the signature can be opened by the dealer (with or without the help of signers). The dealer is a trusted party of the group signature protocol. He creates the secret parameters used by the signers.

The collective signature to a document is the signature on behalf of each of m declared signers. The collective signature means that each of the declared signers has signed the document. The collective signature can be considered as some digest of m individual signatures. No trusted party participates in the collective signature protocol. The secret used by each of the signers is private. It is sup-

2010 Mathematics Subject Classification: 11T71, 94A60, 94A62
Keywords: Cryptographic protocol, public key, digital signature, group signature, collective signature, discrete logarithm problem, one-way function
This work was financially supported by Government of Russian Federation, Grant 074-U01

posed the participants of the collective signature protocol use their private keys corresponding to their public keys used to verify their individual signatures, i.e. the collective signature protocols and individual signature protocols can use the same public key infrastructure. The last represents an important advantage of the collective signatures.

This paper proposes a new design of the group signature protocols based on difficulty of the discrete logarithm problem. Novelty of the design consists in using both the collective signature scheme and the transformation masking the public keys of the signers. The described approach provides possibility to create the group signature protocols that are free from participation of a trusted party and use the standard public key infrastructure, i.e. each of the signers can use the same private key when computing his individual signature and participating in computation of the group signature. Thus, the proposed group signature protocol requires no distribution of the secret keys and uses the standard public key infrastructure. Therefore the set of signers included in the group can be arbitrarily changed by the dealer whose public key is used as public key of the group.

Each group signature contains an additional parameter that can be used only by the dealer to open the signature without help of the signers. Practical application scenario for the proposed protocol is as follows. An official information Bureau with geographically distributed staff is headed by a director (dealer) and issues electronic documents. The documents are signed on behalf of the Bureau. Usually different documents are prepared by different subsets of the employees. Produced documents are signed with collective signature of the respective subsets of the employees and presented to the director. He approves the documents with transforming the collective signatures into the group signatures.

2. The proposed signature protocol

In the proposed protocol there are used the following parameters: 1) sufficiently large prime p (for example, having the size 2500 bits), such that number $p-1$ contains large prime divisor q (for example, having the size 256 bits); 2) number α order of which modulo p is equal to q. Each signer of the group generates his private key as a random number x (for example, having the size 256 bits) and computes his public key $y = \alpha^x \bmod p$. The public key of the dealer $Y = \alpha^X \bmod p$, where X is his private key, represents the public key of the group which is used by verifier while performing the group signature verification procedure.

The group signature generation procedure includes both the mechanism of masking (modifying) the public keys of the signers, which is performed with help of the dealer, and the mechanism of forming the collective signature described in paper [8]. The modified public keys are used in the second mechanism that is performed as follows. It is computed the collective randomization parameter E that is one of elements of the group signature. Depending on the value E each signer computes his share in the collective signature S_c, taking into account his modified public key. The collective signature S_c represents the preliminary value of the group signature element S. The value S_c is used by dealer to produce the final value S.

In the mechanism of masking the public keys there is used the internal public key of the dealer, which represents the pair of numbers (n, e), and is generated, like in the RSA cryptosystem [11], as follows. The dealer generates two strong [7] primes r and w, computes $n = wr$ and $\phi(n) = (w-1)(r-1)$, selects number e that is mutually prime with $\phi(n)$, and calculates his private value $d = e^{-1} \bmod \phi(n)$. The internal public key (n, e) is actual only for the signers of the group headed by the dealer. It is not used in the group signature verification procedure. The generalized scheme of the proposed group signature protocol includes the following steps:

i. Taking into account the document M to be signed the dealer masks the public keys of the assigned signers. To mask the public key y_i of the ith signer the dealer computes the exponent $\lambda_i = (H+y_i)^d \bmod n$, where H is the hash-function value computed from M, and sends the value λ_i to the ith signer.

ii. The assigned subset of signers and leader computes the collective randomization parameter E.

iii. Using the value λ_i each ith signer computes his share in the collective signature and sends it to the dealer.

iv. The dealer verifies the share of all assigned signers and computes his share in the group signature. Then he computes the group signature as triple (U, E, S), where S is sum (modulo q) of all shares; U is the product (modulo p) of the modified public keys of all signers.

The value U contains the information about all signers participating in the given group signature to the document M. In the case of disputes the identification of the signers can be performed by the dealer. Except the dealer opening of the given group signature can be performed only by all signers participating in the signature. If one of them is not agree the group signature be opened the others are not able to open the signature.

One of possible particular implementations of the group signature protocol is described as follows. Suppose there are m signers assigned by dealer to process the document M and to generate the group signature to M. The signature generation procedure includes the following steps:

1. Using some specified 256-bit hash-function F_H the dealer computes the hash value from the document $H = F_H(M)$ and the masking exponents $\lambda_i = (H + y_i)^d \bmod n$ for all public keys $y_i = \alpha^{x_i} \bmod p$, where x_i is private key of the ith signer, and sends the value λ_i to the ith signer $(i = 1, 2, \ldots, m)$. Then dealer computes the first element of the group signature

$$U = \prod_{i=1}^{m} y_i^{\lambda_i} \bmod p.$$

The value U represents the masked collective public key of the assigned subset of signers.

2. Each ith signer ($i = 1, 2, \ldots, m$) computes the hash value $H = F_H(M)$, verifies that equation $\lambda_i^e = y_i + H \bmod n$ holds (it means the value λ_i has been provided by the dealer), generates a random number $k_i < q$, computes the value $R_i = \alpha^{k_i} \bmod p$, and sends R_i to the dealer.

3. Dealer generates the random number $K < n$ and computes values $R' = \alpha^K \bmod p$,

$$R = R' \prod_{i=1}^{m} R_i \bmod p = \alpha^{K + \sum_{i=1}^{m} k_i \bmod q} \bmod p,$$

and $E = F_H(H||R||U)$, where E is the second element of the group signature; $||$ denotes the concatenation operation. Then he sends the value E to each signer.

4. Each ith signer ($i = 1, 2, \ldots, m$) computes his share $S_i = k_i + \lambda_i x_i E \bmod q$ in the third element of the group signature and sends it to the dealer.

5. Dealer computes the collective signature S_c of the assigned set of signers: $S_c = \sum_{i=1}^{m} S_i \bmod q$ and verifies it with formula $R/R' = U^{-E}\alpha^{S_c} \bmod p$. If S_c is valid, he computes his share $S' = K + XE \bmod q$ and the third element of the group signature $S = S' + S_c \bmod q$.

The verification of the group signature (U, E, S) to document M is performed with the public key of the group Y that coincides with the public key of the dealer. The verification procedure includes the following steps:

1. The verifier computes the hash value from the document M: $H = F_H(M)$.

2. Using the group public key Y and signature (U, E, S) he computes the value $R^* = (UY)^{-E}\alpha^S \bmod p$.

3. Then he computes the value $E^* = F_H(H||R^*||U)$ and compares the values E^* and E. If $E^* = E$, then the verifier concludes the group signature is valid.

Correctness proof of the protocol is performed with substitution of the signature (U, E, S) in the signature verification procedure:

$$R^* \equiv (UY)^{-E}\alpha^S \equiv U^{-E}Y^{-E}\alpha^{S' + \sum_{i=1}^{m} S_i} \equiv$$

$$\equiv \left(\prod_{i=1}^{m} \alpha^{\lambda_i x_i}\right)^{-E} \alpha^{-XE}\alpha^{S' + \sum_{i=1}^{m} S_i} \equiv$$

$$\equiv \alpha^{-E\sum_{i=1}^{m} \lambda_i x_i}\alpha^{-XE}\alpha^{K + XE + \sum_{i=1}^{m}(k_i + \lambda_i x_i E)} \equiv$$

$$\equiv \alpha^K \alpha^{\sum_{i=1}^{m} k_i} \equiv \alpha^K \prod_{i=1}^{m} \alpha^{k_i} \equiv R' \prod_{i=1}^{m} R_i \equiv R \bmod p \Rightarrow$$

$$\Rightarrow \quad R^* = R \;\Rightarrow\; F_H(M||R^*||U) = F_H(M||R||U) \Rightarrow\; E^* = E.$$

3. Discussion

The proposed group signature protocol needs no dealer's distributing any secrete values among signers of the group. This is one of the advantages of the new protocol compared with known group signature protocols [5]. Another advantage is using the standard public key infrastructure, i.e. the public keys of the signers and dealer can be used in both the individual signature protocol and the proposed group signature protocol. Since in the protocol there is used no secret sharing, no special communication channels are needed to implement the protocol. Therefore using Internet is sufficient and the staff of the group can include geographically distributed employees. Besides, the staff of the group can be often and easily changed (when it is needed).

Including the value U as one of the elements of the group signature provides possibility of the dealer's opening the signature in the case of disputes. The last can be performed as follows. Using his private value d the dealer computes the values $\lambda_i = (H + y_i)^d \bmod n$ and $U_i = y_i^{\lambda_i} \bmod p$, multiplies the masked public keys U_i of all possible subsets of signers, and finds the subset for which the product of the values U_i is equal to U, i.e. to the masked collective public key. No other person can open the group signature since computing the masked public keys requires using the secret value d. Except the dealer, only joint action of all signers participating in the group signature can open it, this trivial case is not critical for majority of practical applications. One can note that opening the signature by all m signers participating in the group signature is possible due the fact that they can present all masking exponents λ_i used while computing the value U and show the formulas $\lambda_i^e = H + y_i \bmod n$ $(i = 1, 2, \ldots, m)$ holds. If it will be required this attack can be eliminated defining computation of the value U (see step 1 of the described protocol) in accordance with the following formula:

$$U = Y^{\lambda} \prod_{i=1}^{m} y_i^{\lambda_i} \bmod p,$$

where $\lambda = (H + Y)^d \bmod n$. This modification leads to changing the formula for computing the share of dealer in the signature element S (see step 5 of the protocol) as follows:

$$S' = K + (1 + \lambda)XE \bmod q.$$

While proving correctness of the results of the procedure of opening the group signature the dealer presents the values λ_i (and λ in the modified version of the protocol), however this does not compromise his private value d connected with his internal public key acting in frame of the group.

To provide 128-bit security, i.e. security equal to 2^{128} modulo p multiplication operations, the size of the primes p and q should be equal to about 2500 and 256 bits, respectively. This defines the signature size equal approximately to 3012 bits, while using 256-bit hash-function F_H. For practical applications it is desired to have shorter group signatures. We estimate the proposed cryptoscheme implemented with using elliptic curves defined over the finite field $GF(p)$, where p is a 256-bit prime, will provide 128-bit security with the signature size equal to 770 bits and 641 bits (the last figure relates to the case of implementing the protocol on the base of the cryptoschemes providing 128-bit security with 128-bit value E).

In frame of the group it is used local (internal) public key of the dealer, which is denoted as (n, e) and used by signers at step 2 of the protocol. The private key d connected with the public key (n, e) is used by dealer to compute the masking coefficients λ_i (at step 1 of the protocol and while performing procedure of the opening signature). For further investigation it is interesting to simplify the mechanism of masking the public keys of signers in order to eliminate using the internal public key of the dealer. For example, the masking coefficients can be computed as follows $\lambda_i = F_H(H||y_i||\delta)$, where δ is internal secret key of the dealer. This formula provides possibility for dealer to restore the masking coefficients with using the secret value δ and open the signature in the case of disputes.

However this variant of computing the masking coefficients is connected with proposing a new mechanism providing for users possibility to verify the values λ_i at step 2 of the protocol. The dealer can directly sign each value λ_i with his signature using his private key X and, for example, the Schnorr signature algorithm [12]. Using the dealer's public key Y the ith user will be able to verify validity of the dealer's signature to λ_i. Significant disadvantage of this verification mechanism is essential increasing the computational difficulty of the group signature generation procedure. Indeed, the dealer has to generate m additional individual signatures (this requires performing m exponentiation operations modulo p) and each of the m signers participating in the group signature is to perform the Schnorr signature verification procedure (for each signer this requires performing 2 exponentiations modulo p). In total this variant of verifying values λ_i introduces $3m$ additional exponentiations in the group signature generation procedure.

It is more practically to exclude verification of the values λ_i from the step 2 of the proposed protocol and to inset the verifying masking exponents procedure in step 5 that is performed by the dealer. After such modification these two steps acquire the following form:

2. Each ith signer $(i = 1, 2, \ldots, m)$ generates a random number $k_i < q$, computes the value $R_i = \alpha^{k_i} \bmod p$, and sends R_i to the dealer.

5. Dealer verifies correctness of each value S_i $(i = 1, 2, \ldots, m)$ with formula $R_i = y_i^{-\lambda_i E}\alpha^{S_i} \bmod p$. If each value S_i is correct, he computes his share $S' = K + XE \bmod q$ and the third element of the group signature $S = S' + \sum_{i=1}^{m} S_i \bmod q$.

To provide possibility for the dealer to open the group signature in the case of disputes without disclosing his private key in the modified protocol one can use the following formula for computing the masking exponents λ_i:

$$\lambda_i = F_H\left(H||y_i||F_H\left(M||y_i||\delta\right)\right).$$

Indeed, while opening a group signature, the dealer justifies each value λ_i

assigned to the opened group signature presenting the value $\Delta = F_H(M||y_i||\delta)$, from which it is computationally infeasible to compute the secret value δ.

4. Conclusion

The paper proposes a new group signature protocol characterized in dealer's participating in the procedure of the signature generation. The described group signature protocol has the following merits:

- it uses the standard public key infrastructure;
- it is free from sharing any secret values;
- the set of signers can be easily changed.

In the considered implementation of the protocol the group signature size is comparatively large, 3012 bits in the case of 128-bit security. This parameter can be reduced to about 640 bits with using computations on elliptic curves to implement the protocol like the described one, however it is a topic of individual consideration.

References

[1] **A. Boldyreva**, *Efficient threshold signature, multisignature and blind signature schemes based on the gap-Diffie-Hellman group signature scheme*, Lecture Nnotes Comp. Sci. **2567** (2003), 31-46.

[2] **C. Boyd**, *Digital multisignatures*, Proceedings IMA Conference on Cryptography and Coding. Clarendon, Oxford, 1989, 241-246.

[3] **J. L. Camenisch, J. M. Piveteau, M. A. Stadler**, *Blind signatures based on the discrete logarithm problem*, Lecture Notes Comp. Sci. **950** (1995), 428 – 432.

[4] **D. Chaum**, *Blind signatures for untraceable payments*, Advances in Cryptology: Proc. of CRYPTO'82. Plenum Press, 1983, 199 – 203.

[5] **Y. Desmedt and Y. Frankel**, *Threshold cryptosystems*, Lecture Notes Comp. Sci. **435** (1990), 307 – 315.

[6] **T. ElGamal**, *A public key cryptosystem and a signature scheme based on discrete logarithms*, IEEE Trans. Information Theory **IT−31** (1985), 469 – 472.

[7] **J. Gordon**, *Strong primes are easy to find*, Lecture Notes Comp. Sci. **209** (1985), 216 – 223.

[8] **A. A. Moldovyan and N. A. Moldovyan**, *Blind collective signature protocol based on discrete logarithm problem*, Intern. J. Network Security **11** (2010), 106−113.

[9] **T. Okamoto**, *A digital multisignature scheme using bijective public key cryptosystems*, ACM Transactions on Computer Systems **6** (1988), 432 – 441.

[10] **R. Ostrovsky, S. Lu, A. Sahai, H. Shacham, and B. Waters**, *Sequential aggregate signatures and multisignatures without random oracles*, Lecture Notes Comp. Sci. **4004** (2006), 465 – 485.

[11] **R. L. Rivest, A. Shamir and L. Adleman**, *A method for obtaining digital signatures and public-key cryptosystems*, Commun. ACM **21** (1978), 120 – 126.

[12] **C.P. Schnorr**, *Efficient signature generation by smart cards*, Journal of Cryptology **4** (1991), 161 – 174.

Received Febuary 10, 2014

ITMO University,
Kronverksky pr., 10, St. Petersburg 197101, Russia
E-mail: nmold@mail.ru

Quasigroups and Related Systems **22** (2014), 141 − 146

Sequentially dense flatness of semigroup acts

Leila Shahbaz

Abstract. s-dense monomorphisms and injectivity with respect to these monomorphisms were first introduced and studied by Giuli for acts over the monoid $(\mathbb{N}^{\infty}, \min)$. Ebrahimi, Mahmoudi, Moghaddasi, and Shahbaz generalized these notions to acts over a general semigroup. In this paper, we study flatness with respect to the class of s-dense monomorphisms. The theory of flatness properties of acts over monoids has been of major interest over the past some decades, but so far there are not any papers published on this subject that relate specifically to the class of s-dense monomorphisms. We give some sufficient conditions for s-dense flatness of semigroup acts. Also, we characterize a large number of semigroups over which s-dense flatness coincides with flatness. This gives a useful criterion for flatness of acts over such semigroups. In fact it is shown that the study of s-dense flatness is also useful in the study of ordinary flatness of acts.

1. Introduction

One of the very useful notions in many branches of mathematics as well as in computer science is the notion of an action of a semigroup or a monoid on a set. Let S be a semigroup. Recall that a right *S-act* or *S-system* denoted by A_S, is a set A together with a function $\lambda : A \times S \to A$, called the *action* of S (or the S-action) on A, such that for each $a \in A$ and $s, t \in S$ (denoting $\lambda(a, s)$ by as) $a(st) = (as)t$. If S is a monoid with an identity e, we add the condition $xe = x$. Analogously, a left S-act ${}_SA$ is defined.

A morphism $f : A_S \to B_S$ between right S-acts A_S, B_S is called an *S-map* if, for each $a \in A$, $s \in S$, $f(as) = f(a)s$.

Since id_A and the composite of two S-maps are S-maps, we have the category **Act**-S (S-**Act**) of all right (left) S-acts and S-maps between them (for more information about acts see [1] and [7]).

The study of flatness properties of acts over monoids was first considered in the early 1970's by Mati Kilp and Bo Stenström as a way to generalize the notions of flatness of modules to the non-additive setting. Since then many researchers continued working in this subject that all culminated in [7].

The tensor functors are of as great importance in the theory of acts as they are in the theory of modules.

2010 Mathematics Subject Classification: 08A60, 18A20, 20M30, 20M50.
Keywords: s-dense flat, s-dense injective, s-dense monomorphism.

Let $A \in$ **Act**-S, $B \in S$-**Act**, and let υ be the smallest equivalence relation on the set $A \times B$ generated by the pairs $((as, b), (a, sb))$ for $a \in A, b \in B, s \in S$.

Define $A_S \otimes {}_S B := (A \times B)/\upsilon$, and $a \otimes b := [(a, b)]_\upsilon \in A_S \otimes {}_S B$, $a \in A, b \in B$.

In [7] the following results are proved for acts over monoids, but for semigroup acts the proofs are similar.

Proposition 1.1. *Take $B \in S$-**Act** and $A = \coprod_{i \in I} A_i \in$ **Act**-S with the injections $u_i : A_i \to A$ where $A_i, i \in I$, are right S-acts. Then*

$$(\coprod_{i \in I} A_i) \otimes B \cong \coprod_{i \in I}^{\mathbf{Set}} (A_i \otimes B)$$

with the injections $u_i \otimes id_B, i \in I$, where $u_i \otimes id_B(a \otimes b) = u_i(a) \otimes id_B(b)$.

*Analogously, if $B = \coprod_{i \in I} B_i \in S$-**Act** with the injections $u_i : B_i \to B$ where $B_i, i \in I$, are left S-acts and $A \in$ **Act**-S then*

$$A \otimes (\coprod_{i \in I} B_i) \cong \coprod_{i \in I}^{\mathbf{Set}} (A \otimes B_i)$$

with the injections $id_A \otimes u_i, i \in I$. $\square$

Definition 1.2. Let A be a right S-act, ${}_E\mathbf{2} = \{0, 1\}$ the left E-act for $E = \{1\}$ and $\mathbf{2}^A = Hom({}_E A_S, {}_E\mathbf{2})$ the left S-act where for any $\varphi \in \mathbf{2}^A$ and for any $s \in S$ the mapping $s\varphi$ is defined by $(s\varphi)(a) = \varphi(as)$ for any $a \in A$. The left S-act $\mathbf{2}^A$ is called the *character act* of A.

Definition 1.3. For $A \in \mathbf{Act} - \mathbf{S}$ we have that $A \otimes - : \mathbf{S} - \mathbf{Act} \longrightarrow \mathbf{Set}$ given by $M \mapsto A \otimes M$ and $(g : M \to M') \mapsto (id_A \otimes g : A \otimes M \to A \otimes M')$ is a covariant functor.

Theorem 1.4. *Let A be a right S-act. The functor $A \otimes -$ preserves the monomorphism $i : {}_S N \to {}_S M$ if and only if $\mathbf{2}^A$ is injective relative to the monomorphism i.* $\square$

2. s-dense flatness

In this section, we recall the class of s-dense monomorphisms needed to define s-dense flatness and then flatness with respect to this class of monomorphisms is studied. The notion of s-dense monomorphisms was first defined in [6] and [8] for acts over the monoid $(\mathbb{N}^\infty, \min)$, and then generalized and studied in some other papers.

Definition 2.1. A subact A of a left S-act B is said to be *s-dense* in B if $Sb \subseteq A$ for each $b \in B$. An S-map $f : A \to B$ is said to be *s-dense* if $f(A)$ is an s-dense subact of B.

Notice that in the case where S is a monoid, the only s-dense subact of an S-act B is B itself, and the only s-dense monomorphisms are isomorphisms. So, this notion makes more sense for semigroup acts than for monoid acts, or for acts over the semigroup parts of the monoids of the form $T = S^1$, in which an identity is adjoined to the semigroup S.

Definition 2.2. A right S-act A is called *s-dense flat* or *s-flat* if the functor $A \otimes -$ takes s-dense monomorphisms of left S-acts to monomorphisms.

Lemma 2.3. *Let $\{A_i : i \in I\}$ be a family of right S-acts and $A_S = \coprod_{i \in I} A_i$. Then A_S is s-flat if and only if each A_i is s-flat.*

Proof. It is similar to the case of usual flatness. □

Lemma 2.4. *A right S-act A_S is s-flat if the functor $A \otimes -$ takes all s-dense inclusions of left S-acts into inclusions, i.e., if ${}_SN$ is an s-dense subact of ${}_SM$ and elements $a \otimes m$ and $a' \otimes m'$ are equal in $A \otimes M$ then they are equal already in $A \otimes N$.*

Proof. Let $f : {}_SN \to {}_SM$ be an s-dense monomorphism. Assume that $a_1 \otimes n_1$, $a_2 \otimes n_2 \in A \otimes N$ are such that $(id_A \otimes f)(a_1 \otimes n_1) = (id_A \otimes f)(a_2 \otimes n_2)$. Thus $a_1 \otimes f(n_1) = a_2 \otimes f(n_2)$ in $A \otimes M$. It follows by hypothesis that $a_1 \otimes f(n_1) = a_2 \otimes f(n_2)$ already in $A \otimes Imf$. Let $g : Imf \to N$ be an S-map such that $g \circ f = id_N$. Then $a_1 \otimes n_1 = (id_A \otimes gf)(a_1 \otimes n_1) = (id_A \otimes g)((id_A \otimes f)(a_1 \otimes n_1)) = (id_A \otimes g)((id_A \otimes f)(a_2 \otimes n_2)) = (id_A \otimes gf)(a_2 \otimes n_2) = a_2 \otimes n_2$. Thus $id_A \otimes f$ is a monomorphism. Hence A is s-flat. □

Now we show the relation between s-flatness and s-injectivity (injectivity with respect to s-dense monomorphisms).

Theorem 2.5. *Let A be a right S-act. The functor $A \otimes -$ takes the s-dense monomorphism $i : {}_SN \to {}_SM$ to a monomorphism if and only if $\mathbf{2}^A$ is s-injective relative to the s-dense monomorphism i.*

Proof. The proof is similar to the case of usual flatness. □

Recall the following proposition from [9].

Proposition 2.6. *For a semigroup S, the following are equivalent.*

(*i*) *All right* (*left*) *S-acts are s-injective.*

(*ii*) *S has a left* (*right*) *identity element.* □

Recall that a right S-act A is called *principally weakly flat* if the functor $A \otimes -$ preserves all embeddings of principal left ideals into S.

Remark 2.7. Each flat act is s-flat, but the converse is not true in general. For example, let $S = (\mathbb{N}, .)$. Then $A_{\mathbb{N}} = \mathbb{N} \sqcup^{\mathbb{N}\setminus\{1\}} \mathbb{N} = \{(1,x)\}\dot{\cup}\{\mathbb{N} \setminus \{1\}\}\dot{\cup}\{(1,y)\}$ is not principally weakly flat by Example III.14.4 of [7] and so it is not flat. But since S is a monoid, each S-act is s-injective by Proposition 2.6. So, $\mathbf{2}^{A_{\mathbb{N}}}$ is s-injective and hence $A_{\mathbb{N}}$ is s-flat by the above theorem.

Now, we apply the relationship between s-flatness and s-injectivity to obtain sufficient conditions for s-flatness similar to the Baer-Skornjakov criterion for s-injectivity.

First we recall the following theorem from [9].

Theorem 2.8. *For a right S-act A, the following are equivalent.*

(i) *A is s-injective.*

(ii) *For every s-dense monomorphism $h : B \to cS^1$ to a cyclic act and every S-map $f : B \to A$ there exists an S-map $g : cS^1 \to A$ such that $gh = f$.*

(iii) *Every S-map $f : cS \to A$ from a cyclic act can be extended to $\overline{f} : cS^1 \to A$.*

(iv) *Every S-map $f : S \to A$ can be extended to an S-map $\overline{f} : S^1 \to A$.*

(v) *For every s-dense monomorphism $h : B \to B \cup cS^1$ to a singly generated extension of B and every S-map $f : B \to A$ there exists an S-map g from $B \cup cS^1$ to A such that $gh = f$.* □

Proposition 2.9. *Let A be a right S-act. Then the following conditions are equivalent.*

(i) *A is s-flat.*

(ii) *The functor $A \otimes -$ takes all s-dense embeddings of left S-acts into cyclic left S-acts to monomorphisms.*

(iii) *The functor $A \otimes -$ takes an inclusion ${}_S cS \hookrightarrow {}_S cS^1$ to a monomorphism.*

(iv) *The functor $A \otimes -$ takes all s-dense monomorphisms $h : {}_S B \to {}_S(B \cup cS^1)$ into a singly generated extension of ${}_S B$ to monomorphisms.*

(v) *The functor $A \otimes -$ takes an inclusion ${}_S S \to {}_S S^1$ to a monomorphism.*

Proof. $(i) \Rightarrow (ii)$, $(i) \Rightarrow (iii)$, $(i) \Rightarrow (iv)$, $(i) \Rightarrow (v)$ are clear.

$(ii) \Rightarrow (i)$ Let the functor $A \otimes -$ take all s-dense embeddings of left S-acts into cyclic left S-acts to monomorphisms. By Theorem 2.5 we get that ${}_S\mathbf{2}^A$ is s-injective relative to all s-dense embeddings of left S-acts into cyclic left S-acts.

Now by Theorem 2.8, ${}_S\mathbf{2}^A$ is s-injective. Applying once more Theorem 2.5, one gets that A is s-flat.

$(iii) \Rightarrow (i)$ Let the functor $A \otimes -$ take ${}_S cS \hookrightarrow {}_S cS^1$ to a monomorphism. By Theorem 2.5, ${}_S\mathbf{2}^A$ is s-injective relative to ${}_S cS \hookrightarrow {}_S cS^1$ and so by Theorem 2.8, it is s-injective. Applying once more Theorem 2.5, one gets that A is s-flat.

$(iv) \Rightarrow (i)$ Let the functor $A \otimes -$ take all s-dense monomorphisms $h : {}_S B \to {}_S(B \cup cS^1)$ into a singly generated extension of ${}_S B$ to monomorphisms. By Theorem 2.5, ${}_S\mathbf{2}^A$ is s-injective relative to all s-dense monomorphisms $h : {}_S B \to {}_S(B \cup cS^1)$. Thus by Theorem 2.8, ${}_S\mathbf{2}^A$ is s-injective. Applying once more Theorem 2.5, one gets that A is s-flat.

$(v) \Rightarrow (i)$ Let the functor $A \otimes -$ take an inclusion ${}_S S \hookrightarrow {}_S S^1$ to a monomorphism. By Theorem 2.5, ${}_S\mathbf{2}^A$ is s-injective relative to an inclusion ${}_S S \hookrightarrow {}_S S^1$. Thus by Theorem 2.8, ${}_S\mathbf{2}^A$ is s-injective. Applying once more Theorem 2.5, one gets that A is s-flat. □

Now we characterize semigroups over which all S-acts are s-flat.

Definition 2.10. A semigroup S is called *right absolutely s-flat* if all right S-acts are s-flat.

Proposition 2.11. *Let S be a semigroup with a right identity element. Then S is right absolutely s-flat.*

Proof. Since S has a right identity element thus each left S-act is s-injective by Proposition 2.6. Then for every S-act A_S, ${}_S\mathbf{2}^A$ is s-injective. Thus A_S is s-flat by Theorem 2.5. □

Now, we characterize a large number of semigroups over which s-dense flatness coincides with flatness. This gives a useful criterion for flatness of acts over such semigroups.

Theorem 2.12. *If S is a(n)*

(i) *semigroup for which $(Id_r(S), \cap, \cup)$ is a Boolean algebra, or*

(ii) *left (right) zero semigroup, or*

(iii) *cyclic semigroup, or*

(iv) *zero semigroup, or*

(v) *idempotent semigroup each of whose proper right ideals is generated by a central idempotent, or*

(vi) *lattice considered as a semigroup with $\wedge$ as its binary operation each of whose proper right ideals is a complete sublattice, or*

(vii) *finite chain considered as a semigroup, or* (*viii*) *Clifford semigroup each of whose proper non-empty ideals is principal*

then each s-flat S-act is flat.

Proof. Let A be an s-flat right S-act. Then by Theorem 2.5, ${}_S\mathbf{2}^A$ is s-injective. Since by [3] each s-injective act over one of the above semigroups is injective thus ${}_S\mathbf{2}^A$ is injective. Now, by Theorem 1.4, A is flat. $\square$

Theorem 2.13. *Each s-flat projection algebra* (S*-act over the monoid* $(\mathbb{N}^\infty, \min)$) *is flat.*

Proof. The proof is similar to the proof of the above theorem, because every s-injective projection algebra is injective by Theorem 3.19 of [8]. $\square$

References

[1] **M. M. Ebrahimi and M. Mahmoudi**, *The category of M-sets*, Italian J. Pure Appl. Math. **9** (2001), 123 − 132.

[2] **M. M. Ebrahimi and M. Mahmoudi**, *Baer criterion and injectivity of projection algebras*, Semigroup Forum **71** (2005), 332 − 335.

[3] **M. M. Ebrahimi, M. Mahmoudi and Gh. Moghaddasi Angizan**, *On the Baer criterion for acts over semigroups*, Communications in Algebra **35** (2007), 3912 − 3918.

[4] **M. M. Ebrahimi, M. Mahmoudi and Gh. Moghaddasi Angizan**, *Injective hulls of acts over left zero semigroups*, Semigroup Forum **75** (2007), 212 − 220.

[5] **M. M. Ebrahimi, M. Mahmoudi and L. Shahbaz**, *Proper-behaviour of sequential injectivity of acts over semigroups*, Communications in Algebra **37** (2009), 2511 − 2521.

[6] **E. Giuli**, *On m-separated projection spaces*, Applied Categorical Structures, **2** (1994), 91 − 99.

[7] **M. Kilp, U. Knauer and A. Mikhalev**, *Monoids, Acts and Categories*, Walter de Gruyter, Berlin, New York, 2000.

[8] **M. Mahmoudi and M. Mehdi Ebrahimi**, *Purity and equational compactness of projection algebras*, Applied Categorical Structures **9** (2001), 381 − 394.

[9] **M. Mahmoudi and L. Shahbaz**, *Characterizing semigroups by sequentially dense injective acts*, Semigroup Forum **75** (2007), 116 − 128.

[10] **M. Mahmoudi and L. Shahbaz**, *Categorical properties of sequentially dense monomorphisms of semigroup acts*, Taiwanese J. Math. **15** (2011), 543 − 557.

[11] **M. Mahmoudi and L. Shahbaz**, *Sequentially dense essential monomorphisms of acts over semigroups*, Applied Categorical Structures, **18** (2010), 461 − 471.

Received July 10, 2013

Department of Mathematics, University of Maragheh, Maragheh 55181-83111, Iran
E-mails: leilashahbaz@yahoo.com, l_shahbaz@maragheh.ac.ir

Quasigroups and Related Systems **22** (2014), 147 − 158

Pentagonal quasigroups

Stipe Vidak

Abstract. The concept of pentagonal quasigroup is introduced as IM-quasigroup satisfying the additional property of pentagonality. Some basic identities which are valid in a general pentagonal quasigroup are proved. Four different models for pentagonal quasigroups and their mutual relations are studied. Geometric interpretations of some properties and identities are given in the model $C(q)$, where q is a solution of the equation $q^4 - 3q^3 + 4q^2 - 2q + 1 = 0$.

1. Introduction

A quasigroup $(Q, \cdot)$ is called *IM-quasigroup* if it satisfies the identities of *idempotency* and *mediality*:

$$aa = a \tag{1}$$

$$ab \cdot cd = ac \cdot bd. \tag{2}$$

Immediate consequences of these identities are the identities known as *elasticity*, *left distributivity* and *right distributivity*:

$$ab \cdot a = a \cdot ba, \tag{3}$$

$$a \cdot bc = ab \cdot ac, \tag{4}$$

$$ab \cdot c = ac \cdot bc. \tag{5}$$

Adding an additional identity to identities of idempotency and mediality some interesting subclasses of IM-quasigroups can be defined. For example, adding the identity $a(ab \cdot b) = b$ *golden section quasigroup* or *GS-quasigroup* is defined (see [9], [2]). Adding the identity of *semi-symmetricity*, $ab \cdot a = b$, *hexagonal quasigroup* is defined (see [10], [1]).

In this paper we study IM-quasigroups satisfying the identity of *pentagonality*:

$$(ab \cdot a)b \cdot a = b. \tag{6}$$

Such quasigroups are called *pentagonal quasigroups*.

2010 Mathematics Subject Classification: 20N05
Keywords: IM-quasigroup, regular pentagon.

Example 1.1. Let $(F, +, \cdot)$ be a field such that the equation

$$q^4 - 3q^3 + 4q^2 - 2q + 1 = 0 \tag{7}$$

has a solution in F. If q is a solution of (7), we define binary operation $*$ on F by

$$a * b = (1-q)a + qb. \tag{8}$$

Then $(F, *)$ is a pentagonal quasigroup.

Idempoteny follows trivially:

$$a * a = (1-q)a + qa = a.$$

To prove mediality, we write

$$\begin{aligned}(a*b)*(c*d) &= ((1-q)a+qb)*((1-q)c+qd)\\ &= (1-q)((1-q)a+qb)+q((1-q)c+qd)\\ &= (1-q)^2a+q(1-q)b+q(1-q)c+q^2d.\end{aligned}$$

This expression remains unchanged applying $b \leftrightarrow c$ and we conclude that

$$(a*b)*(c*d) = (a*c)*(b*d).$$

Since

$$\begin{aligned}(((a*b)*a)*b)*a &= (1-q)((a*b)*a)b+qa\\ &= (1-q)((1-q)((a*b)*a)+qb)+qa\\ &= (1-q)^2((a*b)*a)+(1-q)qb+qa\\ &= (1-q)^2((1-q)(a*b)+qa)+(1-q)qb+qa\\ &= (1-q)^3(a*b)+(1-q)^2qa+(1-q)qb+qa\\ &= (1-q)^4a+(1-q)^3qb+(1-q)^2qa+(1-q)qb+qa\\ &= (q^4-3q^3+4q^2-2q+1)a+(-q^4+3q^3-4q^2+2q)b,\end{aligned}$$

using (7) we get

$$(((a*b)*a)*b)*a = b,$$

which proves pentagonality.

Example 1.2. We put $F = \mathbb{C}$ in the previous example, and q is a solution of the equation (7). Since we are in the set $\mathbb{C}$, that equation has four complex solutions. These are:

$$\begin{aligned}q_{1,2} &= \frac{1}{4}(3+\sqrt{5} \pm i\sqrt{2(5+\sqrt{5})})i,\\ q_{3,4} &= \frac{1}{4}(3-\sqrt{5} \pm i\sqrt{2(5-\sqrt{5})}).\end{aligned}$$

Now $C(q) = (\mathbb{C}, *)$, where $q \in \{q_1, q_2, q_3, q_4\}$, and $*$ is defined by

$$a * b = (1 - q)a + qb$$

is also a pentagonal quasigroup.

Previous example $C(q)$ motivates the introduction of many geometric concepts in pentagonal quasigroups. We can regard elements of the set $\mathbb{C}$ as points of the Euclidean plane. For any two different points $a, b \in \mathbb{C}$ the equality (8) can be written in the form

$$\frac{a * b - a}{b - a} = \frac{q - 0}{1 - 0}.$$

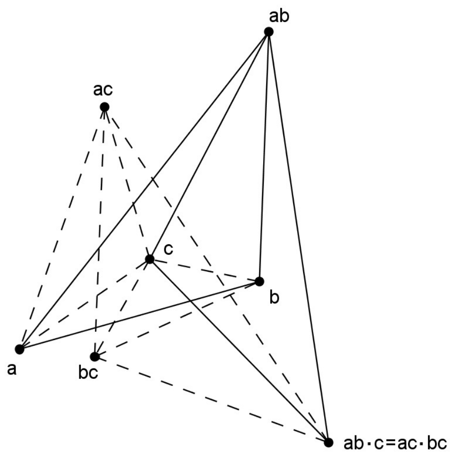


Figure 1. Right distributivity (5) in $C(q_1)$

That means that the points a, b and $a * b$ are vertices of a triangle directly similar to the triangle with vertices 0, 1 and q. In $C(q_1)$ the point $a * b$ is the third vertex of the regular pentagon determined by adjacent vertices a and b. Any identity in the pentagonal quasigroup $C(q) = (\mathbb{C}, *)$ can be interpreted as a theorem of the Euclidean geometry which can be proved directly, but the theory of pentagonal quasigroups gives a better insight into the mutual relations of such theorems. Figure 1 gives an illustration of the right distributivity (5).

In this paper we study different identities in pentagonal quasigroups and their mutual relations. We prove Toyoda-like representation theorem for pentagonal quasigroups, where they are caracterized in terms of Abelian groups with a certain type of automorphism. In the last section, motivated by quasigroups $C(q_i)$, $i = 1, 2, 3, 4$, we study four different models for pentagonal quasigroups.

2. Basic properties and identities

In pentagonal quasigroups, along with pentagonality and the identities which are valid in any IM-quasigroup, some other very useful identities hold.

Theorem 2.1. *In the IM-quasigroup* $(Q,\cdot)$ *identity* (6) *and the identities*

$$(ab\cdot a)c\cdot a=bc\cdot b, \tag{9}$$

$$(ab\cdot a)a\cdot a=ba\cdot b, \tag{10}$$

$$ab\cdot(ba\cdot a)a=b \tag{11}$$

are mutually equivalent and they imply the identity

$$a(b\cdot(ba\cdot a)a)\cdot a=b \tag{12}$$

for every a, b, $c\in Q$.

Proof. First, we prove (6) $\Leftrightarrow$ (9). We have

$$\begin{aligned}bc\cdot b&\overset{(6)}{=}bc\cdot((ab\cdot a)b\cdot a)\overset{(2)}{=}(b\cdot(ab\cdot a)b)\cdot ca\overset{(3)}{=}(b(ab\cdot a)\cdot b)\cdot ca\\&\overset{(2)}{=}(b(ab\cdot a)\cdot c)\cdot ba\overset{(5)}{=}(bc\cdot(ab\cdot a)c)\cdot ba\overset{(2)}{=}(bc\cdot b)\cdot((ab\cdot a)c\cdot a)\end{aligned}$$

Since we have $bc\cdot b\overset{(1)}{=}(bc\cdot b)\cdot(bc\cdot b)$ and

$$(bc\cdot b)\cdot((ab\cdot a)c\cdot a)=(bc\cdot b)\cdot(bc\cdot b),$$

using cancellation in the quasigroup we get $(ab\cdot a)c\cdot a=bc\cdot b$.

Then, we prove (6) $\Leftrightarrow$ (10). We have

$$\begin{aligned}ba\cdot b&\overset{(6)}{=}ba\cdot((ab\cdot a)b\cdot a)\overset{(2)}{=}(b\cdot(ab\cdot a)b)\cdot aa\overset{(3)}{=}(b(ab\cdot a)\cdot b)\cdot aa\\&\overset{(2)}{=}(b(ab\cdot a)\cdot a)\cdot ba\overset{(5)}{=}(ba\cdot(ab\cdot a)a)\cdot ba\overset{(2)}{=}(ba\cdot b)\cdot((ab\cdot a)a\cdot a)\end{aligned}$$

Since we have $ba\cdot b\overset{(1)}{=}(ba\cdot b)\cdot(ba\cdot b)$ and

$$(ba\cdot b)\cdot((ab\cdot a)a\cdot a)=(ba\cdot b)\cdot(ba\cdot b),$$

cancellation again gives $(ab\cdot a)a\cdot a=ba\cdot b$.

Next, we prove (6) $\Leftrightarrow$ (11):

$$ab\cdot(ba\cdot a)a\overset{(2)}{=}a(ba\cdot a)\cdot ba\overset{(3)}{=}(ab\cdot a)a\cdot ba\overset{(5)}{=}(ab\cdot a)b\cdot a.$$

It remains to prove (6), (10) $\Rightarrow$ (12). We get successively:

$$a(b\cdot(ba\cdot a)a)\cdot a \overset{(4)}{=} (ab\cdot(a\cdot(ba\cdot a)a))a \overset{(3)}{=} (ab\cdot((ab\cdot a)a\cdot a))a$$
$$\overset{(10)}{=} (ab\cdot(ba\cdot b))a \overset{(5)}{=} (a\cdot ba)b\cdot a \overset{(3)}{=} (ab\cdot a)b\cdot a \overset{(6)}{=} b. \qquad \square$$

The identity (9) generalises identity (6), so it is called *generalised pentagonality.*

In a pentagonal quasigroup $(Q,\cdot)$ it is often very useful to know how to "solve the equations" of the types $ax = b$ and $ya = b$ for given a, $b \in Q$. The next theorem follows immediately from the identities (12) and (6).

Theorem 2.2. *In the pentagonal quasigroup $(Q,\cdot)$ for a, $b \in Q$ the following implications hold:*

$$ax = b \quad \Rightarrow \quad x = (b\cdot(ba\cdot a)a)a,$$
$$ya = b \quad \Rightarrow \quad y = (ab\cdot a)b. \qquad \square$$

3. Representation theorem

A more general example of the pentagonal quasigroup $C(q)$, where q is a solution of the equation (7) can be obtained by taking an Abelian group $(Q,+)$ with an automorphism φ which satisfies

$$\varphi^4 - 3\varphi^3 + 4\varphi^2 - 2\varphi + \mathbf{1} = 0. \tag{13}$$

The equation $ax = b$ is equivalent with

$$a + \varphi(x-a) = b,$$
$$\varphi(x) = \varphi(a) + b - a,$$
$$x = a + \varphi^{-1}(b-a),$$

which means that $ax = b$ has the unique solution.
The equation $ya = b$ is equivalent with

$$y + \varphi(a-y) = b,$$
$$y - \varphi(y) = b - \varphi(a).$$

Let us check that $y_0 = a + 2\varphi(b-a) - 2\varphi^2(b-a) + \varphi^3(b-a)$ satisfies the last equality:

$$\begin{aligned}
&y_0 - \varphi(y_0) = \\
&\quad = a + 2\varphi(b) - 2\varphi(a) - 2\varphi^2(b) + 2\varphi^2(a) + \varphi^3(b) - \varphi^3(a) \\
&\quad -\varphi(a) - 2\varphi^2(b) + 2\varphi^2(a) + 2\varphi^3(b) - 2\varphi^3(a) - \varphi^4(b) + \varphi^4(a) \\
&\quad = (a - 3\varphi(a) + 4\varphi^2(a) - 3\varphi^3(a) + \varphi^4(a)) + (2\varphi(b) - 4\varphi^2(b) + 3\varphi^3(b) - \varphi^4(b)) \\
&\quad \overset{(1)}{=} -\varphi(a) + b = b - \varphi(a).
\end{aligned}$$

Now let us assume that there exist $y_1, y_2 \in Q$ such that $y_1 a = b$ and $y_2 a = b$. That means that we have

$$\begin{aligned} y_1 a &= y_2 a \\ y_1 + \varphi(y_1) - \varphi(a) &= y_2 + \varphi(y_2) - \varphi(a) \\ (\mathbf{1} + \varphi)(y_1) &= (\mathbf{1} + \varphi)(y_2). \end{aligned}$$

Applying automorphism φ and multiplying by constants we get

$$\begin{aligned} (\mathbf{1} + \varphi)(y_1) &= (\mathbf{1} + \varphi)(y_2) \\ -3(\varphi + \varphi^2)(y_1) &= -3(\varphi + \varphi^2)(y_2) \\ 7(\varphi^2 + \varphi^3)(y_1) &= 7(\varphi^2 + \varphi^3)(y_2) \\ -10(\varphi^3 + \varphi^4)(y_1) &= -10(\varphi^3 + \varphi^4)(y_2) \\ 11(\varphi^4 + \varphi^5)(y_1) &= 11(\varphi^4 + \varphi^5)(y_2). \end{aligned}$$

Adding up all these equalities we get

$$(\mathbf{1} - 2\varphi + 4\varphi^2 - 3\varphi^3 + \varphi^4 + 11\varphi^5)(y_1) = (\mathbf{1} - 2\varphi + 4\varphi^2 - 3\varphi^3 + \varphi^4 + 11\varphi^5)(y_2),$$

from which using (13) and dividing by 11 we get $\varphi^5(y_1) = \varphi^5(y_2)$. Since φ is an automorphism, so is φ^5, and we can conclude $y_1 = y_2$. That shows that the equation $ya = b$ has the unique solution. Hence, $(Q, \cdot)$ is a quasigroup.

Since $a \cdot a = a + \varphi(0) = a$, idempotency is valid. Moreover,

$$\begin{aligned} ab \cdot cd &= (a + \varphi(b - a)) \cdot (c + \varphi(d - c)) \\ &= a + \varphi(b - a) + \varphi(c + \varphi(d - c) - (a + \varphi(b - a))) \\ &= a + \varphi(b - a + c - a) + \varphi(\varphi(d - c - b + a)) \end{aligned}$$

Interchanging b and c that expression remains unchanged, which gives mediality.

If we put $a \cdot b = a + \varphi(b - a)$, we get successively:

$$\begin{aligned} ab \cdot a &= a + \varphi(b - a) + \varphi(a - a - \varphi(b - a)) \\ &= a + \varphi(b - a) - \varphi^2(b - a), \end{aligned}$$

$$\begin{aligned} (ab \cdot a)b &= a + \varphi(b - a) - \varphi^2(b - a) + \varphi(b - a - \varphi(b - a) + \varphi^2(b - a)) \\ &= a + \varphi(b - a) - \varphi^2(b - a) + \varphi(b - a) - \varphi^2(b - a) + \varphi^3(b - a) \\ &= a + 2\varphi(b - a) - 2\varphi^2(b - a) + \varphi^3(b - a), \end{aligned}$$

$$\begin{aligned} (ab \cdot a)b \cdot a &= a + 2\varphi(b - a) - 2\varphi^2(b - a) + \varphi^3(b - a) \\ &\quad + \varphi(a - a - 2\varphi(b - a) + 2\varphi^2(b - a) - \varphi^3(b - a)) \\ &= a + 2\varphi(b - a) - 2\varphi^2(b - a) + \varphi^3(b - a) - 2\varphi^2(b - a) \\ &\quad + 2\varphi^3(b - a) - \varphi^4(b - a) \\ &= a + 2\varphi(b - a) - 4\varphi^2(b - a) + 3\varphi^3(b - a) - \varphi^4(b - a) \overset{(13)}{=} b. \end{aligned}$$

That proves pentagonality in $(Q, \cdot)$.

Based on Toyoda's representation theorem [4], next theorem shows that this is in fact the most general example of pentagonal quasigroups.

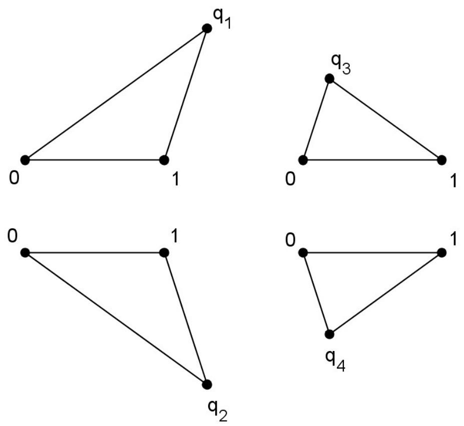


Figure 2. Four characteristic triangles for pentagonal quasigroups

Theorem 3.1. *For every pentagonal quasigroup* $(Q, \cdot)$ *there is an Abelian group* $(Q, +)$ *with an automorphism* φ *such that* (13) *and* $a \cdot b = a + \varphi(b - a)$ *for all* $a,\, b \in Q$.

Proof. Since $(Q, \cdot)$ is a pentagonal quasigroup, it is also an IM-quasigroup. According to the version of Toyoda's theorem for IM-quasigroups, there is an Abelian group $(Q, +)$ with an automorphism φ such that $a \cdot b = a + \varphi(b - a)$ for all $a,\, b \in Q$. The identity of pentagonality (6) is equivalent to (13), which is proved by computation done prior to this theorem. □

4. Four models for pentagonal quasigroups

Depending on the choice of $q \in \{q_1, q_2, q_3, q_4\}$ and if we regard complex numbers as points of the Euclidean plane, we can get four different *characteristic triangles* in $C(q)$ with vertices 0, 1 and q_i, $i = 1, 2, 3, 4$, see Figure 2. Each of the $C(q_i)$, $i = 1, 2, 3, 4$, gives one model for pentagonal quasigroups.

Points q_1 and q_2 are the third vertices of two regular pentagons determined by its two adjacent vertices 0 and 1, while q_3 and q_4 are intersection points of two diagonals of the same two pentagons.

Let us observe a pentagonal quasigroup $(Q, \cdot)$ in the model $C(q_1)$. In the Figure 3 we can spot characteristic triangles from the models $C(q_2)$, $C(q_3)$ and $C(q_4)$.

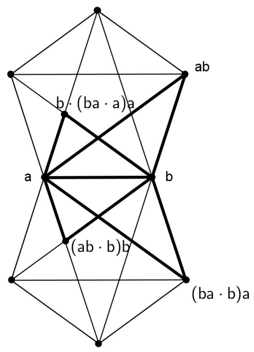


Figure 3. Models for pentagonal quasigroups

Characteristic triangle of the model $C(q_2)$ has vertices a, b and $(ba \cdot b)a$. We will denote

$$a \circ b = (ba \cdot b)a.$$

Characteristic triangle of the model $C(q_3)$ has vertices a, b and $b \cdot (ba \cdot a)a$. We will denote

$$a * b = b \cdot (ba \cdot a)a.$$

Characteristic triangle of the model $C(q_4)$ has vertices a, b and $(ab \cdot b)b$. We will denote

$$a \diamond b = (ab \cdot b)b.$$

The main goal of this section is to prove that $(Q, \circ)$, $(Q, *)$ i $(Q, \diamond)$ are also pentagonal quasigroups. It will be enough to prove that if $(Q, \cdot)$ is a pentagonal quasigroup, then so is $(Q, *)$, because we will show

$$b * (((b * a) * a) * a) = (ba \cdot b)a = a \circ b,$$

$$b \circ (((b \circ a) \circ a) \circ a) = (ab \cdot b)b = a \diamond b.$$

$$b \diamond (((b \diamond a) \diamond a) \diamond a) = ab.$$

In a quasigroup $(Q, \cdot)$ operations of left and right division are defined by

$$a \backslash c = b \Leftrightarrow ab = c \Leftrightarrow c/b = a.$$

Formula is an expression built up from variables using the operations $\cdot$, $\backslash$ and $/$. More precisely:

(1) elements of the set Q (variables) are formulae;

(2) if φ and ψ are formulae, then so are $\varphi \cdot \psi$, $\varphi \backslash \psi$ and φ / ψ.

A formula φ containing at most two variables gives rise to a new binary operation $Q \times Q \to Q$, which will also be denoted by φ.

In [3] the next corollary was proved. We will use it in the proof of the next theorem.

Corollary 4.1. *If $(Q,\cdot)$ is a medial quasigroup, then binary operation defined by the formula φ is also medial.* $\square$

Theorem 4.2. *Let $(Q,\cdot)$ be a pentagonal quasigroup and let $*\colon Q\times Q\to Q$ be a binary operation defined by*

$$a*b = b\cdot(ba\cdot a)a.$$

Then $(Q,*)$ is a pentagonal quasigroup.

Proof. First we prove that $(Q,*)$ is a quasigroup, i.e., that for given a, $b\in Q$ there exist unique x, $y\in Q$ such that $a*x=b$ and $y*a=b$. If we put $x=ab\cdot a$, we get

$$\begin{aligned} a*x &= x\cdot(xa\cdot a)a = (ab\cdot a)\cdot((ab\cdot a)a\cdot a)a \overset{(10)}{=} (ab\cdot a)\cdot(ba\cdot b)a \\ &\overset{(5)}{=} (ab\cdot(ba\cdot b))a \overset{(5)}{=} (a\cdot ba)b\cdot a \overset{(3)}{=} (ab\cdot a)b\cdot a \overset{(6)}{=} b. \end{aligned}$$

Let us now assume that there exist x_1, $x_2\in Q$ such that $a*x_1=a*x_2$. That means that we have

$$x_1\cdot(x_1a\cdot a)a = x_2\cdot(x_2a\cdot a)a.$$

Multiplying by a from the left and applying (4) we get

$$ax_1\cdot(a\cdot(x_1a\cdot a)a) = ax_2\cdot(a\cdot(x_2a\cdot a)a).$$

Now using (3) and (10) we get

$$ax_1\cdot(x_1a\cdot x_1) = ax_2\cdot(x_2a\cdot x_2).$$

After applying (5) and (3) the equality becomes

$$(ax_1\cdot a)x_1 = (ax_2\cdot a)x_2,$$

so multiplying from the right by a and using (6), we finally get $x_1=x_2$.
If we now put $y=(ba\cdot a)a$, we get

$$\begin{aligned} y*a &= a\cdot(ay\cdot y)y = a(((a\cdot(ba\cdot a)a)\cdot(ba\cdot a)a)\cdot(ba\cdot a)a) \\ &\overset{(3),(10)}{=} a(((ba\cdot b)\cdot(ba\cdot a)a)\cdot(ba\cdot a)a) \\ &\overset{(2)}{=} a(((ba\cdot(ba\cdot a))\cdot ba)\cdot(ba\cdot a)a) \overset{(5)}{=} a(((b\cdot ba)a\cdot ba)\cdot(ba\cdot a)a) \\ &\overset{(5)}{=} a(((b\cdot ba)b\cdot a)\cdot(ba\cdot a)a) \overset{(5)}{=} a\cdot((b\cdot ba)b\cdot(ba\cdot a))a \\ &\overset{(2)}{=} a\cdot(((b\cdot ba)\cdot ba)\cdot ba)a \overset{(4)}{=} a\cdot(b(ba\cdot a)\cdot ba)a \overset{(4),(3)}{=} a(b\cdot(ba\cdot a)a)\cdot a \\ &\overset{(4),(3),(10)}{=} (ab\cdot(ba\cdot b))a \overset{(5)}{=} (a\cdot ba)b\cdot a \overset{(3)}{=} (ab\cdot a)b\cdot a \overset{(6)}{=} b. \end{aligned}$$

Let us now assume that there exist y_1, $y_2\in Q$ such that $y_1*a=y_2*a$. We get

$$a\cdot(ay_1\cdot y_1)y_1 = a\cdot(ay_2\cdot y_2)y_2.$$

Using cancellation we get

$$(ay_1 \cdot y_1)y_1 = (ay_2 \cdot y_2)y_2.$$

Multiplying by $y_1 a$ from the left and using (11) we get

$$a = y_1 a \cdot (ay_2 \cdot y_2)y_2.$$

Applying (11) once again gives

$$y_2 a \cdot (ay_2 \cdot y_2)y_2 = y_1 a \cdot (ay_2 \cdot y_2)y_2,$$

wherefrom cancelling first with $(ay_2 \cdot y_2)y_2$ and then with a, we finally get $y_2 = y_1$.
Idempotency of $*$ follows immediately from idempotency of $\cdot$.
Mediality of $*$ follows from Corollary 4.1 by putting $\varphi = *$.
Let us now prove $(a * b) * a = (a \cdot (ab \cdot b)b)b$.

$$\begin{aligned}
(a * b) * a &= a \cdot (a(a * b) \cdot (a * b))(a * b) \\
&= a \cdot (a(b \cdot (ba \cdot a)a) \cdot (b \cdot (ba \cdot a)a))(b \cdot (ba \cdot a)a) \\
&\overset{(4),(3),(10)}{=} a \cdot ((ab \cdot (ba \cdot b)) \cdot (b \cdot (ba \cdot a)a))(b \cdot (ba \cdot a)a) \\
&\overset{(4),(3)}{=} a \cdot ((ab \cdot a)b \cdot (b \cdot (ba \cdot a)a))(b \cdot (ba \cdot a)a) \\
&\overset{(4),(3),(10)}{=} (a \cdot (ab \cdot a)b)(ab \cdot (ba \cdot b)) \cdot (ab \cdot (ba \cdot b)) \\
&\overset{(4),(3)}{=} ((a \cdot (ab \cdot a)b) \cdot (ab \cdot a)b) \cdot (ab \cdot a)b \\
&\overset{(2)}{=} ((a \cdot (ab \cdot a)b) \cdot (ab \cdot a))((ab \cdot a)b \cdot b) \\
&\overset{(2),(6)}{=} (a \cdot ab)b \cdot ((ab \cdot a)b \cdot b) \\
&\overset{(5)}{=} ((a \cdot ab) \cdot (ab \cdot a)b)b \overset{(2)}{=} (a(ab \cdot a) \cdot (ab \cdot b))b \\
&\overset{(3)}{=} ((a \cdot ab)a \cdot (ab \cdot b))b \overset{(2)}{=} (((a \cdot ab) \cdot ab) \cdot ab)b \\
&\overset{(4)}{=} (a(ab \cdot b) \cdot ab)b \overset{(4)}{=} (a \cdot (ab \cdot b)b)b
\end{aligned}$$

Now we prove $((a * b) * a) * b = (ba \cdot a)a$. Let us denote $c = (a * b) * a$. We have

$$\begin{aligned}
((a * b) * a) * b &= b \cdot (bc \cdot c)c \\
&= b(((b \cdot (a \cdot (ab \cdot b)b)b) \cdot (a \cdot (ab \cdot b)b)b) \cdot (a \cdot (ab \cdot b)b)b) \\
&\overset{(3)}{=} b(((b(a \cdot (ab \cdot b)b) \cdot b) \cdot (a \cdot (ab \cdot b)b)b) \cdot (a \cdot (ab \cdot b)b)b) \\
&\overset{(4)}{=} b((((ba \cdot (b \cdot (ab \cdot b)b)) \cdot b) \cdot (a \cdot (ab \cdot b)b)b) \cdot (a \cdot (ab \cdot b)b)b) \\
&\overset{(4),(11)}{=} b((((ba \cdot b)a \cdot b) \cdot (a \cdot (ab \cdot b)b)b) \cdot (a \cdot (ab \cdot b)b)b)
\end{aligned}$$

$$\stackrel{(6)}{=} b((a \cdot (a \cdot (ab \cdot b)b)b) \cdot (a \cdot (ab \cdot b)b)b)$$
$$\stackrel{(4),(1)}{=} (ba \cdot (ba \cdot (b \cdot (ab \cdot b)b))b) \cdot (ba \cdot (b \cdot (ab \cdot b)b))b$$
$$\stackrel{(4),(11)}{=} (ba \cdot ((ba \cdot b)a \cdot b))((ba \cdot b)a \cdot b) \stackrel{(6)}{=} (ba \cdot a)a.$$

Finally, we prove $(((a * b) * a) * b) * a = b$. If we put $d = ((a * b) * a) * b$, we have

$$\begin{aligned}
(((a * b) * a) * b) * a &= a \cdot (ad \cdot d)d \\
&= a(((a \cdot (ba \cdot a)a) \cdot (ba \cdot a)a) \cdot (ba \cdot a)a) \\
&\stackrel{(3)}{=} a((((ab \cdot a)a \cdot a) \cdot (ba \cdot a)a) \cdot (ba \cdot a)a) \\
&\stackrel{(10)}{=} a(((ba \cdot b) \cdot (ba \cdot a)a) \cdot (ba \cdot a)a) \\
&\stackrel{(3)}{=} a(((b \cdot ab) \cdot (ba \cdot a)a) \cdot (ba \cdot a)a) \\
&\stackrel{(5),(11)}{=} a((b \cdot (ba \cdot a)a)b \cdot (ba \cdot a)a) \\
&\stackrel{(4)}{=} ((ab \cdot (a \cdot (ba \cdot a)a)) \cdot ab)(a \cdot (ba \cdot a)a) \\
&\stackrel{(4),(11),(3)}{=} ((ab \cdot a)b \cdot ab)((ab \cdot a)a \cdot a) \\
&\stackrel{(5)}{=} ((ab \cdot a)a \cdot b)((ab \cdot a)a \cdot a) \\
&\stackrel{(4)}{=} (ab \cdot a)a \cdot ba \stackrel{(5)}{=} (ab \cdot a)b \cdot a \stackrel{(6)}{=} b. \qquad \square
\end{aligned}$$

In the end we state three more theorems which express multiplications in quasigroups $(Q, *)$, $(Q, \circ)$ and $(Q, \diamond)$ in terms of multiplication in quasigroup $(Q, \cdot)$. First statements in these theorems follow immediately from Theorem 4.2. Second statements can be proved by rather tedious calculations similar to those in the proof of Theorem 4.2 or using some automated theorem prover. We omit these proofs in this paper.

Theorem 4.3. *Let $(Q, *)$ be a pentagonal quasigroup and let $\circ\colon Q \times Q \to Q$ be a binary operation defined by*

$$a \circ b = b * (((b * a) * a) * a).$$

Then $(Q, \circ)$ is a pentagonal quasigroup. Furthermore

$$a \circ b = (ba \cdot b)a. \qquad \square$$

Theorem 4.4. *Let $(Q, \circ)$ be a pentagonal quasigroup and let $\diamond\colon Q \times Q \to Q$ be a binary operation defined by*

$$a \diamond b = b \circ (((b \circ a) \circ a) \circ a).$$

Then $(Q, \diamond)$ *is a pentagonal quasigroup. Furthermore*

$$a \diamond b = (ab \cdot b)b. \qquad \square$$

Theorem 4.5. *Let* $(Q, \diamond)$ *be a pentagonal quasigroup and let* $\odot\colon Q \times Q \to Q$ *be a binary operation defined by*

$$a \odot b = b \diamond (((b \diamond a) \diamond a) \diamond a).$$

Then $(Q, \odot)$ *is a pentagonal quasigroup. Furthermore*

$$a \odot b = ab. \qquad \square$$

References

[1] **M. Bombardelli and V. Volenec**, *Vectors and transfers in hexagonal quasigroup*, Glasnik Matematički **42 (62)** (2007), 363 – 373.

[2] **Z. Kolar-Begović and V. Volenec**, *Affine regular pentagons in GS-quasigroups*, Quasigroups Related Systems **12** (2004), 103 – 112.

[3] **V. Krčadinac and V. Volenec**, *A note on medial quasigroups*, Math. Commun. **11** (2006), 83 – 85.

[4] **K. Toyoda**, *On axioms of linear functions*, Proc. Imp. Acad. Tokyo **17** (1941), 221 – 227.

[5] **V. Volenec**, *Admissible identities in complex IM-quasigroups I*, Rad JAZU [413] **4** (1985), 61 – 85.

[6] **V. Volenec**, *Admissible identities in complex IM-quasigroups II*, Rad JAZU [421] **5** (1986), 45 – 78.

[7] **V. Volenec**, *Geometry of medial quasigroups*, Rad JAZU [421] **5** (1986), 79 – 91.

[8] **V. Volenec**, *Geometry of IM-quasigroups*, Rad HAZU [456] **10** (1991), 139 – 146.

[9] **V. Volenec**, *GS-quasigroups*, Čas. Pěst. Mat. **115** (1990), 307 – 318.

[10] **V. Volenec**, *Hexagonal quasigroups*, Archivum Mathematicum (Brno) **27a** (1991), 113 – 122.

Received August 20, 2013

Department of Mathematics
University of Zagreb
Bijenička 30
HR-10000 Zagreb
Croatia
Email: svidak@math.hr