INSTITUT ZA MATEMATIKU

NOVI SAD

PROCEEDINGS
of
THE THIRD ALGEBRAIC CONFERENCE
BEOGRAD 1982

1983.

PROCEEDINGS
OF
THE THIRD ALGEBRAIC CONFERENCE

INSTITUT ZA MATEMATIKU
21000 Novi Sad
Jugoslavija

Štampa: FTN OOUR Štamparija za grafičku delatnost
Novi Sad, V.Vlahovića 3
Tiraž: 4oo primeraka

P R E F A C E

The Third Yugoslav Algebraic Conference took place in Belgrade, December 3-4, 1982, and was organized by the Mathematical Institute and the Faculty of Sciences, Belgrade.

This book contains all the papers reported during the Conference. Most of the papers deal with problems on special kinds of algebras.

The next Conference will be organized by the Faculty of Sciences, Zagreb, in 1984.

Belgrade
May 1983

Editors

C O N T E N T S

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

ON THE POSITIONAL PARTITIONS OF ATOMS OF SIMPLE MATROIDS

Dragan M. Acketa

Abstract. We introduce several equivalence relations, which can be used for producing all non-isomorphic non-simple matroids with the lattice of flats isomorphic to the given one.

PRELIMINARIES

We assume familiarity with the notions "(finite) lattice","atom","covering","meet","join" in a lattice,"isomorphic lattices". The minimal,respectively the maximal,element of a finite lattice are called the zero,respectively the unit.

A lattice L is semimodular if it satisfies:

If $X,Y \in L$ and both X and Y cover meet(X,Y), then join(X,Y) covers both X and Y.

A lattice L is atomic if each element of L is the join of some atoms of L.

A set-lattice is the lattice of some sets (some subsets of the unit),ordered by inclusion.

Two set-lattices L_1 and L_2 are isomorphic if there is a bijection between their units,which maps the sets of L_1 onto the sets of L_2.

Remark. We should distinguish between "lattice isomorphism" and "set-lattice isomorphism". The second induces the first,but not conversely.

A matroid M on a finite set S is a semimodilar atomic set-lattice with the unit S,in which the meet of any two atoms is the zero.

The sets of a matroid M are also called the flats of M.

A hyperplane of a matroid M on S is a flat covered by the unit S. A matroid is completely determined by the family of its hyperplanes.

The addition of a new element z to a flat X of a matroid M is the substitution of all flats Y of M, which contain X, by $Y \cup \{z\}$. If X is the zero or an atom, then this operation produces (the flats of) a new matroid. The element z is said to be added to X.

An n-set is a set of cardinality n.

A matroid M is simple if all atoms of M are 1-sets.

A matroid is semisimple if it is not simple, but has the empty zero.

A loop of a matroid is an element of its zero.

The Steiner system S(d,k,n) is the family F of some k-subsets of an n-set A, such that each d-subset of A is contained in exactly one set of F. It is well-known that the sets of a Steiner system S(d,k,n) are hyperplanes of a matroid M, such that all j-subsets of the unit, which satisfy $j < d$, are flats of M.

The abbreviation "CWR" will be used for "combinations with repetitions". The CWR's are denoted by brackets "< >". The carrier of a CWR is the set of different elements included in the combination. The degree of an element in a CWR is the number of repetitions of the element. A CWR is obviously determined by the carrier and all the degrees. Two CWR's are isomorphic if there is a bijection between their carriers which preserves the degrees.

INTRODUCTION

All non-isomorphic non-simple matroids on at most 8 elements were constructed in [1]. For that purpose, new elements were added to the zero or to some atoms of simple matroids on smaller sets.

All non-isomorphic matroids with loops on n+1 elements can be naturally bijected (by deleting one loop) to all non-isomorphic matroids on n elements. This reduces the construction of non-isomorphic non-simple matroids to the construction of non-isomorphic semisimple matroids.

Each semisimple matroid with k atoms on n elements can be obtained by addition of n-k new elements to the atoms of the simple matroid with the isomorphic lattice of flats.

Conversely, given a simple matroid M on k elements, the following question can be raised: "Which non-isomorphic semisimple matroids on n elements can be obtained by addition of n-k new elements to the atoms of M ?"

Equivalently, the problem is to determine the classes of the following partition $\overset{M}{\sim}$ of the class of CWR's of length n-k, composed of atoms of M:

$$\langle x_1,\dots,x_{n-k}\rangle \overset{M}{\sim} \langle y_1,\dots,y_{n-k}\rangle \iff$$
$$\iff M_{\langle x_1,\dots,x_{n-k}\rangle} \simeq M_{\langle y_1,\dots,y_{n-k}\rangle}$$

Here $M_{\langle x_1,\dots,x_{n-k}\rangle}$ denotes the semisimple matroid, which is obtained from M by addition of one new element to each atom x_i (if an atom x appears q times in the CWR, then q new elements are added to x).

This problem is solved for $n \leqslant 8$ ([1]). Our goal is to develop methods for reducing it to some simpler problems in the general case. Although there is little hope that this might be used for producing all non-isomorphic non-simple matroids on 10 elements or more, we believe that it could be useful when applied to some special classes of simple matroids on larger sets.

THE POSITIONAL PARTITIONS

Our main idea is to describe $\overset{M}{\sim}$ by the use of some simpler equivalence relations. We define two partitions of atoms of M:

(a) the "weak positional partition" (WPP)

$$x \overset{M}{\underset{1}{\sim}} y \overset{def}{\iff} M_{\langle x\rangle} \simeq M_{\langle y\rangle}$$

(b) the "strong positional partition" (SPP)

$x \overset{M}{\approx} y \overset{def}{\Longleftrightarrow} M \equiv M(xy)$, where M(xy) denotes the matroid obtained from M by transposition of atoms x and y in all the flats which contain either of x and y.

The relation (a) is the special case of $\overset{M}{\underset{n-k}{\sim}}$ for n-k=1. The word "positional" denotes that these partitions are determined by position of atoms with respect to the other flats.

We prove several properties of the positional partitions. We primarily show that the WPP is tightly connected to the automorphisms of a matroid:

THEOREM 1. <u>The classes of $\overset{M}{\underset{1}{\sim}}$ coincide with the orbits of the automorphism group of the matroid</u> M.

<u>Proof</u>. Given two atoms x and y in the same class of $\overset{M}{\underset{1}{\sim}}$, let x_1 and y_1 denote the new elements added to the atoms x and y respectively, which yield the matroids $M_{\langle x\rangle}$ and $M_{\langle y\rangle}$. Any isomorphism α between $M_{\langle x\rangle}$ and $M_{\langle y\rangle}$ maps $\langle x,x_1\rangle$ onto $\langle y,y_1\rangle$ (these are the only atoms of cardinality 2). We may assume that $\alpha(x_1)=y_1$. Then α induces an automorphism of M, which maps x to y.

Conversely, given an automorphism β of M with $\beta(x)=y$, it can be easily extended to an isomorphism of $M_{\langle x\rangle}$ onto $M_{\langle y\rangle}$ by defining $\beta(x_1)=y_1$. Q.E.D.

A slightly more effective description of classes of $\overset{M}{\approx}$ is given by:

THEOREM 2. <u>If</u> x <u>and</u> y <u>are two atoms of a matroid</u> M <u>on</u> S, <u>then we have</u>: $x \overset{M}{\approx} y$ <u>if and only if</u>

$$\langle s_1,\dots,s_n,x\rangle \text{ is a flat of } M \Leftrightarrow \langle s_1,\dots,s_n,y\rangle \text{ is a flat of } M \text{ for each } \langle s_1,\dots,s_n\rangle \subseteq S\setminus\langle x,y\rangle$$

<u>Proof</u>. The transposition (xy) fixes all flats of M which either contain both of the atoms x,y or none of them. Assuming the above condition for flats, we have that the flats

containing x, but not y, are mapped (under (xy)) to the flats containing y, but not x, and conversely. This gives that all the flats in the matroids M and M(xy) coincide.

Conversely, let $M \equiv M(xy)$ and let $\langle z_1,\dots,z_n,x\rangle$ be a flat of M, where $\langle z_1,\dots,z_n\rangle \subseteq S\setminus\langle x,y\rangle$. Then we have that $\langle z_1,\dots,z_n,y\rangle$ is also a flat of M. Q.E.D.

The following theorem explains our use of the words "weak" and "strong":

THEOREM 3. If x and y are two atoms of a matroid M (on S), then $x \overset{M}{\approx} y$ implies $x \overset{M}{\top} y$.

Proof. Let $M_{\langle x\rangle}$ and $M_{\langle y\rangle}$ denote the matroids obtained from M by addition of x_1 to x, respectively y_1 to y.

We have for each $\langle z_1,\dots,z_n\rangle \subseteq S\setminus\langle x,y\rangle$:

$\langle z_1,\dots,z_n,x,x_1\rangle$ is a flat of $M_{\langle x\rangle} \Leftrightarrow \langle z_1,\dots,z_n,x\rangle$ is a flat of M $\Leftrightarrow \langle z_1,\dots,z_n,y\rangle$ is a flat of M $\Leftrightarrow$
$\Leftrightarrow \langle z_1,\dots,z_n,y,y_1\rangle$ is a flat of $M_{\langle y\rangle}$.

As $M \equiv M(xy)$, it is easy to check that the mapping defined by $\alpha(x)=y$, $\alpha(y)=x$, $\alpha(x_1)=y_1$, $\alpha(z)=z$ for each $z\in S\setminus\langle x,y\rangle$, is an isomorphism of $M_{\langle x\rangle}$ onto $M_{\langle y\rangle}$. Q.E.D.

Our next theorem emphasizes the role of SPP:

THEOREM 4. Let M be a simple matroid on S, where $S=\langle a_1,\dots,a_n\rangle$, and let α be a permutation of S, which preserves the classes of $\overset{M}{\approx}$, that is

$$\alpha(a_i) = a_j \Rightarrow a_i \overset{M}{\approx} a_j$$

Let $M\begin{pmatrix}a_1\dots a_n\\ p_1\dots p_n\end{pmatrix}$ denote the semisimple matroid obtained from M by adding p_i new elements to the atoms a_i ($p_i\in N\cup\langle 0\rangle$, $i=1,\dots,n$) . Then the matroids

$$M_1 = M\begin{pmatrix}a_1\dots a_n\\ p_1\dots p_n\end{pmatrix} \qquad \text{and} \qquad M_2 = M\begin{pmatrix}\alpha(a_1)\dots\alpha(a_n)\\ p_1\ \dots\ p_n\end{pmatrix}$$

are isomorphic.

Proof. Let M_1 be obtained from M by addition of the elements $x_{i1},x_{i2},\dots,x_{ip_i}$ to the atoms a_i, $i=1,\dots,n$ and let

M_2 be obtained from M by addition of the elements $y_{i1}, y_{i2}, \dots, y_{ip_i}$ to the atoms $\alpha(a_i)$, $i=1,\dots,n$.

We claim that the mapping $\beta: S + \bigcup x_{ij} \rightarrow S + \bigcup y_{ij}$ defined by

$$\beta(a_i) = \alpha(a_i) \qquad \text{for } i = 1,\dots,n$$
$$\beta(x_{ij}) = y_{ij} \qquad \text{for } j=1,\dots,p_i \text{ , } i=1,\dots,n$$

is an isomorphism of M_1 onto M_2.

It is easy to check that $\beta(M) = \alpha(M) = M$. Namely, α can be represented as a product of transpositions, so that the two elements of each transposition are in the same class of $\overset{M}{\approx}$. Any of these transpositions fixes the family of flats of M by Theorem 2.

Let X be an arbitrary flat of M_1. It consists of some atoms $a_{i_1},\dots,a_{i_s}$ of M, such that $\{a_{i_1},\dots,a_{i_s}\}$ is a flat of M , and of the added new elements

$$x_{i_1 1},\dots,x_{i_1 p_{i_1}},\dots,x_{i_s 1},\dots,x_{i_s p_{i_s}} .$$

Then $\beta(X)$ consists of the atoms $\alpha(a_{i_1}),\dots,\alpha(a_{i_s})$, such that $\{\alpha(a_{i_1}),\dots,\alpha(a_{i_s})\}$ is a flat of M, and of the (added) elements $y_{i_1 1},\dots,y_{i_1 p_{i_1}},\dots,y_{i_s 1},\dots,y_{i_s p_{i_s}}$.

It is obvious that $\beta(X)$, which satisfies these conditions, is a flat of M_2. Q.E.D.

Roughly speaking, Theorem 4 says that "if we take into account" the classes of $\overset{M}{\approx}$, then we cannot possibly miss a class of $\overset{M}{\sim}$. However, it is often the case that two isomorphic semisimple matroids can be obtained by addition of new elements to different combinations of classes of $\overset{M}{\approx}$.

It is for this reason that we are also trying to describe the classes of $\overset{M}{\sim}$ "from the opposite side".

We define a partition on CWR's of atoms of arbitrary length, which is induced by (the classes of) WPP, as follows:

$\langle x_1,\dots,x_q\rangle \underset{1\,q}{\overset{M}{\sim}} \langle y_1,\dots,y_q\rangle$ if and only if there exists an isomorphism between the CWR's $\langle x_1,\dots,x_q\rangle$ and $\langle y_1,\dots,y_q\rangle$, which preserves the classes of $\underset{1}{\overset{M}{\sim}}$.

Let $\underset{q}{\overset{M}{\sim}}$ denote the restriction of the relation $\overset{M}{\sim}$ to the CWR's of a fixed length q (it coincides with WPP for q=1).

THEOREM 5. __If__ x,y,z,t __are four different atoms of a simple matroid__ M, __then__ $\langle x,y\rangle \underset{2}{\overset{M}{\sim}} \langle z,t\rangle$ __implies__ $\langle x,y\rangle \underset{1\,2}{\overset{M}{\sim}} \langle z,t\rangle$.

__Proof__. Let $M_{\langle x,y\rangle}$ be obtained from M by addition of x_1 to x and y_1 to y and let $M_{\langle z,t\rangle}$ be obtained by addition of z_1 to z and t_1 to t. If $\langle x,y\rangle \underset{2}{\overset{M}{\sim}} \langle z,t\rangle$, then there exists an isomorphism α of $M_{\langle x,y\rangle}$ onto $M_{\langle z,t\rangle}$. It maps $\langle\langle x,x_1\rangle,\langle y,y_1\rangle\rangle$ to $\langle\langle z,z_1\rangle,\langle t,t_1\rangle\rangle$, because these are the only atoms of cardinality 2. We may assume that $\alpha(x_1)=z_1$, $\alpha(y_1)=t_1$. Then $\alpha(M_{\langle x\rangle}) = M_{\langle z\rangle}$, $\alpha(M_{\langle y\rangle}) = M_{\langle t\rangle}$, which gives $x \underset{1}{\overset{M}{\sim}} z$ and $y \underset{1}{\overset{M}{\sim}} t$ and $\langle x,y\rangle \underset{1\,2}{\overset{M}{\sim}} \langle z,t\rangle$. Q.E.D.

THEOREM 6. __If__ x __and__ y __are atoms of a simple matroid__ M, __then__ $\langle x,x\rangle \underset{2}{\overset{M}{\sim}} \langle y,y\rangle$ __if and only if__ $x \underset{1}{\overset{M}{\sim}} y$.

__Proof__. Follows by extension (respectively, by restriction) of isomorphisms between the corresponding matroids. Q.E.D.

The relations of type $\underset{1\,q}{\overset{M}{\sim}}$ are sufficient for generation of all non-isomorphic semisimple matroids on at most 7 elements, with one single exception.

This exception can be obtained in the following way:

Start with the simple matroid on 5 elements with the family of hyperplanes:

$\langle\langle a,b,c\rangle,\langle a,d,e\rangle,\langle b,d\rangle,\langle b,e\rangle,\langle c,d\rangle,\langle c,e\rangle\rangle$

The classes of $\underset{1}{\overset{M}{\sim}}$ are $\langle a\rangle$ and $\langle b,c,d,e\rangle$.

The classes of the partitions $\underset{1\,2}{\overset{M}{\sim}}$ and $\underset{2}{\overset{M}{\sim}}$ do not coincide: The set $\langle\langle b,c\rangle,\langle b,d\rangle,\langle b,e\rangle,\langle c,e\rangle,\langle d,e\rangle\rangle$ is a class of $\underset{1\,2}{\overset{M}{\sim}}$, but it contains two classes of $\underset{2}{\overset{M}{\sim}}$:

$\{\langle b,c\rangle,\langle d,e\rangle\}$ and $\{\langle b,d\rangle,\langle b,e\rangle,\langle c,d\rangle,\langle c,e\rangle\}$

One could hope that the relations $\overset{M}{\underset{1}{\sim}}$ and $\overset{M}{\underset{2}{\sim}}$, together with their induced partitions (one could try to define $\overset{M}{\underset{k\;q}{\sim}}$ as a generalization of $\overset{M}{\underset{1\;q}{\sim}}$) are sufficient for generation of all semisimple matroids (i.e., of all classes of $\overset{M}{\sim}$). This seems to be true for the majority of "small" matroids.

However, this is not true in general. The further counterexamples are of the following type:

Take a simple matroid M, such that the hyperplanes of M are sets of a Steiner system S(d,k,n). Then all the partitions $\overset{M}{\underset{1}{\sim}}$, $\overset{M}{\underset{2}{\sim}}$, ..., $\overset{M}{\underset{d}{\sim}}$ have just one equivalence class and they cannot help in detecting all non-isomorphic semisimple matroids, which can be obtained from M. However, the partition $\overset{M}{\underset{d+1}{\sim}}$ can fulfil this demand.

As no Steiner system S(d,k,n) is known with $d > 5$, we do not know an example of semisimple matroid, for the construction of which a relation $\overset{M}{\underset{j}{\sim}}$ with some $j \geqslant 7$ should be used.

We conjecture that a finite collection of partitions of type $\overset{M}{\underset{j}{\sim}}$ is sufficient for the construction of all non-isomorphic semisimple matroids, which can be obtained from a given simple matroid M.

REFERENCE

1. D.M.Acketa, <u>A construction of non-simple matroids on at most 8 elements</u>. to appear in J.Combin.Inform. System Sci.

Dragan M. Acketa
Institut za matematiku
21000 Novi Sad
dr Ilije Djuričića 4
Yugoslavia

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

CERTAIN IDEMPOTENT SEPARATING CONGRUENCES ON ORTHODOX SEMIGROUPS

Branka P. Alimpić

In this note we describe an idempotent separating congruence, denoted by μ_K, on an orthodox semigroup (Theorem 1). This congruence is defined by an expression which is a generalization of the formula for the greatest idempotent separating congruence μ on an orthodox semigroup (J. Meakin, [2]). Further, we construct a semigroup $\Theta_K(S)$ and a homomorphism of S onto $\Theta_K(S)$ which induces the idempotent separating congruence μ_K on S. In the case of an inverse semigroup S, such a homomorphism coincides with the embedding of the semigroup S in the normal hull $\Phi(K)$ of a normal subsemigroup K of S, obtained by M.Petrich [3]. By the way, we get a new characterization of the greatest idempotent-separating congruence on an orthodox semigroup by elements of the set $\Theta_E(S)$.

Following J. Meakin, the greatest idempotent separating congruence μ on an orthodox semigroup S is given by

$$a\mu b \Leftrightarrow (\exists a'\in V(a))(\exists b'\in V(b))(\forall e\in E)(a'ea = b'eb \wedge aea' = beb')$$

where E is the band of idempotents of S, and V(x) denotes the set of all inverses of an element x of S.

If S is an inverse semigroup, an expression for μ is given (J.M.Howie, [1]) by

$$a\mu b \Leftrightarrow (\forall e\in E)aea^{-1} = beb^{-1}.$$

Let K be an inverse subsemigroup of an inverse semigroup S. K is <u>normal</u> if it is full ($E\subseteq K$) and self-conjugate ($(\forall x\in S)x^{-1}Kx \subseteq K$). Following M.Petrich, a <u>normal hull</u> of an inverse semigroup S is the semigroup $\Phi(K)$ consisting of all isomorphisms among subsemigroups of K of the form eKe, $e\in E$, with composition of these isomorphisms as partial one-one mappings of K.

LEMMA 1. (M.Petrich, [3], Proposition 1) *Let K be A normal subsemigroup of an inverse semigroup S and let $\theta = \theta(S:K)$ be a function defined on S by $\theta : a \to \theta_K^a$, where $\theta_K^a : aKa^{-1} \to a^{-1}Ka$, and $x\theta_K^a = a^{-1}xa$. Then $\Theta(S:K)$ is an idempotent separating homomorphism of S into $\Phi(K)$ and*

$$\ker \theta(S:K)=\{a\in S \mid (\forall x\in K) aa^{-1}xa = axa^{-1}a\}.$$

Let S be an orthodox semigroup, and let E be the band of idempotents of S. Define the set

$$\mathcal{K} = \{K\subseteq S \mid K^2\subseteq K,\ E\subseteq K \quad \text{and} \quad (\forall x\in S)(\forall x'\in V(x))x'Kx\subseteq K\}.$$

Since S is orthodox, we have $E^2\subseteq E$, $(\forall x\in S)(\forall x'\in V(x))x'Ex \subseteq E$, so $E\in\mathcal{K}$.

LEMMA 2. Let a,b be arbitrary elements of S. If $K\in\mathcal{K}$, the following formulae are equivalent

(i) $(\exists a'\in V(a))(\exists b'\in V(b))(\forall x\in K)(a'xa=b'xb \wedge axa'=bxb')$

(ii) $(\forall a'\in V(a))(\exists_1 b'\in V(b))(\forall x\in K)(a'xa=b'xb \wedge axa'=bxb')$.

Proof. First we prove the implication

$$(\forall x\in K)(a'xa=b'xb \wedge axa'=bxb') \Rightarrow (a'a=b'b \wedge aa'=bb'),$$

where $a'\in V(a)$ and $b'\in V(b)$. Suppose that $a'xa=b'xb$, for all x, $x\in K$. Then we get

$$
\begin{aligned}
a'a &= a'(aa')a = b'(aa')b && (\text{Since } aa'\in K)\\
&= b'(aa'bb')b = a'(aa'bb')a && (\text{Since } aa'bb'\in K)\\
&= a'(bb')a = b'(bb')b = b'b && (\text{Since } bb'\in K).
\end{aligned}
$$

Similarly, from $(\forall x\in K)axa'=bxb'$ it follows that $aa'=bb'$.

Therefore, if (i) holds, there are inverses a' of a and b' of b such that $a'xa=b'xb$, $axa'=bxb'$, for all x, $x\in K$, and $a'a=b'b$, $aa'=bb'$. Hence $a\mathcal{H}b$, and for every inverse a^* of a there exists an inverse b^* of b, such that $a^*a=b^*b$ and $aa^*=bb^*$. So we have $a^*xa=a^*aa'aa^*xa=b^*ba'(bb^*x)a=b^*bb'(bb^*x)b=b^*xb$, and similarly $axa^*=bxb^*$, for all x, $x\in K$.

If there is an inverse $\bar{b}$ of b such that

$$(\forall x\in K)(a^*xa=\bar{b}xb \wedge axa^*=bx\bar{b}),$$

we have $a^*a=\bar{b}b$, $aa^*=b\bar{b}$, and so $b^*b=\bar{b}b$, $bb^*=b\bar{b}$, which yields $\bar{b}=\bar{b}b\bar{b}=b^*b\bar{b}=b^*bb^*=b^*$. Hence (i) $\Rightarrow$ (ii).

Since the reverse implication is trivial, the lemma is proved.

The following theorem generalizes the theorem 4.4[2] of J. Meakin.

THEOREM 1. Let S be an orthodox semigroup. If $K\in\mathcal{K}$, the relation μ_K of the set S defined by

$$a\,\mu_K b \Leftrightarrow (\exists a'\in V(a))(\exists b'\in V(b))\ (\forall x\in K)(a'xa=b'xb\ \wedge\ axa'=bxb')$$

is an idempotent separating congruence on S.

Proof. The relation μ_K is obviously reflexive and symmetric, we prove that it is transitive. Suppose that $a\,\mu_K b$ and $b\,\mu_K c$. Then by the lemma 2 there exist inverses a' of a, b' of b and c' of c such that $a'xa=b'xb=c'xc$, and $axa'=bxb'=cxc'$, for all x, $x\in K$, so we get $a\,\mu_K c$.

Now suppose that $a\,\mu_K b$ and $c\in S$. Then there are inverses a' of a and b' of b such that $a'xa=b'xb$ and $axa'=bxb'$, for all x, $x\in K$. Let c' be an inverse of c. Then

$$c'a'xac=c'b'xbc \quad\text{and}\quad acxc'a'=bcxc'b' \qquad (\text{since } cxc'\in K),$$

for all x, $x\in K$. Therefore $ac\,\mu_K cb$, since $c'a'\in V(ac)$ and $c'b'\in V(bc)$. Similarly $ca\,\mu_K cb$, so μ_K is a congruence.

From the proof of the lemma 2 it follows $\mu_K\subseteq\mathcal{H}$, hence μ_K is idempotent separating. This completes the proof of the theorem.

Obviously, if $K=E$, then μ_E is the greatest idempotent separating congruence μ on S.

LEMMA 3. Let $a'\in V(a)$, then

$$(\forall x\in K)(axa'a=a'axa\ \wedge\ aa'xa=axaa') \Rightarrow a'a=aa'.$$

Proof. Let $axa'a=a'axa$ and $aa'xa=axaa'$. Then we have for $x=aa'$ and $x=a'a$, respectively

$$a=aa'(aa')a=a(aa')aa'=a\cdot aa',$$
$$a=a(a'a)a'a=a'a(a'a)a=a'a\cdot a,$$

hence $a'a=a'a\cdot aa'=aa'$, and the lemma is proved.

LEMMA 4. Let S be an orthodox semigroup, $a\in S$ and $K\in\mathcal{K}$. The following conditions are equivalent:

(i) $a\in\ker\mu_K$

(ii) $(qa'\in V(a))(\forall x\in K)(axa'a=a'axa\ \wedge\ aa'xa=axaa')$

(iii) $(qa'\in V(a))(\forall x\in K)(axa'a=a'axa\ \wedge\ aa'=a'a)$,

where $q\in\{\exists,\exists_1\}$.

Proof. Suppose that $a \in \ker \mu_K$, then $a \mu_K e$, for some idempotent e of S. Since $e \in V(e)$, it follows from the lemma 2 that there exists exactly one inverse a' of a such that $axa' = exe = a'xa$, for all $x \in K$, and $a'a = aa' = e$. Hence,

$$\text{(i)} \Rightarrow (\exists_1 a' \in V(a))(\forall x \in K)(axa' = a'axaa' = a'xa) \Rightarrow \text{(ii)}.$$

By lemma 3, we get (ii) $\Leftrightarrow$ (iii). Finaly,

$$\text{(iii)} \Rightarrow \text{(iii)} \wedge \text{(ii)} \Rightarrow (\exists a' \in V(a))(\forall x \in K)(axa' = a'axaa' = a'axa'a$$
$$\wedge\ a'xa = a'axaa' = a'axa'a) \Rightarrow (\exists a' \in V(a))a \mu_K a'a \Rightarrow \text{(i)}.$$

The lemma is proved.

COROLLARY 1. *Let S be an orthodox semigroup and $a \in S$. The following conditions are equivalent:*

(i) $a \in \ker \mu$

(ii) $(qa' \in V(a))(\forall x \in E)(axa'a = a'axa \wedge aa'xa = axaa')$

(iii) $(qa' \in V(a))(\forall x \in E)(axa'a = a'axa \wedge aa' = a'a)$,

where $q \in \{\exists, \exists_1\}$.

For $K \leq S$, the centralizer $K\zeta$ of K is the set

$$K\zeta = \{a \in S \mid (\forall x \in K)ax = xa\}.$$

LEMMA 5. *If S is an orthodox semigroup, and $K \in \mathcal{K}$ then* $\ker \mu_K \leq K\zeta \Leftrightarrow K \leq E\zeta$.

Proof. Let $K \leq E\zeta$ then we have

$$a \in \ker \mu_K \Leftrightarrow (\exists a' \in V(a))(\forall x \in K)(axa'a = a'axa \wedge aa' = a'a)$$
$$\Rightarrow (\exists a' \in V(a))(\forall x \in K)aa'ax = xaa'a$$
$$\Leftrightarrow (\forall x \in K)ax = xa$$
$$\Leftrightarrow a \in K\zeta$$

Conversely, let $\ker \mu_K \leq K\zeta$. Since $E \leq \ker \mu_K$, we have $E \leq K\zeta$, wich is equivalent to $K \leq E\zeta$. The lemma is proved.

Now suppose that S is an inverse semigroup, then the congruence μ_K can be expressed in the following way:

LEMMA 6. *Let S be an inverse semigroup and $K \in \mathcal{K}$. Then*

$$a \mu_K b \Leftrightarrow (\forall x \in K)axa^{-1} = bxb^{-1},$$

and $\ker \mu_K = \{a \in S \mid (\forall x \in K)aa^{-1}xa = axa^{-1}a\}$.

Proof. The implication $a\mu_K b \Rightarrow (\forall x\in K)axa^{-1}=bxb^{-1}$ follows immediately from the definition of μ_K. Conversely, define $a\sim b \Leftrightarrow (\forall x\in K)axa^{-1}=bxb^{-1}$. It is straightforward to verify that $\sim$ is a congruence, so $a\sim b \Rightarrow a^{-1}\sim b^{-1}$, which yields $(\forall x\in K)a^{-1}xa=$ $=b^{-1}xb$. Hence, $(\forall x\in K)axa^{-1}=bxb^{-1} \Leftrightarrow a\mu_K b$.

Suppose that $a\in \ker\mu_K$, then $(\forall x\in K)axa^{-1}=exe$, for some idempotent e, and $aa^{-1}=e$. Hence,

$$a\in \ker\mu_K \Leftrightarrow (\forall x\in K)axa^{-1}=aa^{-1}xaa^{-1}$$
$$\Leftrightarrow (\forall x\in K)axa^{-1}a=aa^{-1}xa,$$

and the lemma is proved.

COROLLARY 2. If S is an inverse semigroup, then

(i) $\ker\mu_K = K\zeta \Leftrightarrow K\leq E\zeta$

(ii) $\ker\mu = E\zeta$.

Let a be an arbitrary element of an orthodox semigroup S and $a'\in V(a)$. If $K\in\mathcal{K}$, we have

$$aKa'=aa'aKa'aa'\leq aa'Kaa'\leq aKa',$$

so $aKa'=aa'Kaa'$, and therefore

$$x\in aKa' \Leftrightarrow x=aa'xaa' \Leftrightarrow x=aa'x=xaa'.$$

From these equivalences we have

$$x,y\in aKa' \Rightarrow x=aa'x \wedge y=yaa' \Rightarrow xy=aa'xyaa' \Rightarrow xy\in aKa',$$

so aKa' is a subsemigroup of K. Since $a\in V(a')$, it follows that $a'Ka$ is a subsemigroup of K, too.

Let $\theta^a_{a'}(K)$ be a mapping of aKa' into $a'Ka$ defined by $x\theta^a_{a'}(K) \overset{def}{=} a'xa$. Since

$$(xy)\theta^a_{a'}(K)=a'xya=a'xaa'ya=x\theta^a_{a'}(K)y\theta^a_{a'}(K) \quad \text{for } x,y\in aKa',$$
$$x\theta^a_{a'}(K)\circ\theta^{a'}_a(K) = aa'xaa'= x, \quad \text{for } x\in aKa', \text{ and}$$
$$x\theta^{a'}_a(K)\circ\theta^a_{a'}(K) = a'axa'a = x, \quad \text{for } x\in a'Ka,$$

the mappings $\theta^a_{a'}(K)$ and $\theta^{a'}_a(K)$ are mutually inverse isomorphisms among aKa' and $a'Ka$.

LEMMA 7. Let S be an orthodox semigroup, and $a,b \in S$. Then

$$(\forall x \in K)(a'xa=b'xb \wedge axa'=bxb') \Leftrightarrow \theta^{a}_{a'}(K) = \theta^{b}_{b'}(K),$$

where a' is an inverse of a, b' is an inverse of b, and $K \in \mathcal{K}$.

Proof. First, we observe that

$$aKa'=bKb' \Rightarrow aa' \in bKb' \wedge bb' \in aKa' \Rightarrow aa'=aa'bb'=bb',$$

and dually, $a'Ka=b'Kb \Rightarrow a'a=b'b$. Now we have

$$\begin{aligned} &(\forall x \in K)(a'xa=b'xb \wedge axa'=bxb') \\ \Rightarrow\ &aKa'=bKb' \wedge (\forall x \in aKa')a'xa=b'xb \\ \Rightarrow\ &\theta^{a}_{a'}(K) = \theta^{b}_{b'}(K). \end{aligned}$$

Conversely, if $\theta^{a}_{a'}(K)= \theta^{b}_{b'}(K)$, then $aKa'=bKb'$, $a'Ka = b'Kb$ and $(\forall x \in aKa')a'xa=b'xb$, so we have $aa'=bb'$ and $a'a=b'b$. Let $x \in K$, then

$$\begin{aligned} a'xa&=a'(aa'xaa')a = b'(aa'xaa')b && (\text{Since } aa'xaa' \in aKa') \\ &=b'(bb'xbb')b = b'xb && (\text{Since } aa'=bb'). \end{aligned}$$

By dual arguments, we may prove that $(\forall x \in K)axa'=bxb'$. The lemma is proved.

Remark. From the proof of the preceding lemma, we get a characterization of the $\mathcal{H}$-equivalence of an orthodox semigroup. If $K \in \mathcal{K}$, we have

$$\begin{aligned} a\mathcal{H}b &\Leftrightarrow (qa')(\exists b')(aKa'=bKb' \wedge a'Ka=b'Kb) \\ &\Leftrightarrow (qa')(\exists b')(aEa'=bEb' \wedge a'Ea=b'Eb), \end{aligned}$$

where $q \in \{\forall, \exists\}$.

Now, for an arbitrary element a of S, and $K \in \mathcal{K}$, we define the set $\theta_K(a)= \{\theta^{a}_{a'}(K) \mid a' \in V(a)\}$. As a consequence of lemmata 2 and 7, we get

THEOREM 2. Let S be an orthodox semigroup, $a,b \in S$, and $K \in \mathcal{K}$. Then the following conditions are equivalent

(i) $\theta_K(a) \cap \theta_K(b) \neq \emptyset$

(ii) $a \mu_K b$

(iii) $\theta_K(a) = \theta_K(b)$.

Proof. $\theta_K(a) \cap \theta_K(b) \neq \emptyset \Leftrightarrow (\exists a' \in V(a))(\exists b' \in V(b))\, \theta^a_{a'}(K) = \theta^b_{b'}(K)$

$\Leftrightarrow (\exists a' \in V(a))(\exists b' \in V(b))(\forall x \in K)(a'xa = b'xb \wedge axa' = bxb')$

(By the lemma 7)

$\Leftrightarrow a \mu_K b$ (By definition of μ_K)

$\Leftrightarrow (\forall a' \in V(a))(\exists b' \in V(b))(\forall x \in K)(a'xa = b'xb \wedge axa' = bxb') \wedge$
$(\forall b' \in V(b))(\exists a' \in V(a))(\forall x \in K)(a'xa = b'xb \wedge axa' = bxb')$

(By the lemma 2)

$\Leftrightarrow (\forall a' \in V(a))(\exists b' \in V(b))\ \theta^a_{a'}(K) = \theta^b_{b'}(K) \wedge$
$(\forall b' \in V(b))(\exists a' \in V(a))\ \theta^b_{b'}(K) = \theta^a_{a'}(K)$

(By the lemma 7)

$\Leftrightarrow \theta_K(a) \subseteq \theta_K(b) \wedge \theta_K(b) \subseteq \theta_K(a)$

$\Leftrightarrow \theta_K(a) = \theta_K(b).$

The theorem is proved.

If K=E, denote by $\theta(a)$ the set $\theta_E(a)$. Then we have

COROLLARY 3. Let S be an orthodox semigroup. If $a, b \in S$, then

$$a \mu b \Leftrightarrow \theta(a) = \theta(b) \Leftrightarrow \theta(a) \cap \theta(b) \neq \emptyset,$$

where μ is the greatest idempotent separating congruence on S.

Let S be an orthodox semigroup, $K \in \mathcal{K}$ and let $\theta_K(S)$ be the set defined by

$$\theta_K(S) = \{\theta_K(a) \mid a \in S\}.$$

Since μ_K is a congruence on the semigroup S, and $a \mu_K b \Leftrightarrow \theta_K(a) = \theta_K(b)$, we may define an operation $*$ on the set $\theta_K(S)$ by

$$\theta_K(a) * \theta_K(b) \overset{def}{=} \theta_K(ab).$$

Therefore, $(\theta_K(S), *)$ is a homomorphic image of the orthodox semigroup S.

If S is an inverse semigroup, the set $\theta_K(a)$ consists of the single element $\theta^a_K = \theta^a_{a^{-1}}(K)$, and

$$\theta_K(a) * \theta_K(b) = \{\theta^a_K\} * \{\theta^b_K\} = \{\theta^{ab}_K\}.$$

If we identify $\{\theta^a_K\}$ with θ^a_K, we get $\theta^a_K * \theta^b_K = \theta^{ab}_K$.

Hence, by the lemma 1, $\theta_K^a * \theta_K^b = \theta_K^a \circ \theta_K^b$, where $\circ$ is the composition of mappings. In this case, the theorem 2 reduces to

THEOREM 3. *Let* S *be an inverse semigroup*, a,b $\in$ S, *and* $K \in \mathcal{K}$. *Then*

$$a \mu_K b \Leftrightarrow \theta_K^a = \theta_K^b .$$

Hence, if K is a normal subsemigroup of an inverse semigroup S, the congruence μ_K coincides with the congruence $\theta(S:K)$, obtained by M.Petrich (the lemma 1).

REFERENCES

1. J.M.Howie, *The maximum idempotent-separating congruence on an inverse semigroup*, Proc.Edinburgh Math.Soc.(2),14(1964), 71-79.

2. J.Meakin, *Congruences on orthodox semigroups*, J.Australian Math.Soc. 12(1971), 323-341.

3. M.Petrich, *Extension normales de demi-groupes inverses*, Fundam. Math. 112, 187-203 (1981).

4. J.M.Howie, *An introduction to semigroup theory*, Academic Press, London 1976.

Branka P. Alimpić
Prirodno-matematički fakultet
Beograd
Studentski trg 16
Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd 3-4 December 1982

FREE REGULAR ORTHOCRYPTOGROUP

Dragan Blagojević, Aleksandar Krapež

A semigroup which is a union of groups is said to be completely regular. Such a semigroup is provided in a natural way with a unary operation (usually called inversion) $a \mapsto a^{-1}$, where a^{-1} is the group inverse of a in the maximal subgroup containing a. This unary operation satisfies the identities

$$(1) \qquad xx^{-1}x = x, \quad x^{-1}xx^{-1} = x^{-1}, \quad xx^{-1} = x^{-1}x.$$

In fact completely regular semigroups can be defined as a unary semigroup (a semigroup with an added unary operation) satisfying these identities. If the idempotents of a completely regular semigroup form a subsemigroup, the semigroup is said to be orthodox and is called an orthogroup. If in addition $\mathcal{H}$ is a congruence, the orthogroup is called an orthocryptogroup and it can be characterized within completely regular semigroups by the identity

$$(2) \qquad (xy)^o = x^o y^o$$

where x^o denotes xx^{-1}, or equally $x^{-1}x$.

The free regular orthocryptogroup is described in [1, Section 5]. Of course, the description is inductive. In this paper we will, following [1], restrict ourselves to regular orthocryptogroups (the idempotents form a regular band) since we want to avoid inductivity and to refine the description. We will also consider the case when $\mathcal{H}$-classes are Abelian groups.

The free unary semigroup is background for our work. So, let X be a given set and let F be the free semigroup on $X \cup \{(,)^{-1}\}$, where $($ and $)^{-1}$ are new symbols not in X. The free unary semigroup on X, i.e. $U(X)$, is the smallest subset of F satisfying the conditions: (i) $X \subseteq U(X)$, (ii) if

$u \in U(X)$, then $(u)^{-1} \in U(X)$, (iii) if $u,v \in U(X)$, then $uv \in U(X)$. When writing words from $U(X)$ usual conventions for dropping parentheses will be addopted. The free unary monoid on X, i.e. $U^{\prime}(X)$, is obtained from $U(X)$ by adding the empty word Θ behaving as an identity: $u\Theta = \Theta u = u$, for every $u \in U(X)$.

Let us recall some notions regarding words. The initial $i(w)$ of a word $w \in U(X)$ is obtained from w by taking only the first occurrence of every variable from X and dropping everything else. The final $f(w)$ of w is defined dually ("last" instead of "first"). The content $c(w)$ of w is the set of variables from X occurring in w. The reduced word $\tilde{r}(w)$ of w is obtained from w by removing from it all occurrences of u^{o} for any word u. In fact $r(w)$ is obtained by solving word problem for groups.

Definition 1. Let $v,w \in U(X)$. Then $v \rho w$ if and only if $i(v) = i(w)$, $f(v) = f(w)$, $r(v) = r(w)$.

THEOREM 1. $U(X)/\rho$ *is the free regular orthocryptogroup on* X.

Proof. It is evident that ρ is an equivalence. I is easy to see that it is also a congruence. The following facts can be used: $\varphi(vw) = \varphi(\varphi(v)\varphi(w))$, for $\varphi \in \{i,f,r\}$, $i(w^{-1}) = i(w^{o}) = i(w)$, $f(w^{-1}) = f(w^{o}) = f(w)$, $r(w^{-1}) = (r(w))^{-1}$; $r(w^{o}) = \Theta$. S/ρ satisfies the identities (1),(2), i.e. the following hold: $xx^{-1}x \rho x$, $x^{-1}xx^{-1} \rho x^{-1}$, $xx^{-1} \rho x^{-1}x$, $(xy)^{o} \rho x^{o}y^{o}$, $(xyxzx)^{o} \rho (xyzx)^{o}$. That can be checked by a straightforward verification. Notice that $i(xyxzx) = i(xyz) = i(xyzx)$, $f(xyxzx) = f(yzx) = f(xyzx)$. The mapping $j: x \mapsto x\rho$ is an injection from X into $U(X)/\rho$, and $U(X)/\rho$ is generated by $\{a\rho \mid a \in X\}$. Let S be any regular orthocryptogroup and $\phi: X \to S$ any mapping. Define $\Psi: U(X)/\rho \to S$ by $(a\rho)\Psi = a\phi$ if $a \in X$, and $((uv)\rho)\Psi = (u\rho)\Psi(v\rho)\Psi$, $(u^{-1})\Psi = (u\phi)^{-1}$. Then Ψ is a homomorphism and $j\Psi = \phi$. So, $U(X)/\rho$ is the free regular orthocryptogroup on X.

A model of the free regular orthocryptogroup on X can be constructed as follows. Let $\overline{U}(X)$ be the set of triples $(a_1 \dots a_n,\ g,\ a_{1\pi} \dots a_{n\pi})$ satisfying: $a_i \in X$, $a_i \neq a_j$, if $i \neq j$; $g \in G(X)$, where $G(X)$ is the free group on X, with $c(g) \subseteq \{a_1,\dots,a_n\}$ (We can equivalently say $g \in G(\{a_1,\dots,a_n\})$, where $G(\{a_1,\dots,a_n\})$ is the free group on $\{a_1,\dots,a_n\}$), and π is any permutation of the set $\{1,\dots,n\}$. Let a product be given by

$$(a_1\dots a_n,\ g,\ a_{1\pi}\dots a_{n\pi})\ (b_1\dots b_m,\ h,\ b_{1\pi}\dots b_{m\pi}) = \\ = (i(a_1\dots a_n b_1\dots b_m),\ gh,\ f(a_{1\pi}\dots a_{n\pi} b_{1\pi}\dots b_{m\pi}))$$

Then in $U(X)$ holds $(a_1\dots a_n,\ g,\ a_{1\pi}\dots a_{n\pi})^{-1} = (a_1\dots a_n,\ g^{-1},\ a_{1\pi}\dots a_{n\pi})$, so $(U(X),\cdot,{}^{-1})$ is a model of the free regular orthocryptogroup on X.

From this model one can get models for free objects in subvarieties of the variety of regular orthocryptogroups. For example, if we drop the second component from elements of $\overline{U}(X)$, we will get a model for the free regular band. A (pretty long) description of the free regular band in set theoretic terms can be found in [2].

THE CASE WHEN $\mathcal{H}$-CLASSES ARE ABELIAN GROUPS

Regular orthocryptogroups having Abelian groups for $\mathcal{H}$-classes can be described by the identities (1),(2) and the identity (see [4])

(3) $$(xy)^0x(xy)^0y(xy)^0 = (xy)^0y(xy)^0x(xy)^0$$

But

$$\begin{aligned}(3) &\iff (xy)^0xx^0y^0y(xy)^0 = x^0y^0y(xy)^0xx^0y \\ &\iff (xy)^0xy(xy)^0 = x^{-1}xy(xy)^0xyy^{-1} \\ &\iff xy = x^{-1}xyxyy^{-1} \\ &\iff x^2y^2 = (xy)^2\end{aligned}$$

So, instead of (3) we can take the identity

(4) $$(xy)^2 = x^2y^2$$

which is simpler than (3). Notice that the identities (1),(2) and (4) do not form a minimal set of identities (see [3, Theorem 2.1]).

Define $e_a(w)$, the exponent of the letter a in the word w, as follows: $e_a(a) = 1$, $e_a(b) = 0$, if b is a letter different from a; $e_a(vw) = e_a(v) + e_a(w)$, $e_a(w^{-1}) = -e_a(w)$, where v and w are from $U(X)$.

Definition 2. Let $v, w \in U(X)$. Then $v\,\bar{\rho}\,w$ if and only if $i(v) = i(w)$, $f(v) = f(w)$, $e_a(v) = e_a(w)$ for every $a \in c(v) = c(w)$.

THEOREM 2. $U(X)/\bar{\rho}$ *is the free regular orthocryptogroup with Abelian groups for* $\mathcal{H}$*-classes.*

The proof is similar to that of Theorem 1 and will be omitted. Even in the case when X is finite the free semigroups in Theorems 1 and 2 are infinite. But it is not the case if we restrict $\mathcal{H}$-classes to be groups from some subvariety of the variety of Abelian groups. These varieties are defined by the identities $x^{n+1} = x$. Let A_n denote the variety of Abelian groups satisfying $x^{n+1} = x$. The last identity together with the identities (1),(2),(4) defines regular orthocryptogroups with $\mathcal{H}$-classes from A_n.

Definition 3. Let $v,w \in U(X)$. Then $v\,\bar{\rho}_n\,w$ if and only if $i(v) = i(w)$, $f(v) = f(w)$, $e_a(v) = e_a(w) (\mathrm{mod}\, m)$, for every $a \in c(v) = c(w)$.

Now we can state the following theorem.

THEOREM 3. $U(X)/\bar{\rho}_n$ *is the free regular orthocryptogroup with* $\mathcal{H}$*-classes from* A_n.

COROLLARY. *If* X *is finite, then* $|U(X)/\bar{\rho}_n| = \sum_{i=1}^{|X|} \binom{|X|}{i} (i!)^2 n^i$.

Proof. The regular band E of idempotents of $U(X)/\bar{\rho}_n$ is free and $|E| = \sum_{i=1}^{|X|} \binom{|X|}{i} (i!)^2$ (see [2, p. 155]). Every idempotent e from E is in an $\mathcal{H}$-class which is the free group on the subset of X determining the $\mathcal{D}$-class of e (Words with the same content are $\mathcal{D}$-related). This free group has $n^{|Y|}$ elements, where Y is the subset under consideration. Now the assertion immediately follows.

Smilarly, using the formula for the number of elements of the free band on a finite set X, we can get the number of elementsof the free orthocryptogroup on X with $\mathcal{H}$-classes from A_n.

REFERENCES

1. J.A. Gerhard, M. Petrich, The word problem for orthogroups, Canad. J. Math. 33(1981), 893 - 900.
2. N. Länger, The free algebra in the variety generated by quasy-trivial semigroups, Semigroup Forum 20(1980), 151 - 156.
3. T. Nordahl, Semigroups satisfying $(xy)^m = x^m y^m$, Semigroup Forum 8(1974), 332 - 346.
4. M. Petrich, Verieties of ortodox bands of groups, Pacific J. Math. 58(1975), 209 - 217.

Matematički institut
Kneza Mihaila 35
11000 Beograd
Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

THE TRANSLATIONAL HULL OF A REES MATRIX SEMIGROUP OVER A MONOID

Stojan Bogdanović

Abstract. We describe the semigroups of all left translations, all right translations and the translational hull of Rees matrix semigroup over a monoid.

Let $D = D^1$ be a monoid with group G of units of D and P be a regular $M \times I$ -matrix over G°. Let $M^\circ(I,D,M,P)$ be a set of elements (i,a,μ), where $a \in D^\circ$ (D with zero adjoined), $i \in I$, $\mu \in M$ (the elements $(i,0,\mu)$ are identified with 0) and operation is definied by

$$(i,a,\mu)(j,b,\nu) = (i,ap_{\mu j}b,\nu) .$$

Then $M^\circ(I,D,M,P)$ is a semigroup which we call the Rees matrix semigroup over D°. (G.Lallement-M.Petrich:A generalization of the Rees theorem in semigroups,Acta Sci.Math.30(1969),113-132).

The semigroup $\Lambda(S)$ for a Rees matrix semigroup over a monoid D, can be constructed by a device analogous to the wreth product of groups. ($\Lambda(S)$ is the set of all left translation of S).

Let $X \neq \emptyset$ and D be a monoid. Let φ and φ' be functions from subsets of X into D, written on the left, and define the product of these two functions by

$$(\varphi \cdot \varphi')x = (\varphi x)(\varphi' x)$$

for all $x \in X$ for which $(\varphi x)(\varphi' x)$ is definied, i.e. for all $x \in \operatorname{dom}\varphi \cap \operatorname{dom}\varphi'$.

If $\mathcal{F}(X)$ is the semigroup of all partial transformations on X written on the left, then for $\alpha \in \mathcal{F}(X)$ and φ as before, define φ^α as the function

$$\varphi^\alpha x = \varphi(\alpha x)$$

for all $x \in X$ for which $\varphi(\alpha x)$ is defined, i.e., for all $x \in \operatorname{dom}\alpha$ such that $\alpha x \in \operatorname{dom}\varphi$.

Definition 1. Let P be a subsemigroup of $\mathcal{F}(X)$ and D be a monoid. The left wreath product of P and D, denoted by $PwlD$, is the set

$$\{(\alpha,\varphi) : \alpha \in P, \ \varphi : \mathrm{dom}\,\alpha \to D\}$$

together with the multiplication

$$(\alpha,\varphi)(\alpha',\varphi') = (\alpha\alpha', \varphi^{\alpha'}\cdot\varphi') .$$

It is easy to see that $PwlD$ is a groupoid. That this multiplication is associative will follow from the next theorem.

THEOREM 1. Let $S = M^{\circ}(I,D,M,P)$. Then the function f defined by $f\lambda = (\alpha,\varphi)$, $(\lambda \in \Lambda(S))$, where $\mathrm{dom}\,\alpha = \mathrm{dom}\,\varphi = \{i \in I : \lambda(i,1,\mu) \neq 0\}$, $\lambda(i,1,\mu) = (\alpha i, \varphi i, \mu)$ if $i \in \mathrm{dom}\,\alpha$ is an isomorphism of $\Lambda(S)$ onto $\mathcal{F}(I)wlD$.

Proof. Assume that $\lambda(i,a,\mu) \neq 0$. Then there exists $j \in I$ such that $p_{\mu j} \neq 0$, so

$\lambda(i,a,\mu) = \lambda[(i,a,\mu)(j,p_{\mu j}^{-1},\mu)] = [\lambda(i,a,\mu)](j,p_{\mu j}^{-1},\mu) \neq 0$.

Hence, $\lambda(i,a,\mu) = (k,b,\mu)$ for some $k \in I$, $b \in D$ and a left translation does not change the index in M.

Assume that $\lambda(i,1,\mu) = (j,b,\mu) \neq 0$, $\lambda(i,1,\nu) = (k,c,\nu) \neq 0$, then for some $m \in I$, $p_{\mu m} \neq 0$, so $(j,b,\nu) = (j,b,\mu)(m,p_{\mu m}^{-1},\nu) = [\lambda(i,1,\mu)](m,p_{\mu m}^{-1},\nu) = \lambda[(i,1,\mu)(m,p_{\mu m}^{-1},\nu)] = \lambda(i,1,\nu) = (k,c,\nu) \neq 0$. Hence, $j = k$, $b = c$, i.e. the first two indices of $\lambda(i,1,\mu)$ depends only on i.

For $f\lambda = (\alpha,\varphi)$, $i \in \mathrm{dom}\,\alpha$ and for any $(i,a,\mu) \in S$ there exists $j \in I$ such that $p_{\mu j} \neq 0$, and thus

$\lambda(i,a,\mu) = \lambda[(i,1,\mu)(j,p_{\mu j}^{-1}a,\mu)] = [\lambda(i,1,\mu)](j,p_{\mu j}^{-1}a,\mu) = (\alpha i,\varphi i,\mu)(j,p_{\mu j}^{-1}a,\mu) = (\alpha i,(\varphi i)a,\mu)$.

Therefore,

$$\lambda(i,a,\mu) = \begin{cases} (\alpha i,(\varphi i)a,\mu) & \text{if } i \in \mathrm{dom}\,\alpha \\ 0 & \text{if } i \notin \mathrm{dom}\,\alpha \end{cases} \tag{1}$$

Let $\lambda,\lambda' \in \Lambda(S)$, $f(\lambda) = (\alpha,\varphi)$, $f(\lambda') = (\alpha',\varphi')$. For $\alpha\alpha' \neq 0$, let $i \in \mathrm{dom}(\alpha\alpha')$. Then $i \in \mathrm{dom}\,\alpha'$, $\alpha i \in \mathrm{dom}\,\alpha$ and using the existence of $j \in I$ such that $p_{\mu j} \neq 0$, we have by (1)

$\lambda\lambda'(i,1,\mu) = \lambda(\alpha' i, \varphi' i,\mu) = (\alpha\alpha' i,(\varphi\alpha' i)(\varphi' i),\mu) = (\alpha\alpha' i,(\varphi^{\alpha'}\cdot\varphi')i,\mu)$. If $\alpha\alpha' = \emptyset$, then $\lambda\lambda' = 0$, since otherwise there would exist $i \in I$ such that $\lambda\lambda'(i,1,\mu) \neq 0$ and the above calculation would imply that $\alpha\alpha' \neq \emptyset$. Therefore f is a homomorphism. It follows from (1) that $f\lambda = f\lambda'$ implies $\lambda = \lambda'$, so that f is one-to-one.

Let $(\alpha,\varphi) \in \mathcal{F}(I)\text{wl}D$ and define λ by (1) .If $i \in \text{dom}\alpha$ and $p_{\mu j} \neq 0$, then

$[\lambda(i,a,\mu)](j,b,\nu) = (\alpha i,(\varphi i)a,\mu)(j,b,\nu) = (\alpha i,(\varphi i)ap_{\mu j}b,\nu) = \lambda(i,ap_{\mu j}b,\nu) = \lambda[(i,a,\mu)(j,b,\nu)]$

or both $[\lambda(i,a,\mu)](j,b,\nu)$ and $\lambda[(i,a,\mu)(j,b,\nu)]$ are zero. Hence, $\lambda \in \Lambda(S)$ and by (1) $f(\lambda) = (\alpha,\varphi)$, so f is onto. Therefore f is an isomorphism of $\Lambda(S)$ onto $\mathcal{F}(I)\text{wl}D$.

Let X be a nonempty set and D a monoid.For the functions ψ and ψ' , written on the right,from subsets of X into D , define their product by

$$x(\psi\cdot\psi') = (x\psi)(x\psi')$$

for all $x \in \text{dom}\psi \cap \text{dom}\psi'$.

If $\mathcal{F}'(X)$ is the semigroup of all partial transformations on X written on the right,then for $\beta \in \mathcal{F}'(X)$ and ψ as before, define ${}^{\beta}\psi$ as function

$$x\,{}^{\beta}\psi = (x\beta)\psi$$

for all $x \in \text{dom}\beta$ such that $x\beta \in \text{dom}\psi$.

Definition 2. Let D be a monoid and Q a subsemigroup of $\mathcal{F}'(X)$. Then the right wreath product of D and Q , denoted by $DwrQ$, is the set

$$\{(\psi,\beta) : \psi : \text{dom}\beta \longrightarrow D ,\ \beta \in Q\}$$

together with multiplication

$$(\psi,\beta)(\psi',\beta') = (\psi\cdot{}^{\beta}\psi', \beta\beta') .$$

The proofs of the next theorems are omitted,and will be given in detail elsewhere.

THEOREM 2. Let $S = M^{\circ}(I,D,M,P)$. Then the function g defined by $\rho g = (\psi,\beta)$, ($\rho \in P(S)$, where $P(S)$ is the set of all right translations of S) ,where $\text{dom}\beta = \text{dom}\psi = \{\mu \in M : (i,1,\mu) \neq 0\}$, $(i,1,\mu)\rho = (i,\mu\psi,\mu\beta)$ if $\mu \in \text{dom}\beta$ is an isomorphism of $P(S)$ onto $Dwr\,\mathcal{F}'(M)$.

The translational hull of S is denoted by $\Omega(S)$.

THEOREM 3. Let $S = M^{\circ}(I,D,M,P)$ and let $f\lambda = (\alpha,\varphi)$ and $\rho g = (\psi,\beta)$. Then $(\lambda,\rho) \in \Omega(S)$ if and only if the following conditions hold:For any $i \in I$, $\mu \in M$,

(i) $i \in \text{dom}\alpha$, $p_{\mu(\alpha i)} \neq 0$ iff $\mu \in \text{dom}\beta$, $p_{(\mu\beta)i} \neq 0$

(ii) $p_{\mu(\alpha i)}(\varphi i) = (\mu\psi)p_{(\mu\beta)i}$ if $i \in \text{dom}\alpha$, $p_{\mu(\alpha i)} \neq 0$.

Further, for $(\lambda,\rho) \in \Omega(S)$, we have $\lambda = 0$ iff $\rho = 0$.

For (α,φ) and (ψ,β) asin Definition 1. and 2. , for the sake of convenience,we let

$$\operatorname{rank}(\alpha,\varphi) = \operatorname{rank}\alpha \ , \quad \operatorname{rank}(\psi,\beta) = \operatorname{rank}\beta \ .$$

The semigroup of all bitranslations of S is denoted by $\Pi(S)$.

THEOREM 4. <u>Let</u> $S = M^{\circ}(I,D,M,P)$. <u>For</u> $0 \neq (\lambda,\rho) \in \Omega(S)$, <u>we have</u> $(\lambda,\rho) \in \Pi(S)$ <u>if and only if</u> $\operatorname{rank} f\lambda = \operatorname{rank} \rho g = 1$.

REFERENCES

1. M.Petrich,<u>Introduction to semigroups</u>,Columbus,Ohio,1973.

INSTITUT ZA MATEMATIKU
Prirodno-matematičkog fakulteta
Univerziteta u Novom Sadu
21001 Novi Sad,p.o.b.224
Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

BI - AND QUASI-IDEAL SEMIGROUPS WITH n-PROPERTY

S.Bogdanović, P.Kržovski, P.Protić, B.Trpenovski

We give a structure description for each semigroup belonging to the classes in the title which we define in a similar way as it was done in /3/ for left-ideal semigroups with n-property.

1. SOME PRELIMINARY RESULTS

Let S be a semigroup. We shall denote by E_s the set of idempotents of S.

THEOREM 1. *A semigroup S is periodic and the mapping $\varphi: S \rightarrow E_S$, defined by $\varphi(x)=e_x$ where e_x is the idempotent in $\langle x \rangle$, is a homomorphism iff for every $a,b \in S$, $n \in N$ there exists $r \in N$ such that $(ab)^r=(a^n b^n)^r$ and $E_S^2=E_S$.*

Proof. Let S be a periodic semigroup and φ a homomorphism, where φ is defined as above. Then $\ker\varphi$ is a congruence with the congruence classes

$$K_e=\{x \in S \mid (n \in N)\ x^n=e\}, \quad e \in E$$

which are power joined semigroups. Hence, according to Theorem 1 /7/, it follows that for every $a,b \in S$, $n \in N$ there exists $r \in N$ such that $(ab)^r=(a^n b^n)^r$. Furthermore since φ is an epimorphism, we have that $S/\ker\varphi = E_s$ which implies that $E_S^2=E_S$.

Conversely, for every $a,b \in S$, $n \in N$ let there be on $r \in N$ such that $(ab)^r=(a^n b^n)^r$; then $a^{2r}=a^{2nr}$ and S is periodic. If we put

$$a \rho b \overset{def}{\Longleftrightarrow} (\exists n \in N)\ a^n=b^n$$

then ρ will turn out to be a band congruence and the congruence classes mod ρ will be periodic unipotent power joined semigroups (/7/ Theorem 1), and then the mapping φ defined by $\varphi(x)=e_x$ will be an epimorphism from S onto E_S.

COROLLARY 1. *A semigroup S is periodic, E_S a rectangular band and $\varphi: S \rightarrow E_S$ ($\varphi(x)=e_x$) a homomorphism iff for every $a,b,c \in S$, $n \in N$ there exists an $r \in N$ such that $(abc)^r=(ac)^{nr}$, $E_S^2=E_S$.*

Proof. Follows from (/7/ Theorem 3) and (/7/, Theorem 1).

Let S be a semigroup with zero 0; we call S a nil-semigroup iff for every $a \in S$ there is an $n \in N$ such that $a^n=0$.

LEMMA 1. A semigroup S is a nil-semigroup iff for every $a,b \in S$ there is an $n \in N$ such that $a^n=b^{n+1}$.

Proof. If S is a nil-semigroup then the statement in the Lemma 1 is obvious.

Conversely, for every $a,b \in S$ let there be an $n \in N$ such that $a^n=b^{n+1}$. Then for a=b we have that $a^n=a^{n+1}$ which implies that a^n is an idempotent; furthermore, from $a^n=a^{n+1}$ it follows that a^n is the zero in $\langle a \rangle$. Let us show that a^n is zero in S; let $b \in S$ is an arbitrary element. From the above discussion it follows that for same $k \in N$, b^k is zero in $\langle b \rangle$. Now, there exists an $m \in N$ such that $(a^n)^m=(b^k)^{m+1}$ and, since a^n, b^k are idempotents we have that $a^n=b^k$ which means that a^n is zero for b. So, S has a zero and is a nil-semigroup.

THEOREM 2. A semigroup S is a band of nil-semigroups iff the following properties are satisfied:

1. $(\forall x \in S)(\exists r \in N)\ x^r=x^{r+1}$,
2. $(\forall x,y \in S)\ (\forall n \in N)(\exists r \in N)\ (xy)^r=(x^n y^n)^r$.

Proof. Let S be a band Y of nil-semigroups S_α, $\alpha \in Y$. Then according to Lemma 1 we have that 1 is satisfied. Since every nil-semigroup is a power joined semigroup, if follows that 2 is satisfied too /7, Th.1/.

Conversely, let the conditions 1 and 2 be satisfied. Then S will be a band Y of periodic power joined semigroups S_α, $\alpha \in Y$ /7, Th.1/. So, for $a,b \in S_\alpha$, $\alpha \in Y$, we have that $a^n=b^n$, $b^k=b^{k+1}$ for some $n,k \in N$ and,

$$a^{nk}=b^{nk}=b^{nk-k}b^k = b^{nk+1}$$

which, according to Lemma 1, implies that S_α is a nil-semigroup.

Let E be a band, P a partial semigroup, $E \cap P=\emptyset$, and $\varphi:P \to E$ a partial homomorphism. Let us extend φ to a mapping $\psi:S=E \cup P \to E$ by $\psi(x)=\varphi(x)$ if $x \in P$ and $\psi(e)=e$ for all $e \in E$. Let us define an operation on S by

$$xy = \begin{cases} xy \text{ as in } P, \text{if } x,y \in P \text{ and } xy \text{ is defined in } P \\ \psi(x)\psi(y), \text{otherwise} \end{cases}$$

Then S will become a semigroup with E an ideal and ψ an epimorphism. In what follows we shall denote the semigroup S constructed above by $S=(E,P,\varphi)$.

A partial semigroup P is said to be a power breaking partial semigroup iff for every $x \in P$ there exists a $k \in N$ such that x^k is not defined in P.

THEOREM 3. The following conditions on a semigroup S are equivalent:

(i) S is periodic, $\varphi:S \to E_S$ $(\varphi(x)=e_x)$ is a homomorphism and $(\forall x \in S)$ $(\forall e \in E_S)$ $xe, ex \in E_S$;

(ii) $(\forall a,b\in S)(\forall n\in N)(\exists r\in N)\ (ab)^r=(a^nb^n)^r$ and $(\forall x\in S)(\forall e\in E)\ xe,ex\in E_s$;

(iii) $S\cong(E,P,\varphi)$ where P is a power breaking partial semigroup.

Proof. From Theorem 1 it follows that (i) ⇒ (ii). If (ii) is true, from the proof of Theorem 1 it follows that S is periodic and, since $xe,ex\in E_s$ for every $x\in S$, $e\in E_s$, we have that E_s is an ideal in S. So, if we put $P=S\setminus E$, we will have that P is a partial power breaking semigroup. According to Theorem 1, the mapping $\varphi|_P(\varphi(x)=e_x)$ will be a partial homomorphism from P to E_s suchthat $\varphi(e)$ = for all $e\in E_s$. So, we have that $S\cong(E,P,\varphi)$ and we have proved that (ii) ⇒ (iii). It is obvious that (iii) ⇒ (i).

2. BI-IDEAL SEMIGROUPS WITH n-PROPERTIES

A subsemigroup B of a semigroup S is said to be a bi-ideal iff $BSB\subseteq B$. The principal bi-ideal $B[a]$ of a semigroup S generated by $a\in S$ is $B[a]=a\cup a^2\cup aSa$.

A semigroup S is said to be a c-bi-ideal semigroup iff every cyclic subsemigroup $\langle a\rangle$ of S is a bi-ideal of S.

THEOREM 4. The following conditions on a semigroup S are equivalent:

(i) S is a c-bi-ideal semigroup;

(ii) $(\forall a\in S)\ aSa\subseteq\langle a\rangle$;

(iii) $(\forall a\in S)\ \ B[a]=\langle a\rangle$.

Proof. From $aSa\subseteq\langle a\rangle S\langle a\rangle\subseteq\langle a\rangle$ it follows that (i) ⇒ (ii). It is obvious that (ii) ⇒ (iii). Let (iii) be satisfied and let $\langle b\rangle$ be a cyclic subsemigroup of S. Then for $b^i,b^j\in\langle b\rangle$ we have that

$$b^iSb^j=b^{i-1}bSbb^{j-1}\subseteq b^{i-1}B\ b\ b^{j-1}=$$
$$=b^{i-1}\langle b\rangle b^{j-1}\subseteq\langle b\rangle,$$

and so, $\langle b\rangle S\langle b\rangle\subseteq\langle b\rangle$ which means that S is a c-bi-ideal semigroup.

Let us recall that S is a bi-ideal semigroup iff every subsemigroup of S is a bi-ideal in S ([2]) and that the bi-ideal $B[C]$ generated by the non-empty subset C of the semigroup S is $B[C]=C\cup C^2\cup CSC$. In a simmilar way as in the case of Theorem 4, the following can be proved:

THEOREM 5. The following conditions on a semigroup S are equivalent:

(i) S is a bi-ideal semigroup;

(ii) $CSC\subseteq\langle C\rangle$ for every non-empty subset C of S;

(iii) $B[C]\subseteq\langle C\rangle$.

A partial subsemigroup R of a partial semigroup P is a bi-ideal in P iff r_1pr_2 is defined in P, $r_1,r_2\in R$, $p\in P$ implies $r_1pr_2\in R$. If every partial subsemigroup of a partial semigroup P is a bi-ideal in P, we call P a partial bi-ideal semigroup.

THEOREM 6 [2]. A semigroup S is a bi-ideal semigroup iff $S \cong (E,P,\varphi)$ where E is a rectangular band and P a partial power breaking bi-ideal semigroup.

We call partial semigroup P a partial c-bi-ideal semigroup iff whenever apa is defined in P, apa $\in \langle a \rangle$ where $\langle a \rangle$ consists of all powers a^n which are defined in P. In a similar way as Theorem 6, the following can be proved:

THEOREM 7. A semigroup S is a c-bi-ideal semigroup iff $S \cong (E,P,\varphi)$ where E is a rectangular band and P a partial power breaking c-bi-ideal semigroup.

It is obvious that the class of c-bi-ideal semigroups is more general than the class of bi-ideal semigroup.

Let S be a semigroup and Q a subset of S. We call S a

(i) β_0^n - semigroup iff $Q \subseteq S$, $Q^{n+1} \subseteq Q \Rightarrow QSQ \subseteq Q$;

(ii) β_1^n - semigroup iff $Q \subseteq S$, $Q^{n+1} \subseteq Q \Rightarrow QS^{n-1}Q \subseteq Q$;

(iii) β_2^n - semigroup iff $Q \subseteq S$, $Q^2 \subseteq Q \Rightarrow QS^{n-1}Q \subseteq Q$.

Observe that for n=1 β_0^n -, β_2^n - semigroups are simply bi-ideal semigroups. It is easily seen that:

LEMMA 2. Every subsemigroup and every homomorphic image of a β_0^n-, β_1^n - semigroup is also a β_0^n-, β_1^n-, β_2^n-semigroup, respectively.

LEMMA 3. (i) Every β_0^n-semigroup is a β - semigroup;

(ii) every β - semigroup is a β_2^n-semigroup;

(iii) every β_1^n-semigroupis a β_2^n - semigroup,

where β- semigroup stands for bi-ideal semigroup.

LEMMA 4. Let S be a semigroup. If S is a β-β_0^n-semigroup then $aSa \subseteq \langle a \rangle$ for every $a \in S$; if S is a β_1^n-, β_2^n-semigroup then $aS^{n-1}a \subseteq \langle a \rangle$ for every $a \in S$.

LEMMA 5. Let S be a β_0^n-, β_1^n-semigroup. Then:

(i) S is periodic; and for every $a \in S$ the periodic part H_a of $\langle a \rangle$ is a trivial subgroup of S;

(ii) E is a rectangular band which is an ideal in S; for every $e \in E$, $x \in S$, exe=e;

(iii) if xyx=x for some $y \in S$, then $x \in E$.

LEMMA 6. (i) If S is a β-semigroup, then $|\langle a \rangle| \leqslant 5$ for every $a \in S$;

(ii) if S is a β_0^n-semigroup, then $|\langle a \rangle| \leqslant 3$ for every $a \in S$;

(iii) if S is a β_1^n-, β_2^n-semigroup, then $|\langle a \rangle| \leqslant n+3$ for every a S.

Proof. Let, for example, S be a β_1^n-semigroup, $a \in S$ and let $\langle a \rangle_n = \{a, a^{n+1}, a^{2n+1}, \ldots\}$ be the n-subsemigroup of S generated by a. Since

$$a^{n+2} = a.a^2.a^{n-2}.a \in \langle a \rangle_n S^{n-1} \langle a \rangle_n \subseteq \langle a \rangle_n,$$

we have that $a^{n+2}=a^{kn+1}$ for some $k\in N$, which means that the index r_a of a is $\leqslant n+2$ and, since the periodic part of $\langle a\rangle$ consists of one element (Lemma 5 (i)), we have that $|\langle a\rangle|\leqslant n+3$.

Let P be a partial semigroup. Then P is said to be a: (i) β_0^n-semigroup iff for every $Q\subseteq P$ which posseses the property $q_0q_1\dots q_nq\in Q$, $q_j\in Q$ whenewer $q_0q_1\dots q_n$ is defined in P we have that, if $q_1^*pq_2^*$ is defined in P, then $q_1^*pq_2^*\in Q$, $q_1^*,q_2^*\in Q$, $p\in P$; (ii) β_1^n-semigroup iff for every $Q\subseteq P$ which possesses the property mentioned in (i), $q_1^*p_1p_2\dots p_{n-1}q_2^*$ defined in P implies $q_1^*p_1p_2\dots p_{n-1}q_2^*\in Q$; (iii) β_2^n-semigroup iff for every $Q\subseteq P$ such that whenever q_1q_2 is defined in P, if $q_1q_2\in Q$ then the following is true: if $q_1^*p_1p_2\dots p_{n-1}q_2^*$ is defined in P then $q_1^*p_1p_2\dots p_{n-1}q_2^*\in Q$, $q_1^*,q_2^*\in Q$, $p_j\in P$.

THEOREM 8. <u>A semigroup S is a β_0^n-semigroup iff $S\cong(P,E,\varphi)$ where E is a rectangular band and P a partial power breaking β_0^n-semigroup</u>.

<u>Proof</u>. Let S be a β_0^n-semigroup. From Lemma 5 it follows that $S=E\cup P$ ($P=S\setminus E$) where E is a rectangular band and ideal in S, and P is a power breaking partial semigroup. Let $Q\subseteq P$ possess the property $q_0q_1\dots q_n\in Q$ whenever $q_0q_1\dots q_n$ is defined in P, $q_i\in Q$ and let $Q^*=Q\cup E$. Then $Q^{*n+1}\subseteq Q^*$; since S is a β_0^n-semigroup, it follows that $Q^*SQ^*\subseteq Q^*$. If $q_1^*,q_2^*\in Q$, $q_1^*pq_2^*\notin E$, we conclude that $q_1^*pq_2^*\in Q$ which proves that P is a partial β_0^n-semigroup. Finally, if we put $\varphi(x)=e_x$, e_x is the idempotent in $\langle x\rangle$, we can easily show that $\varphi:P\to E$ is a homomorphism (as in [2] and by Theorem 3 we have that $S\cong(E,P,\varphi)$.

Conversely, let $S\cong(E,P,\varphi)=T$ with E,P as stated in the Theorem and let $B\subseteq T$, $B^{n+1}\subseteq B$. Then $B^*=B\setminus E$ posseses the property $b_0b_1\dots b_n\in B^*$ whenever $b_0b_1\dots b_n$ is defined in P, so, if $b,c\in B^*$, $p\in P$, then $bpc\in B^*\subseteq B$. Let for $b,c\in B$, $t\in T$, $btc\in E$. If $bc\notin B^*$, then b.c is not defined in P and,

$$btc=\varphi(b)\varphi(t)\varphi(c)=\varphi(b)\varphi(c)=[\varphi(b)]^n\varphi(c)=\varphi(b^n)\varphi(c)=b^nc\in B.$$

If $bc\in P$ then $(bc)^k\in E$ since P is a power breaking partial semigroup. Let $(bc)^k=e$, then

$$btc=\varphi(b)\varphi(t)\varphi(c)=\varphi(b)\varphi(c)=\varphi(bc)=\varphi[(bc)^k]=e.$$

On the other hand we have that

$$e=\varphi(b)\varphi)c)=\varphi(b^{kn}c)=b^{kn}c\in B^{kn+1}\subseteq B$$

if $b^{kn}\in E$. Now, from $bc\in P$ it follows that $b\in P$ and there exists an $m\in N$ such that b^m is not defined in P; then for $k\in N$, $kn\geqslant m$ we have that $b^{kn}\in E$ since E is an ideal in T. So, we have proved that $btc\in B$ for every $b,c\in B$, $t\in T$, which completes the proof.

In a similar way the following can be proved:

THEOREM 9. *A semigroup S is a β_1^n-semigroup iff $S \cong (E,P,\varphi)$ where E is a rectangular band, P a partial power breaking β_1^n-semigroup.*

THEOREM 10. *A semigroup S is a β_2^n-semigroup iff $S \cong (E,P,\varphi)$ where E is a rectangular band and P a partial power breaking β_2^n-semigroup.*

3. QUASIIDEAL SEMIGROUPS WITH n-PROPERTY

In a similar way as in part 2 we can introduce the following classes of semigroups: We call a semigroup S:

(i) q_0^n-semigroup iff $Q \subseteq S$, $Q^{n+1} \subseteq Q \Rightarrow QS \cap SQ \subseteq Q$;

(ii) q-semigroup iff $Q \subseteq S$, $Q^2 \subseteq Q \Rightarrow QS \cap SQ \subseteq Q$;

(iii) q_1^n-semigroup iff $Q \subseteq S$, $Q^{n+1} \subseteq Q \Rightarrow QS^n \cap S^nQ \subseteq Q$;

(iv) q_2^n-semigroup iff $Q \subseteq S$, $Q^2 \subseteq Q \Rightarrow QS^n \cap S^nQ \subseteq Q$

We are not going to reformulate all the results for the semigroups defined above; these results are similar to those in 2. We shall do this only for some of these semigroups, including the theorems which give a structure description for each of these semigroups.

LEMMA 7. *Let S be a semigroup.*

(i) *If S is a q-semigroup, then* $|\langle a\rangle| \leqslant 3$ *for every* $a \in S$;

(ii) *if S is a* q_0^n*-semigroup, then* $|\langle a\rangle| \leqslant 2$ *for every* $a \in S$;

(iii) *if S is a* q_1^n-, q_2^n*-semigroup, then* $|\langle a\rangle| \leqslant n+2$ *for every* $a \in S$.

THEOREM 11. *A semigroup S is a q_0^n-semigroup iff $S \cong (E,P,\varphi)$ where E is a rectangular band, P a nonempty set and $\varphi : P \to E$ a mapping.*

Proof. Since every quasiideal of a semigroup is a bi-ideal tool, it follows that a q_0^n-semigroup is a β_0^n-semigroup too. So, we can use all the properties which a β_0^n-semigroup possesses. Let S be a q_0^n-semigroup, $x,y \in S$ and let $Q=\{x,y,e_x,e_y,e_x e_y,e_y e_x\}$. We shall show that $Q^{n+1} \subseteq Q$. For n=2 we have the following possibilities: (i) if in q=abc all of a,b and c are idempotents, then (E is a rectangular band and $ex, xe \in E$ by Lemma 5) $q=e_xe_y, e_ye_x, e_x, e_y$; $q=ac=e_xe_y$ if $a=e_x$, $c=e_y$. (ii) if one of a,b and c is idempotent, for example if b is idempotent, then ab and bc will be idempotents also and $q=abc=a.bcb=ab.cbc=abe=abab.e_c=e_abe_c=e_ae_c$ and again $q \in Q$; (iii) since $x^2=e_x$, $y^2=e_y$ (Lemma 7 (ii)), the product q=abc doesn't contain any idempotent in the following two cases: $q=xyx=e_x$ and $q=yxy=e_y$ since from $xyx \in \langle x\rangle$ if follows that xyx=x (and then x is idempotent) if $xyx=e_x$ and similar for yxy. So, if n=2 we have proved that $Q^{n+1} \subseteq Q$. Now, let $n>2$; then according to previous considerations, in any product of n+1 elements from Q, the product of any three elements, as we have shown above, will be equal to an idempotent and, accordingly, in a similar way we can prove that all the product is equal to an idempotent which belongs to Q. So, Q will be an n-subsemigroup of S, i.e. $Q^{n+1} \subseteq Q$. From this it follows that Q is a quasiideal in S which implies that Q is a subsemigroup of S; we have proved that $xy \in Q$. If $xy=y$ then $y=xy=x^2y=e_xy=e_xy=e_xe_y$ which is impossible if we take x and y not to be idempotents. Similarly for $xy=x$. So, xy must be an idempotent:

$$xy=xyx.y = e_xy=e_x.ye_xy = e_xe_y$$

Now, if we put $P=S\setminus E$, we have that for every $x,y \in P$, $xy \in E$. Furthermore, with $\varphi(x)=e_x$, $x \in P$ and e_x the idempotent in $\langle x\rangle$ we can define a mapping from P to E which can be considered as a partial homomorphism from P to E and Theorem 3 concludes the proof.

Conversely, let $Q \subseteq T = E \cup P$ where E is a rectangular band, P a set such that $E\cap P=\emptyset$ and let $\varphi:P \to E$ be a mapping, and let $Q^{n+1} \subseteq Q$. If $x \in QT \cap TQ$, i.e. $x=q_1x_1=x_2q_2$, $q_1,q_2 \in Q$, $x_1,x_2 \in T$, we have that $x \in E$ and, according to the definition of operation in (E,P,φ), we have that

$$x=x^2=q_2x_2x_1q_1= \varphi(q_2)\varphi(x_2)\varphi(x_1)\varphi(q_1)=\varphi(q_2)\varphi(q_1)=\varphi(q_2^n)\varphi(q_1) =$$
$$=\varphi(q_2^nq_1) = q_2^nq_1 \in Q$$

which shows that Q is a quasi-ideal in T.

Let P be a partial semigroup. Then P is said to be a: (i) q-semigroup iff for every $Q \subseteq P$ which posseses the property $q_1q_2 \in Q$ whenever q_1q_2 is defined in P, $q_1,q_2 \in Q$, we have that, if pq is defined in P, $p\in P$, $q\in Q$ and, for some $p'\in P$, $q'\in Q$ $pq=q'p'=x$, then $x\in Q$; (ii) q_1^n-semigroup iff for every $Q \subseteq P$ which posseses the property $q_0q_1\ldots q_n \in Q$ whenever $q_0q_1\ldots q_n$ is defined in P, $q_i \in Q$ we have that, if $p_1p_2\ldots p_nq$ is defined in P for $p_i \in P$, $q \in Q$ and for some $p_i' \in P$, $q' \in Q$, $p_1p_2\ldots p_nq=q'p_1'p_2'\ldots p_n' = x$ then $x \in Q$; (iii) q_2^n-semigroup iff for every $Q \subseteq P$ which posseses the property $q_1q_2 \in Q$, $q_1,q_2 \in Q$, whenever q_1q_2 is defined in P we have that if $p_1p_2\ldots p_nq$ is defined in P, $p_i \in P$, $q \in Q$ and for some $p_i' \in P$, $q' \in Q$, $p_1p_2\ldots p_nq=q'p_1'p_2'\ldots p_n' = x$ then $x \in Q$.

Using a similar procedure as for Theorem 8, and using also Theorem 9 and 10, the following can be proved:

THEOREM 12. <u>A semigroup S is a q-semigroup iff $S \cong (E,P,\varphi)$ where E is a rectangular band and P a partial power breaking q-semigroup.</u>

THEOREM 13. <u>A semigroup S is a q_1^n-semigroup iff $S \cong (E,P,\varphi)$ where E is a rectangular band and P a partial power breaking q_1^n-semigroup.</u>

THEOREM 14. A semigroup S is a q_2^n-semigroup iff $S \cong (E,P,\varphi)$ where E is a rectangular band and P a partial power breaking q_2^n-semigroup.

REFERENCES

[1] Б.Л.Трпеновски, За една класа полугрупи, Год.зборник на ЕМФ, Скопје, 2(1968), 5-8

[2] B.Trpenovski, Bi-ideal semigroups, Algebraic conference,Skopje,1980,109-114

[3] B.Trpenovski, Semigroups with n-properties, Algebraic conference, Novi Sad, 1981, 7-12

[4] П.Кржовски, За би-идеалните полугрупи, Год.зборник на Математички факултет, Скопје, 1979, 29-33

[5] P.Protić, S.Bogdanović, On a class of semigroups, Algebraic conference, Novi Sad, 1981

[6] P.Protić, S.Bogdanović, A structural theorem for (m,n)-ideal semigroups, Proc. Symp. n-ary structures, Skopje,1982.

[7] S.Bogdanović, Bands of power joined semigroups, Acta Sci. Math. Szeged, 44(1982) 3-4

[8] S.Bogdanović, Some characterizations of bands of power joined semigroups, Algebraic conference, Novi Sad, 1981

[9] M.Petrich, Introduction to semigroups, Columbus, Ohio, 1973.

Branko Trpenovski, Pano Kržovski
Univerzitetski centar za matematičko-tehnički nauki
OOZT Matematički fakultet
ul.Orce Nikolov, b.b.
91000 Skopje
Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

(m,n)-IDEAL SEMIGROUPS

S.BOGDANOVIĆ and S. MILIĆ

In this paper the structural theorem for (m,n)-ideal semigroups is given and in this way the results of [2,5,6,7,9,10] are generalized.

A subsemigroup A of a semigroup S is an (m,n)-ideal of S if $A^mSA^n \subseteq A$, where $m,n \in N \cup \{0\}$, $(A^oS = SA^o = S)$, [3]. S is an (m,n)-ideal semigroup if every subsemigroup of S is an (m,n)-ideal of S, [5].

A subset R of a partial semigroup Q is a partial subsemigroup of Q if $x,y \in R$, $xy \in Q$ implies $xy \in R$. A partial subsemigroup R of a partial semigroup Q is an (m,n)-ideal of Q if $R^mQR^n \subseteq R$. If all partial subsemigroups of a partial semigroup Q are (m,n)-ideals in Q, then we call Q a partial (m,n)-ideal semigroup. A partial semigroup Q is power breaking if for every $a \in Q$ there exists $k \in N$ such that $a^k \notin Q$.

For nondefinied notions we refer to [1,8].

<u>CONSTRUCTION.</u> Let $E = I \times J$ be a rectangular band and let Q be a partial (m,n)-ideal $(m,n \geq 1)$ power breaking semigroup such that $E \cap Q = \emptyset$.

Let $\xi : p \to \xi_p$ be a mapping from Q into the semigroup $T(I)$ of all mappings from I into itself and $\eta : p \to \eta_p$ be a mapping from Q into $T(J)$.

For all $p,q \in Q$ let:

(i) $pq \in Q \Rightarrow \xi_{pq} = \xi_q\xi_p$, $\eta_{pq} = \eta_p\eta_q$

(ii) $pq \notin Q \Rightarrow \xi_q\xi_p = \text{const.}$, $\eta_p\eta_q = \text{const.}$

Let us define a multiplication on $S = E \cup Q$ with:

(1) $(i,j)(k,\ell) = (i,\ell)$

(2) $p(i,j) = (i\xi_p, j)$

(3) $(i,j)p = (i, j\eta_p)$

(4) $pq = r \in Q \Rightarrow pq = r \in S$

(5) $pq \notin Q \Rightarrow pq = (i\xi_q\xi_p, j\eta_p\eta_q)$.

Then S with this multiplication is a semigroup, [4,5].

A subsemigroup B of S is of the form $B = E_B \cup Q_B$, where $E_B = I_B \times J_B$ ($I_B \subseteq I$; $J_B \subseteq J$) is a rectangular band and Q_B is a partial subsemigroup of Q.

If for $p,q \in Q_B$, $p \in Q_B^m$, $q \in Q_B^n$ the following conditions hold:

(iii) $\xi_p : I \to I_B$, $\eta_q : J \to J_B$

then a semigroup which is constructed in this way will be denoted by $M(I,J,Q,\xi,\eta)$.

Let us quote some of the results from [5].

LEMMA. *Let S be an (m,n)-ideal semigroup. Then*

1° *S is periodic;*

2° *The set E of all idempotents of S is a rectangular band and it is an ideal of S;*

3° *$S \setminus E$ is a partial power breaking semigroup;*

4° *Any subsemigroup of S is an (m,n)-ideal subsemigroup of S.*

THEOREM. *S is an (m,n)-ideal $(m,n \geq 1)$ semigroup if and only if S is isomorphic to some $M(I,J,Q,\xi,\eta)$.*

Proof. Let S be an (m,n)-ideal semigroup. Then by Lemma and by Theorem 1.1. [4] (see also Theorem 1.1. [5]) we have that S is isomorphic to a semigroup from the above construction with (i), (ii) and (1)-(5). We shall show that the condition (iii) holds. Assume that B is a subsemigroup of S. Then $B = I_B \times J_B \cup Q_B$ ($I_B \subseteq I$; $J_B \subseteq J$). For $p,q \in Q_B$, $p \in Q_B^m$, $q \in Q_B^n$ and arbitrary $(i,j) \in I \times J$ we have that

$$p(i,j)q \in B^m S B^n \subseteq B$$

$$p(i,j)q \in E = I \times J$$

(since E is an ideal of S), so

$$p(i,j)q \in B \cap E = E_B = I_B \times J_B .$$

Hence,

$$p(i,j)q = (i\xi_p, j\eta_q) \in I_B \times J_B$$

i.e.

$$\xi_p : I \to I_B \,, \quad \eta_q : J \to J_B$$

so the condition (iii) holds.

Conversely, let $S = M(I,J,Q,\xi,\eta)$ and let B be a subsemigroup of S. Then $B = E_B \cup Q_B$, where $E_B = I_B \times J_B$ ($I_B \subseteq I$; $J_B \subseteq J$) is a rectangular band and Q_B is a partial subsemigroup of Q.

It is clear that

(6) $$B^m S B^n = E_B S E_B \cup Q_B^m S E_B \cup E_B S Q_B^n \cup Q_B^m S Q_B^n \,.$$

E_B is a bi-ideal of $E = I \times J$, so

(7) $$E_B S E_B = E_B^2 S E_B^2 \subseteq E_B E S E E_B \subseteq E_B E E_B \subseteq E_B \,.$$

Consider first the term $Q_B^m S E_B$. Assume that $b \in Q_B^m$, $s \in S$, $c \in E_B$. Then $bsc \in E$. Let $c = (i,j) \in I_B \times J_B$. We have the following cases:

(8.1) $bs \notin E$, $b \in Q_B$, $s \notin E$.

Then $sc = (i',j)$ and by (iii) we have $bsc = b(i',j) = (i'\xi_b, j) \in E_B$.

(8.2) $bs \in E$, $b \notin E$, $s \in E$.

Then $s = (k,\ell)$ and

$$bsc = (k\xi_b, \ell)c = (k\xi_b, \ell)(i,j) = (k\xi_b, j) \in E_B \,.$$

(8.3) $bs \in E$, $b \notin E$, $s \notin E$.

Then $sc = (i\xi_s, j)$ and

$$bsc = b(i\xi_s, j) = (i\xi_s\xi_b, j) \in E_B$$

(8.4) $bs \in E$, $b \in E$. Similarly to the case (7).

Since there are no other possibilities we conclude:

(8) $$Q_B^m S E_B \subseteq E_B \subseteq B \,.$$

Similarly we have that

(9) $$E_B S Q_B^n \subseteq B.$$

Consider the term $Q_B^m S Q_B^n$ and let $b \in Q_B^m$, $s \in S$, $c \in Q_B^n$. If $bsc \in Q$,

$bsc \in Q_B^m Q Q_B^n \subseteq Q_B \subseteq B$

since Q is a partial (m,n)-ideal semigroup. If $bsc \in E$, then we have the following cases:

(10.1) $b \in E_B$. Similarly to the case (9).

(10.2) $b \in E_B$, $s \in E$, $c \in E_B$.

Then $s = (k,\ell)$, $c = (i,j)$ and

$$bsc = (k\xi_b,\ell)c = (k\xi_b,j) \in E_B .$$

(10.3) $b \notin E$, $s \in E$, $c \in Q_B$.

Then $s = (k,\ell)$ and

$$bsc = (k\xi_b,\ell)c = (k\xi_b,\ell\eta_c) \in I_B \times J_B = E_B$$

(10.4) $b \notin E$, $s \notin E$, $c \in E_B$. See (8.3).

(10.5) $b \notin E$, $s \notin E$, $c \notin E$, $bs \in E$.

We may take that $bs = (i\xi_s\xi_b, j\eta_b\eta_s)$ and so

$$bsc = (i\xi_s\xi_b, j\eta_b\eta_s\eta_c) \in E_B .$$

(10.6) $b \notin E$, $s \notin E$, $c \notin E$, $bs \notin E$.

then

$$bsc = (i\xi_c\xi_{bs}, j\eta_{bs}\eta_c) = (i\xi_c\xi_s\xi_b, j\eta_{bs}\eta_c) \in E_B .$$

Since there are no other possibilities, we conclude

(10) $$Q_B^m S Q_B^n \subseteq B.$$

By (6),(7),(8),(9) and (10) we have $B^m S B^n \subset B$, i.e. S is an (m,n)-ideal semigroup.

In the special case, if $m,n \geq 1$, then we have the following:

THEOREM. S _is a_ (0,n)-_ideal_ ((m,0)-_ideal_) _semigroup if and only if_ S _is isomorphic to some_ $M(I,J,Q,\xi,\eta)$, _where_ $|I| = 1$ (_and_ Q _is a partial_ (0,n)-_ideal semigroup_ ($|J| = 1$ _and_ Q _is a partial_ (m,0)-_ideal semigroup_).

If S is a (0,0)-ideal semigroup, then S is trivial.

R E F E R E N C E S

[1] Howie,J.: An Introdiction to Semigroup Theory, Acad. Press 1976.

[2] Kimura,N. and T.Tamura and R.Merkel: Semigroups in which all subsemigroups are left ideals, Canad. J.Math. 17(1965), 52-62.

[3] Lajos,S.: Generalized ideals in semigroups, Acta Sci. Math. 22(1961), 217-222.

[4] Milić,S. and V.Pavlović: Semigroups in which some ideal is a completely simple semigroup, Publ. Inst. Math. 30(44), (1981) 123-130.

[5] Protić,P. and S.Bogdanović: On a class of semigroups, Algebraic conference Novi Sad, 1981, 113-119.

[6] Protić,P. and S.Bogdanović: A structural theorem for (m,n)-ideal semigroups, Proc. Symp. n-ary structures, Skopje, 1982, 135-139.

[7] Shutov,E.G.: Semigroups with ideal subsemigroups, Math. Sbornik, 57 (1962), 179-186 (in Russian).

[8] Steinfeld,O.: Quasi-ideals in rings and semigroups, Akadémiai Kiadó, Budapest 1978.

[9] Trpenovski,B.: Bi-ideal semigroups, Algebraic conference, Skopje 1980. 109-114.

[10] Trpenovski,B.: Semigroups with n-properties, Algebraic conference , Novi Sad, 1981, 7-12.

Institut za matematiku
Ilije Djuričića 4
21000 Novi Sad
Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

EQUATIONAL REFORMULATION OF THE HEYTING FIRST-ORDER PREDICATE CALCULUS

Branislav R. Boričić

According to the paper [4] of A. G. Dragalin, the uniform algebras (abbreviated UA) - algebraic analogue of the Heyting first-order predicate calculus I - are a special case of pseudo-Boolean algebras (abbreviated PBA) (v. [8]), where we have two additional unary operations corresponding to the universal and existential quantifiers and the explicit treatment of substitution. In other words, UA are algebraic structures similar to cylindric (v. [6]) and poliadic (v. [5]) algebras. At the same time UA are a generalization of the notion of functional Brouwerian algebras defined in [3].

On the other hand, a possibility of assignment of an equational formal theory, denoted by $T(\sim)$, to any formal theory T, is given in the paper [7] of S. B. Prešić. The theory $T(\sim)$ is defined axiomatically in such a way that the symbol $\sim$ is a formalization of the equiconsequence (or interdeducibility) relation of T (v. Theorem 1, [7]). If the conditions (i) $A\wedge B\vdash_T A$; $A\wedge B\vdash_T B$ and $A,B\vdash_T A\wedge B$, and (ii) $A\vdash_T B$ iff $\vdash_T A\rightarrow B$, are satisfied for some connectives $\wedge$ and $\rightarrow$ which are definable in T, then the formal theory $T(\sim)$, which we call an equational reformulation of T, is of particular importance for the algebraic model theory.

In this paper we will point at the connections between uniform algebras and equational reformulation $I(\sim)$ of the Heyting first-order predicate calculus I (formulated as in [1] p. 434).

In a similar way as in [6], where the cylindric algebra of formulas is introduced, we can consider the uniform algebra of formulas: UA(For)=(For, $\leqslant$, Ind, Sub), where For is the set of the first-order formulas, Ind - the set of individual constants of the first-order language and Sub - substitution of terms for the variables in elements of For.

THEOREM. $\vdash_{I(\sim)} A\sim B$ *iff* $A\approx B$ *in* UA(For).

For the propositional part of the Heyting calculus, a similar assertion has been given in [2], and leaning on it we will consider only those axioms which are related to the quantifiers.

LEMMA 1. *Let* $A,B\in$ For *and* $1\approx(\mathrm{def})A\to A$. *Then the conditions*

(1) $\forall xA\wedge\forall xB\leqslant\forall x(A\wedge B)$

(2) $\forall x(A\to B)\to(\forall xA\to\forall xB)\approx 1$

(3) $\forall x(A\to B)\to(\exists xA\to\exists xB)\approx 1$

(4) $A\to\forall xA\approx 1$ (x *is not free in* A)

(5) $\exists xA\to A\approx 1$ (x *is not free in* A)

(6) $\forall xA\to A(x/t)\approx 1$ (t *is any term free for* x *in* A)

(7) $A(x/t)\to\exists xA\approx 1$ (t *is any term free for* x *in* A)

(8) $1\wedge\forall x1\approx 1$

are satisfied in UA(For).

Proof. (1) $\forall xA\wedge\forall xB\leqslant\forall xA$ (provable in PBA)

$\forall xA\leqslant A(x/y)$ (by [4], 2.1.7))

Herefrom, by transitivity, $\forall xA\wedge\forall xB\leqslant A(x/y)$. Similarly: $\forall xA\wedge\forall xB\leqslant$ $\leqslant B(x/y)$, and $\forall xA\wedge\forall xB\leqslant A(x/y)\wedge B(x/y)\leqslant(A\wedge B)(x/y)$ (by [4], 2.1.6) and 2.1.3)). From $\forall xA\wedge\forall xB\leqslant(A\wedge B)(x/y)$ follows $\forall xA\wedge\forall xB\leqslant$ $\leqslant\forall x(A\wedge B)$ (by [4], 2.1.7)).

(2) $\forall x(A\to B)\wedge\forall xA\leqslant\forall x((A\to B)\wedge A)$ (by (1))

$\leqslant(A(x/y)\to B(x/y))\wedge A(x/y)$ (by [4], 2.1.7) and b), d) p. 188)

$\leqslant B(x/y)$ (in PBA)

By [4], 2.1.7), we have $\forall x(A\to B)\wedge\forall xA\leqslant\forall xB$, i. e. $\forall x(A\to B)\to(\forall xA\to\forall xB)\approx 1$ (in PBA).

(3) $((A\to B)\wedge A)(x/y)\leqslant B(x/y)\leqslant\exists xB$ (by [4], 2.1.8) and PBA)

$(A\to B)(x/y)\leqslant A(x/y)\to\exists xB$ (in PBA)

$\forall x(A\to B)\leqslant A(x/y)\to\exists xB$ (by [4], 2.1.7))

$A(x/y)\leqslant\forall x(A\to B)\to\exists xB$ (in PBA)

$A(x/y)\leqslant\exists xA\leqslant\forall x(A\to B)\to\exists xB$ (by [4], 2.1.8))

i. e. $\forall x(A\to B)\to(\exists xA\to\exists xB)\approx 1$ (in PBA).

(4) and (5) are immediate consequences of the conditions 7) and 8) of the definition 2.1. [4] of UA.

(6) and (7) are given in [4] as Lemma 2.2.6.

(8) follows from the condition 7) of the def. 2.1. [4], too.⊣

Remark. In general, the conditions (1)-(8) of the LEMMA 1 are satisfied in any UA.

LEMMA 2. Let A and B be the first-order formulas and y a variable which does not occur in the above formulas. Then:

(1) if $\vdash_{I(\sim)} B \sim A(x/y) \& B$, then $\vdash_{I(\sim)} B \sim \forall xA \& B$;

(2) if $\vdash_{I(\sim)} A(x/y) \sim B \& A(x/y)$, then $\vdash_{I(\sim)} \exists xA \sim B \& xA$;

(3) $\vdash_{I(\sim)} \forall xA \sim A(x/y) \& \forall xA$;

(4) $\vdash_{I(\sim)} A(x/y) \sim \exists xA \& A(x/y)$.

Proof. Having in mind that $I(\sim)$ is the equational reformulation of I, it is sufficient to prove that $\vdash B \to \forall xA \wedge B$ follows from $\vdash B \to A(x/y) \wedge B$, and $\vdash \exists xA \to B \wedge \exists xA$ follows from $\vdash A(x/y) \to B \wedge A(x/y)$ (in I) (v. [7], Theorem 3). For instance, we will demonstrate (1). Firstly, by induction on the length of the proof for A in I, we can show that the rule $\frac{\vdash A}{\vdash \forall xA}$ is permissible in I. Then from $\vdash B \to A(x/y) \wedge B$ we have $\vdash \forall y(B \to A(x/y) \wedge B)$, i. e. $\vdash \forall yB \to \forall y(A(x/y) \wedge B)$ (by axiom (9.2) [1] and modus ponens). Further, by axiom (9.4) [1] we have $\vdash B \to \forall y(A(x/y) \wedge B)$, i. e. $\vdash B \to \forall yA(x/y) \wedge B$ (by axiom $\forall yB \to B$ and the known fact that $\vdash \forall x(C(x) \wedge D(x)) \longleftrightarrow \longleftrightarrow \forall xC(x) \wedge \forall xD(x)$ in I).

Similarly, (2), (3) and (4) are immediate consequences of Theorem 3 [7] and known facts about I.⊣

Note that the conditions [(1) and (3)] and [(2) and (4)] are equivalent to the conditions 7) and 8) of the definition of UA [4], respectively. The conditions 9)-17) of this definition are well-known facts which are related to the substitution of variables in the first-order language, and hence in the theory $I(\sim)$.

The above theorem follows immediately from lemmas 1 and 2.

REFERENCES

1. J. Bell, M. Machover, A course in mathematical logic, North-

-Holland, Amsterdam, 1977.

2. B. R. Boričić, Equational reformulations of intuitionictic propositional calculus and classical first-order predicate calculus, Publ. Inst. Math. (Beograd), 29(43)(1981), 23-25.

3. А. Г. Драгалин, Математический интуиционизм - введение в теорию доказательств, Наука, Москва, 1979.

4. А. Г. Драгалин, Алгебраический подход к интуиционистским моделям типа реализуемости, Исследования по неклассическим логикам и теории множеств, Наука, Москва, 1979, 183-201. (See also Math. Rew. 82a:03057.)

5. P. R. Halmos, Algebraic logic, Chelsea, New York, 1962.

6. L. Henkin, J. D. Monk, A. Tarski, Cylindric algebras (Part I), North-Holland, Amsterdam, 1971.

7. S. B. Prešić, Equational reformulation of formal theories, Publ. Inst. Math. (Beograd), 19(33), 1975, 131-138. (See also Math. Rew. 1977:4921.)

8. H. Rasiowa, R. Sikorsky, The mathematics of metamatematics, Państwowe Wydawnictwo Naukowe, Warszawa, 1963.

EKONOMSKI FAKULTET
Kamenička 6
11000 Beograd
Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

ON SOME PROPERTIES OF RINGS IN WHICH $x^n=x$ HOLDS

Blagoje Cerović

In this paper we shall discuss the class of rings $\mathcal{R}_n$, $n>1$, with the property that for every $R\in\mathcal{R}_n$

$$\forall x\in R(x^n=x)$$

holds.

According to the theorem of N.Jacobson, rings from $\mathcal{R}_n$ are commutative and regular since, for every $x\in R$ we have $xx^{n-2}x=x$ for all $n>2$, and $xxx=x$ for $n=2$.

Example 0.1. The ring Z_6 and the fields Z_2 and Z_3 all belongs to $\mathcal{R}_3$ while the field GF(4) belongs to the class $\mathcal{R}_4$.

Example 0.2. For every set S the Boolean ring $(P(S),+,\cdot)$ belongs to $\mathcal{R}_n$ for all $n>1$. If $R\in\mathcal{R}_n$ and if P(S) is the Boolean ring then the ring of the form $R\times P(S)$ belongs to $\mathcal{R}_n$.

The following two lemmas were proved in [1].

Lemma 0.1.([1]). *If $R\in\mathcal{R}_n$ then for all $x\in R$, $(2^n-2)x=0$.*

Lemma 0.2.([1]). *If $R\in\mathcal{R}_n$ is an integral domain then R is a field.*

1. We shall prove that the ring from the class $\mathcal{R}_n$ does not have nonzero nilpotent ideals, i.e. that the class $\mathcal{R}_n$ is the subclass of the class of semisimple rings.

Lemma 1.1. Every ideal of a ring $R \in \mathcal{R}_n$ is idempotent.

Proof. If n=2 then $I^2=I$ for every ideal $I \subseteq R$. If $n>2$ then for all $x \in I$ we have $x^{n-1} \in I$ and so $x=x^{n-1}x \in I^2$, i.e. $I \subseteq I^2$. Since $I^2 \subseteq I$ we have $I^2=I$.

Proposition 1.1. Every ring from $\mathcal{R}_n$ is semisimple.

Proof. Let I be the nilptent ideal of a ring $R \in \mathcal{R}_n$, i.e. the ideal such that for some m, $I^m=0$. According to the previous lemma $I^2=I$ and so $I^m=I$. This means that if I is nilpotent ideal of R then I=0, i.e. that R does not have nonzero nilpotent ideals, or that R is semisimple.⊣

2. In this chapter we shall investigate some properties of the idempotents of the rings from $\mathcal{R}_n$.

Lemma 2.1. If $R \in \mathcal{R}_n$ then for every $x \in R$, x^{n-1} is idempotent.

Proof. If n=2 then R is a Boolean ring so that lemma trivially holds. If $n>2$ then we have

$$x^{n-1}x^{n-1}=x^{2n-2}=x^n x^{n-2}=x^{n-1},$$

i.e. x^{n-1} is an idempotent of R.⊣

The notion of orthogonal idempotents, i.e. the idempotents e_1 and e_2, different from zero, for which $e_1e_2=0$ holds, will be important in our further investigations. For example, using orthogonal idempotents we can give a necessary and sufficient condition for the rings with unit from the class $\mathcal{R}_n$ that are fields.

Proposition 2.1. A ring with unit $R \in \mathcal{R}_n$ is a field if and only if it has no orthogonal idempotents.

Proof. If R is a ring without orthogonal idempotents then R is a ring without zero divisors. To see this assume that for some x,y R that are not zero we have $xy=0$. In that case $x^{n-1}y^{n-1}=0$ and $x^{n-1}\neq 0$ and $y^{n-1}=0$, i.e. x^{n-1} and y^{n-1} are orthogonal idempotents of R which is the contradiction. Trivially, if R is a field then it has no orthogonal idempotents.⊣

Definition 2.1. A set E of pairwise orthogonal idempotents of a ring R is an m-set if there is no idempotent element of R E which is orthogonal to all elements from E.

Lemma 2.2. *If $R\in\mathcal{R}_n$ is a nonzero ring with unit then R is a field or it has orthogonal idempotents (m-sets).*

Proof. Let $R\in\mathcal{R}_n$ be a nonzero ring with unit which is not a field. According to the Lemma 2.1., for every x R that is not zero, x^{n-1} is an idempotent. The elements of the form $1-x^{n-1}$ are not zero since in that case we would have for all $x\in R$, if $x\neq 0$ and $xy=0$ then $x^{n-1}y=0$, and so $y=0$, which means that R is without zero divisors, or that R is a field.

From

$$(1-x^{n-1})^2=1-2x^{n-1}+(x^{n-1})^2=1-x^{n-1},$$

we see that the element $1-x^{n-1}$ is idempotent which with

$$x^{n-1}(1-x^{n-1})=x^{n-1}-(x^{n-1})^2=0$$

means that the idempotents x^{n-1} and $1-x^{n-1}$ are orthogonal.⊣

Lemma 2.3. *Let E be a nonvoid set of pairwise orthogonal idempotents of a ring $R\in\mathcal{R}_n$ and $I_o=\{x\in R:\ xe=0,\ e\in E\}$. Then E is an m-set if and only if $I_o=0$.*

Proof. Assume that E is an m-set and that $I_o\neq 0$, then for nonzero elements $x\in I_o$ we have $x^{n-1}\in I_o$ and $x^{n-1}\neq 0$, (if not, it would be $x=0$). For all $e\in E$ we have that $x^{n-1}\neq e$, since if it is not so we would have that for some $e\in E$, $x^{n-1}=e$ which implies that $e=ee=x^{n-1}e=x^{n-2}xe=0$. Since x^{n-1} is an idempotent which is not in E and for all $e\in E$, $x^{n-1}e=0$ we have that E is not an m-set which is a contradiction. So $I_o=0$.

If $I_o=0$ and $e\in E$ an idempotent orthogonal to every other idempotent from E then $e\in I_o$, i.e. e=0 and so E is an m-set. ⊣

If $e_1,..,e_s$ are pairwise orthogonal idempotents of an arbitrary ring R then R is the direct summ of the ideal I_o and the ideals Re_k, k=1,..,s. In case $R\in\mathfrak{R}_n$, according to the lemma 2.3. we have

Proposition 2.2. *If $E=\{e_1,..,e_s\}$ is an m-set of a ring $R\in\mathfrak{R}_n$ then R is the direct sum of the ideals Re_i, $e_i\in E$.*

3. Definition 3.1. An m-set M of a ring $R\in\mathfrak{R}_n$ is a maximal m-set if for all $e\in M$,in the ideal Re there is no idempotents other than 0 and e.

Example 3.1. The set of all singletons of the Boolean ring P(S) is maximal m-set since for every $a\in S$ the idempotent a generates the ideal $\{A\cap\{a\}: A\in P(S)\}=\{\emptyset,\{a\}\}$.

Proposition 3.1. *Let M be a maximal m-set of a ring $R\in\mathfrak{R}_n$. The ideals of the form Re, $e\in M$, are the only minimal ideals of R.*

Proof. To prove that the ideal Re is minimal it is enough to prove that for every $x\in Re$, Rx=Re ([3]). From the Lemma 2.1 we have that for every $x\in Re$, $x\neq 0$, $x^{n-1}\in Re$ is an idempotent. Since M is a maximal m-set,$x^{n-1}=e$, and so $Re=Rx^{n-1}\subseteq Rx$.

Obviously, $Rx \subseteq Re$ and so $Re=Rx$.

If $I \neq 0$ is a minimal ideal of R different from Re, $e \in M$, then, according to the Proposition 1.1, R is a semisimple ring and I is generated by some idempotent $e' \neq 0$ ([3]). Since I and Re, $e \in M$, are minimal ideals we have that $I \cap Re=0$, and so $e'e=0$ for all $e \in M$. Therefore, e' is orthogonal to all idempotents of the set M. This gives the contradiction with the assumption that M is the maximal m-set.⊣

From the Proposition 3.1 if follows that the maximal m-set of a ring $R \in \mathcal{R}_n$ consists of all idempotents which generates minimal ideals of R.

<u>Corollary 3.1</u>. <u>Maximal m-set of a ring</u> $R \in \mathcal{R}_n$ <u>is unique</u>.

<u>Proposition 3.2</u>. <u>If the maximal m-set</u> M <u>of a ring</u> $R \in \mathcal{R}_n$ <u>is finite then there is no m-set</u> E <u>of</u> R <u>such that</u> $|E|>|M|$.

<u>Proof</u>. Let E be an m-set such that $|E|>|M|$. Since the ideals Re, $e \in M$, are minimal, for every $f \in E$, $Re \cap Rf=0$ or $Re \cap Rf=Re$. Let $E_0=\{f \in E: \exists e \in M(Re \cap Rf=Re)\}$. Since $Rf \cap Rg=0$ for all $f \neq g$, $f,g \in E$, for every $e \in M$ there exists at most one $f \in E$ such that $Re \cap Rf=Re$. Therefore, $|E_0| \leq |M|$, and so there exists $f \in E \setminus E_0$ such that $Re \cap Rf=0$ for all $e \in M$. Since $f \neq e$ and $ef=0$ for all $e \in M$, M is not an m-set. ⊣

<u>Proposition 3.3</u>. <u>If the maximal m-set of a ring</u> $R \in \mathcal{R}_n$ <u>is finite then</u> R <u>is the direct sum of its minimal ideals</u>.

<u>Proof</u>. Follows from the Propositions 2.2 and 3.1.

When the maximal m-set of a ring $R \in \mathcal{R}_n$ is finite it is possible to give a characterization of idempotents of R.

Proposition 3.4. Let $M=\{e_1,..,e_t\}$ *be the maximal m-set of a ring* $R\in\mathcal{R}_n$. *An element* $a\neq 0$ *of R is idempotent iff it is the sum of different elements of M.*

Proof. If a is the sum of elements of M then it is idempotent of R. If a is an idempotent then, since R is the sum of its minimal ideals Re_i, $i=1,..,t$, we have

$$a=r_1e_1+..+r_te_t, \text{ for some } r_i\in R,$$

and so $$r_1^2e_1+..+r_t^2e_t=r_1e_1+...+r_ne_n$$

which after multiplication by e_i gives $r_i^2e_i=r_ie_i$, i.e. $(r\ e_i)^2=r_ie_i$ for all $i=1,..,t$. Therefore, r_ie_i is an idempotent and since M is maximal m-set, $r_ie_i=0$ or $r_ie_i=e_i$, $i=1,..,t$. ⊣

Corollary 3.2. If the maximal m-set of a ring $R\in\mathcal{R}_n$ *has k elements then R has* 2^k *idempotents.*

Proposition 3.5. If a ring $R\in\mathcal{R}_n$ *has finite maximal m-set then it is a ring with unit.*

REFERENCES

1. B. Cerović, *Anti-inverse rings*, Publ. Inst. Math. (Beograd) (N.S.) 29(43)(1981), 45-48.
2. N. Jacobson, *Sructure theory of algebras of bounded degree*, Ann. of Math. 46(1945), 695-707.
3. M. Petrich, *Rings and Semigroups*, Lecture Notes in Math., vol. 380, Springer-Verlag, Berlin-Heidelberg-New York, 1974.

Nastavnički fakultet
81400 Nikšić
Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

A SET OF SEMIGROUP n-VARIETIES

Ǵ. Čupona

Let $\underline{S}=(S;\cdot)$ be a semigroup and $\underline{Q}=(Q;[\,])$ be an n-semigroup such that $Q\subseteq S$ and $[a_1\ldots a_n]=a_1\ldots a_n$, for any $a_\nu\in Q$. Then, $\underline{Q}$ is called an n-subsemigroup of $\underline{S}$. If V is a semigroup variety, then we denote by $V(n)$ the class of n-semigroups that are n-subsemigroups of V-semigroups, and it is well known that $V(n)$ is a quasivariety of n-semigroups. (See, for example [6; p.274], or [3].) We say that V is an n-variety iff $V(n)$ is a variety of n-semigroups; otherwise, i.e. if $V(n)$ is a proper quasivariety, V is called a quasi n-variety. (Clearly, $V(2)=V$ for every semigroup variety). It is well known that both the set of semigroup n-varieties, and the set of semigroup quasi n-varieties are infinite for any $n \geq 3$. The same is true for the varieties of abelian semigroups. (The corresponding results can be found in [1], [7], [8] and [2]). Here we establish a sufficient condition for a semigroup variety to be an n-variety. It is shown that almost all the known n-varieties satisfy that condition, and some new examples are obtained.

0. PRELIMINARIES

<u>0.1</u>. Let $X=\{x_1,x_2,\ldots\}$ be an infinite countable set, elements of which are called variables and let X^+ be the free semigroup on X. Elements of X^+ are called semigroup terms, and if ξ,η are semigroup terms, then (ξ,η) is said to be a semigroup identity. A semigroup $\underline{S}=(S;\cdot)$ satisfies a semigroup identity $(x_{i_1}\cdots x_{i_p},\ x_{j_1}\cdots x_{j_q})$ if for every sequence $a_1,a_2,\ldots$ of elements of S the following equation holds in $\underline{S}$: $a_{i_1}\cdots a_{i_p} = a_{j_1}\cdots a_{j_q}$. If Λ is a set of semigroup identities, then by $\mathrm{Var}\Lambda$ we denote the variety of semigroups which satisfy all the semigroup identities belonging to Λ. The complete system $\langle\Lambda\rangle$ of semigroup identities which are consequences of Λ is the transitive extension of Λ_2, where:

$$\Lambda_o = \Lambda\cup\Lambda^{-1}\cup\{(\xi,\xi)\mid \xi\in X^+\},$$

$$\Lambda_1 = \{(\xi_{i_1}\cdots\xi_{i_p},\xi_{j_1}\cdots\xi_{j_q})\mid(x_{i_1}\cdots x_{i_p},x_{j_1}\cdots x_{j_q})\in\Lambda_o,\ \xi_k\in X^+\},$$

$$\Lambda_2 = \{(\xi_1\cdots\xi_s,\ \eta_1\cdots\eta_s)\mid(\xi_k,\eta_k)\in\Lambda_1,\ s\geq 1\}.$$

(See also [4] or [5].)

If $\xi \in X^+$ and $x_i \in X$, then we denote by $|\xi|_i$ the number of occurences of x_i in ξ, and thus $|\xi| = \Sigma|\xi|_i$ is the length of ξ.

A semigroup term ξ is said to be (n,Λ)-irreducible iff $(\xi,\eta) \in \langle\Lambda\rangle$ implies $|\xi| \equiv |\eta|$ (mod n-1). Otherwise, i.e. if there is a $\zeta \in X^+$ such that $(\xi,\zeta) \in \langle\Lambda\rangle$ and $|\xi| \equiv |\zeta|$ (mod n-1), then ξ is (n,Λ)-reducible.

0.2. To every set Λ of semigroup identities we associate an index $r=\text{ind}\,\Lambda$ and a period $m=\text{per}\,\Lambda$. First, if $|\xi|_i = |\eta|_i$ for every $i \in \{1,2,\dots\}$ and for every semigroup identity $(\xi,\eta) \in \Lambda$, then we write $\text{ind}\Lambda=1$, $\text{per}\Lambda=0$. (Namely, this is satisfied iff the variety of abelian semigroups ABSEM is a subvariety of Var Λ). Assume now that there exists a semigroup identity $(\xi,\eta) \in \Lambda$ and an integer $i \in \{1,2,\dots\}$ such that $|\xi|_i \neq |\eta|_i$. Then, per Λ and indΛ are defined by:

$$\text{per}\Lambda = \text{g.c.d.}\{\,|\,|\xi|_i - |\eta|_i\,|\ (\xi,\eta) \in \Lambda,\ i \in \{1,2,\dots\}\},$$
$$\text{ind}\Lambda = \min\ \{\,|\xi|\ |\ (\exists\eta)\ \ (\xi,\eta) \in \Lambda_1,\ \ |\xi| \neq |\eta|\,\}.$$

It can be easily seen that $\text{ind}\Lambda=\text{ind}\langle\Lambda\rangle$ and $\text{per}\Lambda=\text{per}\langle\Lambda\rangle$, and thus we can say that indΛ(perΛ) is the index (the period) of the variety VarΛ. We notice that if $m=\text{per}\Lambda > 0$ and $r=\text{ind}\Lambda$, then $(x_1^r, x_1^{r+m}) \in \langle\Lambda\rangle$, and moreover if $(x_1^s, x_1^{s+k}) \in \langle\Lambda\rangle$, where $k \geq 1$, then $s \geq r$ and m is a divisor of k.

0.3. Let $\underline{Q}=(Q;[\ ])$ be an n-semigroup. Then the general associative law holds, i.e. for any $k \geq 1$ and $a_0,\dots,a_{k(n-1)} \in Q$, the "product" $[a_0 \dots a_{k(n-1)}]$ is uniquelly determined in Q; we also write $[a] = a$, for every $a \in Q$.

If (ξ,η) is a semigroup identity such that $|\xi| \equiv |\eta| \equiv 1$ (mod n-1) then it can be also interpreted as an n-semigroup identity. And, if every semigroup identity $(\xi,\eta) \in \Lambda$ is an n-semigroup identity, then ve denote by $\text{Var}_n\Lambda$ the variety of n-semigroups which satisfy all the n-semigroup identities $(\xi,\eta) \in \Lambda$.

Assume now that Λ is a set of semigroup identities, and denote by $\Lambda^{[n]}$, the set of n-semigroup identities belonging to $\langle\Lambda\rangle$. It is clear that if $\mathcal{V}=\text{Var}\Lambda$, $\mathcal{V}_n=\text{Var}_n\,\Lambda^{[n]}$, then $\mathcal{V}(n) \subseteq \mathcal{V}_n$. Moreover: $\mathcal{V}$ is an n-variety iff $\mathcal{V}(n) = \mathcal{V}_n$.

1. MAIN RESULT

Theorem. Let $\mathcal{V}=\mathrm{Var}\Lambda$ be a semigroup variety with a period m, and let $n \geq 2$ be such that the following condition is satisfied:

(α) If ξ is an (n,Λ)-reducible semigroup term, then there exist $x,y \in X$ such that $(x^{km}\xi,\xi)$, $(\xi,\xi y^{km}) \in \langle\Lambda\rangle$, for every positive integer k.

Then $\mathcal{V}$ is an n-variety.

The proof will be given in three steps, and the condition (α) will be not assumed in the first two of them.

1.1. Let $\underline{Q}=(Q;[\,])$ be an n-semigroup and let Q_Λ be the free semigroup in $\mathcal{V}$ with a basis Q. Thus, Q is a generating subset of Q_Λ, and if $a_1,a_2,\dots$ is a set of different elements of Q then $a_{i_1}\dots a_{i_p}=a_{j_1}\dots a_{j_q}$ iff $(x_{i_1}\dots x_{i_p}, x_{j_1}\dots x_{j_q}) \in \langle\Lambda\rangle$. Define a relation $\vdash$ in Q_Λ by: $\dots a\dots \vdash \dots a_0\dots a_{k(n-1)}\dots$, where $a=[a_0\dots a_{k(n-1)}]$ in $\underline{Q}$. Let $\vdash\!\dashv$ be the symmetric extension of $\vdash$, and $\approx$ be the transitive extension of $\vdash\!\dashv$. The following two propositions are obvious.

1.1.1. $\approx$ is a congruence on the semigroup Q_Λ.

1.1.2. $\underline{Q} \in \mathcal{V}(n)$ iff the following statement is satisfied:

$$a,b \in Q \Longrightarrow (a \approx b \Longrightarrow a = b).$$

1.2. Assume now that $\underline{Q} \in \mathcal{V}_n=\mathrm{Var}_n\Lambda^{[n]}$, and that Q_Λ, $\vdash$, $\vdash\!\dashv$, $\approx$ are defined as in 1.1. A partial mapping $u \mapsto [u]$ from Q_Λ in Q can be defined in a usual way. Namely, $u \in Q_\Lambda$ is in the domain of $[\ ]$ iff $u=a_0a_1\dots a_{k(n-1)}$, where $a_\nu \in Q$, and then the "value" $[u]$ of u is defined by $[u]=[a_0a_1\dots a_{k(n-1)}]$. The assumption $\underline{Q} \in \mathcal{V}_n$ implies that $[\ ]$ is a well defined partial mapping.

Let $a_1,a_2,\dots$ be different elements of Q, and let $u=a_{i_1}a_{i_2}\dots a_{i_p}$. We say that u is irreducible (reducible) iff the semigroup term $x_{i_1}\dots x_{i_p}$ is (n,Λ)-irreducible ((n,Λ)-reducible).

The following three proposition can be easily shown.

1.2.1. If $u \in Q_\Lambda$ is in the domain of $[\ ]$, then $[u] \vdash u$.

1.2.2. Let u,v Q_Λ be such that $u \vdash\!\dashv v$, and u is irreducible. If u is in the domain of $[\ ]$, then v is also in the domain of $[\ ]$ and moreover $[u]=[v]$.

1.2.3. V is an n-variety iff every $Q \in V_n$ satisfies the following condition. If $u,v \in Q_\Lambda$ are in the domain of $[\ ]$ and $u \approx v$, then $[u]=[v]$.

From 1.2.2 and 1.2.3 we obtain the following proposition.

1.2.4. If every semigroup term is (n,Λ)-irreducible, then $V=\mathrm{Var}\Lambda$ is an n-variety.

1.3. The proof of Theorem will be completed here, by assuming that the condition (α) is satisfied.

If $m=0$, then all the semigroup terms are (n,Λ)-irreducible, and by 1.2.4 we obtain that V is an n-variety. Thus, we can assume that $m > 0$.

Let $Q \in V_n$, and $u,v \in Q_\Lambda$ be such that $u \approx v$ and both u and v are in the domain of $[\ ]$. By 1.2.3 we have to show that $[u]=[v]$.

From $u \approx v$ it follows that there exists a sequence $w_1,\dots w_k \in Q_\Lambda$ such that $k \ge 0$ and $u \vdash\!\dashv w_1 \vdash\!\dashv w_2 \vdash\!\dashv \dots \vdash\!\dashv w_k \vdash\!\dashv v$. If one of u,v is irreducible, then, by 1.2.2, the sequence $u,w_1,\dots,w_k,v$ can be shortened in the case $k > 0$, and we have $[u]=[v]$ in the case $k=0$. Thus we can assume that both u and v are reducible.

Let s be such that $w=w_s$ is reducible, and w_t is irreducible for any $t < s$. (If w_1 is reducible, then $w=w_1$, and $w=v$ if all the $w_1,\dots,w_k$ are irreducible.)

The condition (α) implies that there exist $a,b \in Q$ such that $u=a^{im}u$, $w=wb^{jm}$, for any pair of positive integers i,j. The assumption u to be in the domain of $[\ ]$ implies that i can be chosen in such a way that all the members of the sequence $a^{im}w_1,\dots,a^{im}w_{s-1},a^{im}w$ are in the domain of $[\ ]$. Then we also have: $u \vdash\!\dashv a^{im}w_1 \vdash\!\dashv \dots \vdash\!\dashv a^{im}w$, and this implies that $[u]=[a^{im}w] = \dots = [a^{im}w]$. Let j be such that $j(n-1)m \ge r$, where r is the index of V. Then we have: $w=wb^{j(n-1)m}$, $b^{j(n-1)m+im}=$

$=b^{j(n-1)m}$, and this implies that: $a^{im}ub^{j(n-1)m}=ub^{j(n-1)m+im}$. Therefore we have:

$$a^{im}w = a^{im}wb^{j(n-1)m} \vdash\!\dashv \ \ldots \vdash\!\dashv \ a^{im}ub^{j(n-1)m} = ub^{j(n-1)m+im},$$

and:

$$ub^{j(n-1)m+im} \vdash\!\dashv \ w_1 b^{j(n-1)m+im} \vdash\!\dashv \ \ldots \vdash\!\dashv \ wb^{j(n-1)} wb^{j(n-1)m+im} = w$$

Finally, we obtain:

$$[u] = [a^{im}w] = [a^{im}ub^{j(n-1)m}] = [ub^{j(n-1)m+im}] = \\ = \ldots = [wb^{j(n-1)m+im}] = [w].$$

This completes the proof of Theorem.

2. COROLLARIES

Cor. 1. If ABSEM is a subvariety of a variety $\mathcal{V}$, then $\mathcal{V}$ is an n-variety for any $n \geq 2$.

Proof. The assumption is equivalent to the statement that $\mathrm{per}\mathcal{V}=0$, and then all the semigroup terms are (n,Λ)-irreducible for every $n \geq 2$.

Cor. 2. Let m be a non-negative integer and $n \geq 2$ be such that n-1 is a divisor of m. If $\mathcal{V}$ is a semigroup variety with a period m, then $\mathcal{V}$ is an n-variety.

Proof. If $\mathcal{V}=\mathrm{Var}\Lambda$, then every semigroup term is (n,Λ)-irreducible. (Clearly Cor. 1 is a special case of Cor. 2.)

Cor. 3. If $\mathcal{V}$ is a semigroup variety with an index $r=1$, then $\mathcal{V}$ is an n-variety for every $n \geq 2$.

Proof. Let $m=\mathrm{per}\mathcal{V}$. If $m=0$, then we can apply Cor. 1, and thus we can assume that $m > 0$. If $\xi=x_i \ldots x_j$, and $k > 0$, then we have: $(x_i^{km}\xi,\xi)$, $(\xi,\xi x_j^{km}) \in \langle \Lambda \rangle$, where $\mathcal{V}=\mathrm{Var}\Lambda$. Thus, the condition (α) is satisfied.

A semigroup variety $\mathcal{V}=\mathrm{Var}\Lambda$ is a variety of periodic groups iff $\mathrm{ind}\mathcal{V}=1$, $\mathrm{per}\Lambda=m \geq 1$ and $(x_1x_2^m,x_1)$, $(x_1^m x_2,x_2) \in \langle \Lambda \rangle$. From Cor. 3 we obtain the following one:

Cor. 4. A variety of periodic groups is an n-variety for every $n \geq 2$.

Cor. 5. Let $\mathbb{V}=\mathrm{Var}\Lambda$ be a variety of abelian semigroups with an index r, and let the following condition be satisfied:

(β) If (ξ,η) is a nontrivial semigroup-identity belonging to Λ, i.e. $(\xi,\eta)\in\Lambda$ is such that $|\xi|_i\neq|\eta|_i$ for some $i\geq 1$, then there exist $j,k\geq 1$ such that $|\xi|_j\geq r$ and $|\eta|_k\geq r$.

Then $\mathbb{V}$ is an n-variety for every $n\geq 2$.

Proof. We notice first that $\langle\Lambda\rangle$ also satisfies the condition (β). If r=1, then the conclusion follows from Cor. 3. Thus we can assume that $r>1$ and $m>0$. Let ξ be an (n,Λ)-reducible semigroup-term. Then there is a semigroup term η such that $(\xi,\eta)\in\langle\Lambda\rangle$, and $|\xi|\not\equiv|\eta| \pmod{n-1}$. Therefore, $|\xi|_i\neq|\eta|_i$ for some $i\in\{1,2,\dots\}$ and this implies that there is an $x_j\in X$ such that $|\xi|_j\geq r$. Thus, we have $(x_j^{km}\xi,\xi)$, $(\xi,\xi x_j^{km})\in\langle\Lambda\rangle$, for any $k>0$, and we can apply Theorem.

Cor. 5'. $\mathbb{A}_{r,m}=\mathrm{Var}\{x_1x_2=x_2x_1,\ x_1^r=x_1^{r+m}\}$ is an n-variety for every $n\geq 2$, $r\geq 1$, $m\geq 0$. (This is in fact Theorem 2 of [1].)

Cor. 6. Denote by $\Delta_{(k)}$ the following set of semigroup identities:

$$\Delta_{(k)}=\{(x_1\dots x_k,x_1\dots x_ix_jx_{i+1}\dots x_k)\mid 2\leq i\leq k-1,\ j\in\{1,k\}\},$$

where $k\geq 3$. Then $\mathbb{D}_k=\mathrm{Var}\,\Delta_{(k)}$ is an n-variety for every $n\geq 2$.

Proof. First, it can be easily shown that if $n\geq 3$, and a semigroup term ξ is $(n,\Delta_{(k)})$-reducible, then $|\xi|\geq k$. In this case, if $\xi=x\eta y$, then $(x^i\xi,\xi)$, $(\xi,\xi y^i)\in\langle\Delta_{(k)}\rangle$ for any $i>0$, and thus the condition (α) is satisfied.

(We notice that it is shown in the paper [8] that $\mathbb{D}=\mathbb{D}_3$ is an n-variety for any $n\geq 2$, and that the same proof can be applied for the general case.)

Cor. 7. $\mathbb{D}_k\cap$ ABSEM is an n-variety for every $k\geq 3$, $n\geq 2$.

Proof. It is easy to show that (α) is satisfied.

(Cor. 7 is also proved in [2]).

The following proposition is the main result of the paper [7].

Prop. 8. If $L_k = \mathrm{Var}(x_1 \ldots x_k, x_1 \ldots x_k x_{k+1})$, $R_k = \mathrm{Var}(x_1 \ldots x_k, x_{k+1} x_1 \ldots x_k)$, $O_k = L_k \cap R_k$, then L_k, R_k, O_k are n-varieties for any $k \geq 1$, $n \geq 2$.

We note that O_k satisfies the condition (α), but neither of the varieties L_k, R_k satisfies (α).

The above examples exhaust all the known semigroup n-varieties. A list of the known semigroup quasi n-varieties will be given below. (see [1], [7], [2]).

Prop. 9. If $r > 1$, and $n-1$ is not a divisor of m, then $P_{r,m} = \mathrm{Var}(x_1^r, x_1^{k+m})$ is a quasi n-variety.

Prop. 10. If $n \geq 3$ and $D^\ell = \mathrm{Var}(x_1x_2x_3, x_1x_2x_1x_3)$, $D^r = \mathrm{Var}(x_1x_2x_3, x_1x_3x_2x_3)$, then both D^ℓ and D^r are quasi n-varieties.

Prop. 11. Let s,m,n and k be positive integers such that:

$$n \geq 3,\ m \equiv 0 \pmod{n-1},\ m \neq 2s+1,\ m \neq 2s+2,\ s+2 \leq m,\ k \geq m+2,$$

and let $\Delta_{(k)}$ be as in Cor. 6, and

$$\Delta_{(k,s,m)} = \Delta_{(k)} \cup \{(x_1^s x_2^{m-s}, x_1^{s+2} x_2^{m-s-1})\}.$$

Then both the varieties

$$\mathrm{Var}\ \Delta_{(k,s,m)} \text{ and } \mathrm{ABSEM} \cap \mathrm{Var}\ \Delta_{(k,s,m)}$$

are quasi n-varieties.

R E F E R E N C E S

[1] Ǵ.Čupona: n-subsemigroups of semigroups satisfying the law $x^r=x^{r+m}$, Annuare de la Faculté des Mathematiques, Skopje, T.30 (1979), 5-14

[2] Ǵ.Čupona: n-subsemigroups of some commutative semigroups, Annuare T.32 (1981)

[3] S.Markovski: On quasivarieties of generalized subalgebras, Algebraic Conference Skopje 1980, 125-129

[4] E.Nelson: The lattice of equational classes of commutative semigroups, Can.J. Math Vol. XXIII, No 5 (1971), 875-895

[5] А.Я.Айзенштат, Б.К.Богута: О решетке многообразий полугрупп, Ленингр. Госуд. педаг. институт, Сборник научных трудов, Ленинград (1979)

[6] А.И.Мальцев: Алгебрические системы, Москва 1970

[7] С.Марковски: За една класа полугрупи, Математ.Билтен 1(XXVII) (1978), 29-36

[8] С.Марковски: За дистрибутивните полугрупи, Годишен зборник на Матем.фак., Скопје 30(1979), 15-27

Ǵ.Čupona, Matematički fakultet,
P.F. 504,
91000 Skopje
Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

ON *-REGULAR SEMIGROUPS

Siniša Crvenković

The *-regular semigroups were introduced by M.Drazin in [2], K.S.S.Nambooripad and F.Pastijn in [4].

In the present paper we consider some basic properties of *-regular semigroups.

1. Introduction

A *-semigroup is a semigroup equipped with a unary operation $*: S \longmapsto S$ satisfying

1.) $(a^*)^* = a$,

2.) $(ab)^* = b^*a^*$.

Such a unary operation * is sometimes called an involution.

A semigroup S is regular if for each $a \in S$, there exists $x \in S$ such that $a = axa$. For $a \in S$, an element $x \in S$ is an inverse of a if $a = axa$, $x = xax$. An idempotent of *-semigroup is called a projection if $e^* = e$. Denote the set of idempotents by $E(S)$.

It is well-known that every semigroup is embeddable in a regular semigroup. Also, it is easy to see that every semigroup is embeddable in a regular semigroup with involution. Namely, let S be a semigroup and S_1 a regular semigroup such that $S \subseteq S_1$. Take S_2 to be left-right dual of S_1 and ϕ bijection such that $\phi(S_1) = S_2$. If T is the 0-direct union of S_1 and S_2, define $*: T \longmapsto T$ to be

$$x^* = \begin{cases} \phi(x), & x \in S_1 \\ 0, & x = 0 \\ \phi^{-1}(x), & x \in S_2 \end{cases}$$

Obviously, S_2 is a regular semigroup with involution * such that $S \subseteq T$.

2. Basic properties

Let S be a semigroup with involution. If every $\mathcal{L}$-class of S contains a projection, then S is called a *-regular semigroup.

THEOREM 1 [4]. *Let S be a semigroup with involution *. Then the following statements are equivalent.*

(i) *Every $\mathcal{L}$-class of S contains a projection,*

(ii) *for every $a \in S$ we have $a^*a \mathcal{L} a$,*

(iii) *for $a \in S$, a^* is $\mathcal{L}$-equivalent to some inverse of a*

(iv) *for every $a \in S$, a^* is $\mathcal{H}$-equivalent to some inverse of a,*

(v) *for every $a \in S$ there exists an element x which satisfies* $axa = a$, $xax = x$, $(ax)^* = ax$, $(xa)^* = xa$.

Many nice examples of *-regular semigroups are given in [4]. From the paper of R.Penrose [6] we see that the semigroup $M_n(C)$, of complex $n \times n$ matrices, is a *-regular semigroup with * as the conjugate transpose of a matrix. Some statements from [6], for matrices, could be applied to any *-regular semigroup.

LEMMA 1.2 *Let S be a semigroup with involution. The conditions of Theorem 1 are equivalent to each of the following.*

(vi) *For every $a \in S$ there exists $x \in S$ such that*

$$xx^*a^* = x,\ xaa^* = a^*;$$

(vii) *For every $a \in S$ there exists $y \in S$ such that*

$$a^*y^*y = y,\ a^*ay = a^*.$$

Proof. If S satisfies (v) of Theorem 1 we have

$$xax = x(ax)^* = xx^*a^* = x$$

and

$$a^*x^*a^* = (xa)^*a^* = xaa^* = a^*.$$

Conversely, if $xx^*a^* = x$, then

(1) $x(ax)^* = x$

i.e.

(2) $ax(ax)^* = ax$.

From (2) we have $(ax)^* = ax(ax)^* = ax$. From (1) we get $xax = x$. Analogously, from $xaa^* = a^*$ we have that $xa = (xa)^*$ and $axa = a$.

(vii) is similar to (vi).

LEMMA 2.2 [2] _If S is a *-regular semigroup then there exists a unique x such that the condition_ (v) _of Theorem 1 is satisfied._

We denote with $a^\dagger$ an x satisfying the condition (v).

LEMMA 3.2 [4] _If S is a *-regular semigroup, then for every_ $a \in S$ _we have_

1.1 $(a^\dagger)^\dagger = a$,

1.2 $(a^\dagger)^* = (a^*)^\dagger$,

1.3 $(a^*a)^\dagger = a^\dagger a^{\dagger *}$

1.4 $a^\dagger a^{\dagger *} a^* = a^\dagger = a^* a^{\dagger *} a^\dagger$, $a^\dagger a a^* = a^* = a^* a a^\dagger$.

LEMMA 4.2 _In a *-regular semigroup S, if_ $xaa^* = a^*$ _and_ $a^*ay = a^*$, _then_ $a^\dagger = xay$.

Proof. From $xaa^* = a^*$ we have that $xaa^*x^* = a^*x^*$ i.e. $(xa)^* = xa$ and $axa = a$. Analogously, from $a^*ay = a^*$ we have $(ay)^* = ay$ and $aya = a$. It is easy to see that xay satisfies (v) i.e. $a^\dagger = xay$.

THEOREM 2. _Let S be a semigroup with involution. Then the following conditions are equivalent._

(A) _S is a *-regular semigroup;_

(B) _For any_ $a \in S$, _there exists_ $z \in S$ _such that_ $aa^*az = a$;

(C) _For any_ $a \in S$, _there exists_ $w \in S$ _such that_ $waa^*a = a$.

Proof. (A)$\Longrightarrow$(B). Lemma 1.2 implies that for every $a \in S$ there exists $x \in S$ such that $xx^*a^* = x$ and $xaa^* = a^*$.

We have that $xx^*a^*aa^* = a^*$. If we put $z = xx^*$, then $aa^*az = a$.

(B)$\Longrightarrow$(A). From $aa^*az = a$ we have $z^*a^*aa^* = a^*$. Denote $x = (az)^*$. Then, $xaa^* = a^*$ i.e. $a^*x^*a^* = a^*$ so that $xx^*a^* = z^*a^*x^*a^* = z^*a^* = (az)^* = x$.

(C) is the dual condition of (B).

From consideration above, we have that $aa^*az = a$ implies $a(az)^*a = a$. Conversely, if in a semigroup with involution, for every $a \in S$ there exists $z \in S$ such that $a(az)^*a = a$, then S is a *-regular semigroup. Namely, $a(az)^*a = a$ means that $az^*a^*a = a$ i.e. $a^*aza^* = a^*$. Denote $za^* = y$. There exists $v \in S$ such that $a^*(a^*v)^*a^* = a^*$. We have that $a^*v^*aa^* = a^*$. Denote $a^*v^* = x$. From Lemma 4.2 we see that $a^\dagger = xay$. Thus we have proved the following:

COROLLARY. <u>A semigroup S with involution is a *-regular semigroup if and only if for every $a \in S$ there exists $z \in S$ such that</u> $a(az)^*a = a$.

PROPOSITION 1.2 <u>Let S be finite *-regular semigroup. Then, for each $a \in S$,</u>

$$a^\dagger = (a^*a)^{t-1}a^*,$$

<u>for some</u> $t \geq 1$.

<u>Proof.</u> If $a^*aa^*a = a^*a$, then $a^*aa^*aa^\dagger = a^*aa^\dagger$. As $a^*aa^\dagger = ((aa^\dagger)^*a)^* = (aa^\dagger a)^* = a^*$ we have $a^*aa^* = a^*$ i.e. $aa^*a = a$ so that $a^\dagger = a^*$. In monogenic semigroup $\langle a^*a \rangle$ there exists an idempotent $(a^*a)^t$, for some $t \geq 1$.

$$(a^*a)^t(a^*a)^t = (a^*a)^t$$

i.e.

$$(a^*a)^{t-1}(a^*a)^{t+1} = (a^*a)^t.$$

Multiplying the last equality with $a^\dagger$ and $a^{\dagger *}$ successively, we have $(a^*a)^{t-1}a^*aa^* = a^*$ i.e. $aa^*a(a^*a)^{t-1} = a$. From the proof of Theorem 2 we have that $a^\dagger = (a^*a)^{t-1}a^*$.

THEOREM 3. <u>Let S be a *-regular semigroup. Then</u>

$$a^\dagger = a^*u^*ava^*$$

for any u,v such that $aa^*uaa^* = aa^*$ and $a^*ava^*a = a^*a$.
Proof. From $aa^*uaa^* = aa^*$ we have $aa^*uaa^*a^{\dagger *} = aa^*a^{\dagger *}$ i.e. $aa^*ua = a$ so that $a^*u^*aa^* = a^*$. Similarly, we have $a^*ava^* = a^*$. If in Lemma 4.2 we take a^*u^* to be x and va^* to be y, we see that $a^{\dagger} = a^*u^*ava^*$.

3. Congruences.

A relation ρ on a *-semigroup S is called a *-relation if $(a\rho)^* = a^*\rho$ for all $a \in S$, where $a\rho$ denotes the ρ-class containing a. We say that ρ preserves *.

Let S be a regular semigroup. An equivalence π on E(S) is called normal if and only if there is a congruence ρ on S so that $\pi = \rho \cap (E(S) \times E(S))$. We say that π is normal equivalence associated with ρ. If ρ is a congruence on S, then $\mathrm{Ker}\rho = \{a \in S: a\rho = e\rho, \text{ for some } e \in S\}$ is the kernel of ρ.

P.G.Trotter in [7] gave description of congruence on regular semigroups in terms of normal equivalences on sets of idempotents and kernels of congruences. Let π be a normal equivalence on E(S). For notions of π-kernel $\mathscr{L}_\pi$, $\mathscr{R}_\pi$ and $\mathscr{H}_\pi$-relations we refer [7]. Let S be a *-regular semigroup. It follows that

$$\mathscr{R}_\pi = \{(a,b) \in S \times S;\ (aa^{\dagger}\pi)(bb^{\dagger}\pi) \cap bb^{\dagger}\pi \neq \emptyset,\ (bb^{\dagger}\pi)(aa^{\dagger}\pi) \cap aa^{\dagger}\pi \neq \emptyset\},$$

$$\mathscr{L}_\pi = \{(a,b) \in S \times S;\ (a^{\dagger}a\pi)(b^{\dagger}b\pi) \cap a^{\dagger}a\pi \neq \emptyset,\ (b^{\dagger}b\pi)(a^{\dagger}a\pi) \cap b^{\dagger}b\pi \neq \emptyset\}$$

and $\mathscr{H}_\pi = \mathscr{L}_\pi \cap \mathscr{R}_\pi$.

From Theorem 2.2 in [7], we have

PROPOSITION 1.3 Let $(S,.,\dagger,*)$ be a *-regular semigroup. If ρ is a congruences of $(S,.)$, then

$$\rho = \{(a,b) \in \mathscr{H}_\pi:\ ab^{\dagger},\ a^{\dagger}b \in K\},$$

where $K = \mathrm{Ker}\rho$ and π is the normal equivalences associated with ρ.

If ρ is an idempotent separating congruence on $(S,.)$, we have

(1´) $(a,b)\in \mathcal{H}_{\pi} \Longrightarrow (a^{\dagger},b^{\dagger})\in \mathcal{H}_{\pi}$

(2´) $(a,b)\in \mathcal{H}_{\pi} \Longrightarrow (a^{*},b^{*})\in \mathcal{H}_{\pi}$.

Namely, $aa^{\dagger}\pi = aa^{\dagger}$, $bb^{\dagger}\pi = bb^{\dagger}$, $a^{\dagger}a\pi = a^{\dagger}a\pi$ and $b^{\dagger}b\pi = b^{\dagger}b$ so that $(a,b)\in \mathcal{H}_{\pi}$ implies $a^{\dagger}a = b^{\dagger}b$, $aa^{\dagger} = bb^{\dagger}$ from which (1´) and (2´) immediately follows. Also, $(a,b)\in \rho \Longrightarrow (a^{\dagger},b^{\dagger})\in \rho$, as $a^{\dagger}(b^{\dagger})^{\dagger} = a^{\dagger}b$ and $(a^{\dagger})^{\dagger}b = ab^{\dagger}$.

PROPOSITION 2.3 _Let_ $(S,.,\dagger,*)$ _be a *-regular semigroup and_ ρ _be an idempotent separating congruence on_ $(S,.)$. _Then_ ρ _preserves_ $\dagger$ _and_ $*$ _if and only if_ $(\mathrm{Ker}\rho)^{*} = \mathrm{Ker}\rho$.

Proof. If ρ preserves $\dagger$ and $*$, then, obviosly, $(\mathrm{Ker}\rho)^{*} = \mathrm{Ker}\rho$. Conversely, if $(\mathrm{Ker}\rho)^{*} = \mathrm{Ker}\rho$, since ρ is symetric, from (2´) we have that $(a,b)\in \rho$ implies $(a^{*},b^{*})\in \mathcal{H}_{\pi}$, $ab^{\dagger}$, $a^{\dagger}b$, $ba^{\dagger}$, $b^{\dagger}a\in K$ and $a^{*}b^{*\dagger}$, $a^{*\dagger}b^{*}\in K^{*} = K$. It follows that $(a^{*},b^{*})\in \rho$.

THEOREM 4. _Let_ $(S,.,\dagger,*)$ _be a *-regular semigroup. Then_ ρ _preserves_ $\dagger$ _and_ $*$ _if and only if_ $(\mathrm{Ker}\rho)^{*} = \mathrm{Ker}\rho$ _and_ $(e,f)\in \rho \Longrightarrow (e^{*},f^{*})\in \rho$, _where_ $e,f\in E(S)$.

Proof. Similar to the proof of Theorem 4.4 [5] . It should be noticed that S/σ , in the proof of Theorem 4.4 [5] , is a *-regular semigroup and the relation

$$\rho/\sigma = \{(a\sigma,b\sigma)\in S/\sigma \times S/\sigma \; : \; (a,b)\in \rho\}$$

is an idempotent separating congruence on S/σ with $(\mathrm{Ker}\rho/\sigma)^{*} = \mathrm{Ker}\rho/\sigma$. From Proposition 2.3 we have that ρ/σ preserves $*$ so that ρ preserves $*$.

In [3] T.Imaoka gave a characterization of congruences on special *-semigroups.

Using the previous considerations and the notion of normal(admissible) set of subsets [1] p.58, it is possible to give similar characterization of congruences on *-regular semigroups. This will be presented elswhere.

REFERENCES

[1] A.H.Clifford, G.B.Preston, The Algebraic Theory of Semigroups, Amer.Math.Soc., Providence,R.I.,Vol 1,1961, Vol 2,1967.

[2] M.P. Drazin, Regular Semigroups with Involution, Symposium on Regular Semigroups, April 1979, Northern Illionois University, De Kolb(1979), 29-46.

[3] T. Imaoka, *-congruences on Regular *-semigroups, Semigroup Forum, Vol 33, No.4(1981)321-326.

[4] K.S.S. Nambooripad, F.J.C.M. Pastijn, Regular Involution Semigroups(to appear).

[5] T.E. Nordahl, H.E. Scheiblich, Regular * Semigroups, Semigroup Forum, Vol 16(1978)369-377.

[6] R. Penrose, A Generalised Inverse for Matrices, Proc. Cambridge Philos. Soc., 51(1955),406-416.

[7] P.G. Trotter, Congruences on Regular and Completely Regular Semigroups, J. Austral. Math. Soc.(Series A)32 (1982), 388-398.

Institut za matematiku
Ilije Djuričića 4
21000 Novi Sad
JUGOSLAVIJA

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

SOME PROPERTIES OF THE DEFECT OF DISTRIBUTIVITY OF A NEAR-RINGS

V.Dašić

Abstract

The near-rings with defect of distributivity generalize the distributively generated (d.g.) near-rings. In the case when the defect D is zero, we obtain the class of the d.g. near-rings. In this paper we consider some properties of the defect which are related to a structure of a near-rings.

A near-ring R is an algebraic system with two binary operations, addition and multiplication, such that

1^o (R,+) is a group

2^o (R,.) is a semigroup

3^o $x(y+z)=xy+xz$ for all $x,y,z\in R$

We suppose also $ox=o$ for all $x\in R$.

Let R be a near-ring. We recall that the subsemigroup (S,.) of the semigroup (R,.) is a set of generators, if (R,+) is generated by S. The defect of distributivity of the near-ring R is the normal subgroup D of the group (R,+) generated by the set

$$\{d : d=-(xs+ys)+(x+y)s,\ x,y\in R,\ s\in S\}$$

The near-ring R with the defect D will be denoted by (R,S) when we wish to stress the set of generators S. Every element of R can be represented as $\sum(\pm s_i)$, $(s_i\ S)$.

When we say that the near-ring (R,S) has the defect D, this means that $D\neq R$. If addition to S=R we obtain the class of the D-distributive near--rings. In this case, for all $x,y,z\in R$ there axists $d\in D$ such that

$$(x+y)z = xz+yz+d.$$

Finally, if $D=R$ then the defect D depends no upon the set of generators, In this extreme case R is the D-distributive near-ring as well.

A subgroup (B,+) of the group (R,+) is called a right R-subgroup iff $BR=\{br: b\in B,\ r\in R\}\subseteq B$. A subgroup (B,+) of (R,+) is called a left R-subgroup iff $RB\subseteq B$. A normal subgroup (B,+) of (R,+) is a right ideal of R iff $(x+b)y-xy\in B$ for all $x,y\in R$, $b\in B$. A right ideal B of R which is a left R-subgroup is an ideal of R.

Let (R,S) be a near-ring with the defect D and let (A,+) be a normal subgroup of (R,+). The normal subgroup of the group (R,+) generated by the elements of the form

$$d=-as-xs+(x+a)s, \quad (x\in R, s\in S, a\in A)$$

is called the relative defect of the subset A with respect to R. At similar way, we define a relative defect of a subset $A\subset R$ as the relative defect of $\bar{A}$, where $\bar{A}$ is the normal subgroup of (R,+) generated by A. The relative defect of the subset $A\subset R$ will be denoted by $D_r(A)$. For basic definitions and properties about near-ring with defect see [1].

PROPOSTION 1. Let R be a near-ring with the defect D. The set $A_D(R)=\{a\in R: aR\subseteq D\}$ is a nilpotent ideal of R if and only if D is nilpotent.

Proof, By Theorem 3 of [2] $A_D(R)$ is an ideal of R. If D is a nilpotent ideal of R, where the index of niopotence is n, then for all a_i, $a_j\in A_D(R)$ we have $a_ia_j\in D$ and $a_1a_2...a_{2n-1}a_{2n}=(a_1a_2)...(a_{2n-1}a_{2n})=0$. Thus, $A_{D(R)}$ is a nilpotent ideal of R.

The converse follows immediately, because $D\subseteq A_D(R)$.

The following theorem generalize a result of Dover ([3], T_6) and a result of Freidman ([5], Lemma 2.1).

THEOREM 2. Let R be a D-distributive near-ring, then $R'\subseteq A_D(R)$, where R' is the commutator subgroup of (R,+) . If D is contained in the commutator subgroup R', then R' is a nilpotent ideal of R if and only if D is nilpotent.

Proof. By Corollary 2 of Proposition 2.7 of [1] $R'R\subseteq D$. Hence $R'\subseteq A_D(R)$. If D is contained in R', then by Theorem 3.4 of [1] R' is an ideal of R. Let D be a nilpotent ideal of R. Then by Proposition 1 $A_D(R)$ is a nilpotent ideal of R. But $R'\subseteq A_D(R)$, i.e. R' is nilpotent.

The converse is immediate.

THEOREM 3. ([1] , Lemma 3.2.) Let A be a normal S-subgroup of the near-ring R with the defect D. A is a right ideal of R if and only if $D_r(A)\subseteq D\cap A$, where $D_r(A)$ is a relative defect of the subset A.

The following theorem characterize the relative defect of a subset A.

THEOREM 4. Let (R,S) be a near-ring with the defect D. a) If A is a right ideal of R, then the relative defect $D_r(A)$ of the subset A is an ideal of R.

b) If A is an ideal of R, then the relative defect $D_r(A)$ of the subset A is an ideal of R.

Proof. a) Let $d=\sum(r_i\pm(-a_is_i-x_is_i+(x_i+a_i)s_i)-r_i)\in D_r(A)$ $(r_i,x_i\in R,\ s_i\in S,\ a_i\in A)$. We need to show that for all y, $z\in R$ and $d\in D_r(A)$ it follows $(y+d)z-yz\in D_r(A)$, Let $z=\sum(\pm s_j)$ $(s_j\in S)$.

Applying induction on j we need only to show that

$[y+(-as-xs+(x+a)s]\, s_j-ys_j \in D_r(A)$ $(x,y\in R,\ s,s_j\in S,\ a\in A)$.

Clearly,

$[y+(-as-xs+(x+a)s]\, s_j-ys_j=ys_j+[-as-xs+(x+a)s]\, s_j-ys_j+ys_j-[-as-xs+(x+a)s]\, s_j-ys_j+$
$+[y+(-as-xs+(x+a)\ s)]s_j-ys_j$.

It is easy to see that $-as-xs+(x+a)s=-as-xs+(x+a)s-xs+xs\in A$. By definition of $D_r(A)$ we have

$-[-as-xs+(x+a)s]s_j-ys_j+[y+(-as-xs+(x+a)s]\, s_j\in D_r(A)$.

From Theorem 3 it follows that $D_r(A)$ is a right S-subgroup of R, since D is an ideal of R. Hence $[-as-xs+(x+a)s]s_j\in D_r(A)$. Since $D_r(A)$ is a normal subgroup of (R,+) we have

$$ys_j+[-as-xs+(x+a)s]\, s_j-ys_j\in D_r(A).$$

Thus

$[y+(-as-xs+(x+a)s)]\, s_j-ys_j \in D_r(A)$, i.e. $D_r(A)$ is a right ideal of R

b) By definition of $D_r(A)$ every element in $D_r(A)$ has the form $\sum(r_i\pm d_i-r_i)$, where $d_i=-(x_is_i+a_is_i)+(x_1+a_i)s_i$ $(x_i,r_i\in R, s_i\in S,\ a_i\in A)$. For all $r\in R$ and $d=-as-xs+(x+a)s\in D_r(A)$, $(x\in R,\ s\in S,\ a\in A)$ we have $r[-as-xs+(x+a)s]=-ras-rxs+(rx+ra)\ s\in D_r(A)$, because A is a left R-subgroup, i.e. $ra\in A$. Thus $D_r(A)$ is a left R-subgroup. Conseguently, $D_r(A)$ is an ideal of R.

Definition. Let (R,S) be a near-ring with the defect D. The subset B of R is a subnear-ring with a defect if and only if B is a subnear-ring of R and (B,+) is generated by $S'\subseteq S$.

Clearly, every subnear-ring with defect is a subnear-ring too. The converse is not true in general. Therefore the class of all near-rings with defect is no variety as well as the class of the d.g. near-ring. Meanwhile the class of all D-distributive near-rings just like the class of the distributive near-rings is a variety.

Let B be a subnear-ring with the defect D(B). Clearly $D(B)\subseteq B\cap D$. By Theorem 3.3 of [1] it follows that D(B) is an ideal of B. If B is an ideal of the near-ring (R,S) with the defect D, where the set of generators of (B,+) is $S'\subseteq S$, then

$$D(B)\subseteq D_r(B)\subseteq B\cap D.$$

From Corollary of the Theorem 2.6 of [1] we obtain the following two propositions.

PROPOSITION 5. Let (R,S) be a near-ring with the defect D and let A be an ideal of R. If $B \supseteq A$ is a subnear-ring of R, where (B,+) is generated by $S' \subseteq S$, then B/A is a d.g. near-ring if and only if $D(B) \subseteq A$.

PROPOSITION 5. Let R be a D-distributive near ring with the defect D and let A be an ideal of R. If $B \supseteq A$ is a subnear-ring of R, then B/A is a distributive near-ring if and only if $D(B) \subseteq A$.

THEOREM 6. Let (R,S) be a near-ring with the defect D and let B be a subnear-ring of R, where (B,+) is generated by $S' \subseteq S$. If $B \cap D = \{o\}$, then B is distributively generated as a subnear-ring.

Proof. From $B \cap D = \{o\}$ it follows $B \cap D(B) = \{o\}$, since $D(B) \subseteq D$. Thus by the Lemma 4.2o of [4] it follows $B+D(B)/D(B) \simeq B/D(B) \cap B$. By using the Proposition 5 we have that B+D(B)/D(B) is a d.g. near-ring. Thus B is distributively generated as a subnear-ring.

The proof of the following theorem is analogous to the proof of the Theorem 6.

THEOREM 6'. Let R be a D-distributive near-ring with the defect D and let B be a subnear-ring of R. If $B \cap D = \{o\}$, then B is distributive as a subnear-ring.

For example, the near-ring on D_8 ([6], (4) p.345) is a near-ring with the defect $D = \{o,2a\}$. The subnear-ring $B = \{o,b\}$ is a d.g. subnear-ring, just a distributive subnear-ring.

THEOREM 7. Let (R,S) be a near-ring with the defect D and let R be a finite direct sum of a non-empty collection of the ideals A_i $i \in \{1,2,\dots,n\}$ where $D = A_j$ for some $j \in \{1,2,\dots,n\}$. If for all $i \neq j$, the set of generators S_i of the subgroup $(A_i,+)$ is a subset in S, then R is a direct sum of the defect D and of the d.g. subnear-ring $B = \bigoplus_{i \neq j} A_i$.

Proof. By Theorem 6, A_i is a d.g. near-ring for all $i \neq j$. From Theorem 6.9 a) of [6] every direct sum of d.g. near-rings is a d.g. near-ring. Thus $B = \bigoplus_{i \neq j} A_i$ is a d.g. near-ring. Hence $R = B \oplus D$.

R E F E R E N C E S

1. V.Dašić., A defect of distributivity of the near-rings. Math. Balkanica (to appear).

2. V.Dašić., Some properties of D-distributive near-ring. Glasnik matematički (to appear).

3. R.E.Dover., Quasi-rings, Thesis, University of Texas at Arlington, 1968, pp 1-22.

4. C.G.Fain., Some structure theorems for near-ring., Ph.D. Dissertation, The University of Oklahoma, 1968 pp 1-63

5. P.A. Freidman., Distributively solvable near-rings, Proceedings of the Riga Seminar on Algebra (Russian), 1969, 297-309.

6. G.Pilz., Near-rings, North-Holland, New York, 1977

Dašić Vučić

Institut za matematiku i fiziku
81000 Titograd
Jugoslavia

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

ON THE TWO-CARDINAL PROBLEM

Aleksandar Jovanović

For a first order theory T with a unary predicate symbol P it is interesting to know all pairs (α,β) admitted by T.

The following two theorems are from (1).

THEOREM 1. (GCH) Suppose $\alpha \geqslant \alpha' \geqslant \beta' \geqslant \beta \geqslant \omega$ and $\|L\| \leqslant \alpha'$. Then every theory T in L which admits (α,β), admits also (α',β').

THEOREM 2. Let L have a unary predicate symbol P. If $\alpha \geqslant \beta \geqslant \omega$ and $\alpha^{\omega} \geqslant \beta' \geqslant \beta^{\omega}$ then every (α,β) model has a complete extension which is an (α^{ω},β') model.

Now it is quite clear that the most interesting cases are the extreme ones, motivating the following definitions.

The pair (α,β) is (when exists):

Left Large Gap (LLG) for T iff T admits (α,β) and does not admit any (α',β) for $\alpha' > \alpha$.

Right Large Gap (RLG) for T iff T admits (α,β) and does not admit any (α,β') for $\beta' < \beta$.

Large Gap (LG) for T iff (α,β) is LLG and RLG.

Left Small Gap (LSG) for T iff T admits (α,β) and does not admit any (α',β) for $\alpha' < \alpha$.

Right Small Gap (RSG) for T iff T admits (α,β) and does not admit any (α,β') for $\beta' > \beta$.

Small Gap (SG) for T iff (α,β) is LSG and RSG.

It is clear that we can correspond partial cardinal functions Λ_i, $i \in 4$, to any theory T, so that (when exists):

$(\Lambda_0(\kappa),\kappa)$ is LLG

$(\kappa,\Lambda_1(\kappa))$ is RLG

$(\Lambda_2(\kappa),\kappa)$ is LSG

$(\kappa,\Lambda_3(\kappa))$ is RSG

for all κ.

For a given theory T it would be interesting to determine the functions Λ_i and their domains. On the other hand it would be nice to know what pairs can be (_)_G. Lacking the characterization we offer the following discussion.

THEOREM 3. <u>Let</u> Λ_0 <u>and</u> Λ_0' <u>be cardinal operations defining</u> LLG <u>for theories</u> T_1 <u>and</u> T_2, <u>for many</u> κ. <u>If one of the following holds</u>

1. GCH
2. Λ_0 <u>is monotonous</u>
3. $|\Lambda_0'(\kappa)|^\omega = \Lambda_0'(\kappa)$

<u>then there is a theory</u> T <u>such that</u> $((\Lambda_0 \circ \Lambda_0')(\kappa), \kappa)$ <u>is</u> LLG <u>for</u> T. <u>The similar is true for</u> RLG.

<u>Proof</u>. Let $\mathfrak{A} = \langle A, V, \dots \rangle$ be a model for T_1 such that V is an interpretation of predicate symbol Q and $|V| = \Lambda_0'(\kappa)$, $|A| = (\Lambda_0 \circ \Lambda_0')(\kappa)$. Let $\mathfrak{B} = \langle B, U, \dots \rangle$ be a model for T_2 such that U is an interpretation of predicate symbol P and $|U| = \kappa$, $|B| = \Lambda_0'(\kappa)$. We may suppose that $L_{T_1} \cap L_{T_2} = \phi$ and that T_2 has closed axioms. Consider the extension T of T_1 obtained in the following way. First, take T' to be a theory in the language $L_{T_1} \cup L_{T_2}$ with the axioms of T_1. Extend T' to T adding interpretations of axioms of T_2 in the language $L_{T_1} \cup L_{T_2}$. The interpretation is defined in the following way. On L_{T_2} it is the identity. In the axioms of T_2 every subformula of the form $\exists x \varphi$ is replaced with the formula $\exists x (Q(x) \& \varphi)$. The universe of the interpretation is Q, so we introduce the axiom $\exists x Q(x)$. If F is an n-ary function symbol of the language then the axiom of T is formula $Q(x_1) \& \dots \& Q(x_n) \Rightarrow Q(F(x_1 \dots x_n))$. Using the bijection $|B| = |V|$, a model $\mathfrak{A}'$, an expansion of $\mathfrak{A}$ is constructed. Let f be such a bijection. Extend f to an isomorphisam. For $c \in L_{T_2}$ define $c^{\mathfrak{A}} = f(c)$. If F is a function symbol in L_{T_2} define

$$F^{\mathfrak{A}}(a_1 \dots a_m) = \begin{cases} F^{\mathfrak{B}}(f^{-1}a_1 \dots f^{-1}a_m) & \text{if } a_1, \dots, a_m \in V \\ \text{arbitrary} & \text{otherwise.} \end{cases}$$

If R is a predicate symbol in L_{T_2} define the interpretation of R

$$R^{\mathfrak{A}}(a_1 \dots a_m) \quad \text{iff} \quad R^{\mathfrak{B}}(f^{-1}a_1 \dots f^{-1}a_m).$$

Now consider predicate symbol P in L_T and model $\mathfrak{A}'' = \langle A, U, \dots \rangle$ for T. $\mathfrak{A}''$ is $((\Lambda_0 \circ \Lambda_0')(\kappa), \kappa)$ model.

Let $\mathfrak{A} = \langle A, V, U, \ldots \rangle$ be some model for T with $|U| = \kappa$. Let V and U be interpretations for Q and P, respectively. Let $L_{T_2'}$ be (the reduct of L_T) $\{Q\} \cup L_{T_1}$ and let T_2' have the interpretations of axioms of T as the only axioms. It follows that $|V| \leq \Lambda_0'(\kappa)$. Using the hypothesis in the similar way, we get $|A| \leq (\Lambda_0 \circ \Lambda_0')(\kappa)$.

COROLLARY. <u>Let</u> T_1 <u>and</u> T_2 <u>have</u> $(\Lambda(\kappa), \kappa)$ <u>and</u> $(\kappa, \Gamma(\kappa))$ <u>as</u> LLG <u>and</u> RLG, <u>many</u> κ, <u>respectively</u>. <u>Then there is a theory</u> T <u>for which</u> $(\Lambda(\kappa), \Gamma(\kappa))$ <u>is</u> LG.

THEOREM 4. <u>With the hypothesis of the corollary the following is true for any ultrafilter</u> D:

$$\Gamma(|\prod_D \kappa|) \leqslant |\prod_D \Gamma(\kappa)| \leq |\prod_D \kappa| \leqslant |\prod_D \Lambda(\kappa)| \leqslant \Lambda(|\prod_D \kappa|).$$

<u>Proof</u>. If a theory admits pairs (α_i, β_i) for $i \in I$ and if D is any ultrafilter over I then the theory admits pair $(|\prod_D \alpha_i|, |\prod_D \beta_i|)$. It follows that T_1 admits the pair $(|\prod_D \Lambda(\kappa)|, |\prod_D \kappa|)$ and that T_2 admits the pair $(|\prod_D \kappa|, |\prod_D \Gamma(\kappa)|)$. Since $(\Lambda(|\prod_D \kappa|), |\prod_D \kappa|)$ is LLG for T_1 and $(|\prod_D \kappa|, \Gamma(|\prod_D \kappa|))$ is RLG for T_2, the proof follows from basic ultrapower cardinality relations.

The following theorem is from (1).

THEOREM 5. <u>There are theories</u> T_1 <u>and</u> T_2 <u>such that for all</u> κ

(κ^+, κ) <u>is</u> LLG <u>for</u> T

$(2^\kappa, \kappa)$ <u>is</u> LLG <u>for</u> T .

The above theorem gives some examples. There is a theory such that for all κ, (κ, κ) is LG. The axioms of Boolean algebra and the definition of cellularity are first order, so we can consider models $(\kappa, \mathrm{cel}(\kappa))$. Let $\mathrm{ded}(D, <)$ be the cardinality of the number of Dedekind cuts in $(D, <)$. Michell has prooved the independence of $\kappa < \mathrm{ded}(\kappa) < 2^\kappa$ for all κ . In (3) is given an example of a theory T such that for all κ, $(\mathrm{ded}(\kappa), \kappa)$ is LLG for T. It would be interesting to have more examples. Here we mention some consequences of the above.

1. <u>for all</u> $n \in \omega$ <u>and all cardinals</u> λ ,

   $(\omega_n(\lambda), \lambda)$ <u>and</u>

   $(\beth_n(\lambda), \lambda)$ <u>are</u> LLG.

2. for all $n\in\omega$, all cardinals λ and any ultrafilter D

$|\prod_D \omega_n(\lambda)| \leq \omega_n(|\prod_D \lambda|)$,

$|\prod_D \beth_n(\lambda)| \leq \beth_n(|\prod_D \lambda|)$,

$|\prod_D \mathrm{ded}(\lambda)| \leq \mathrm{ded}(|\prod_D \lambda|)$.

3. let Λ be any finite combination of operations $\omega_n(\ )$, $\beth_n(\ )$ and $\mathrm{ded}^l(\ )$, as example $\Lambda = {}^{++} \circ \beth_7(\ ) \circ \mathrm{ded}^3(\ )$. Then

$|\prod_D \Lambda(k)| \leq \Lambda(|\prod_D k|)$, in the example

$|\prod_D \beth_7^{++}(\mathrm{ded}^3(k))| \leq \beth_7^{++}(\mathrm{ded}^3(|\prod_D k|))$.

We note that if (α,β) is LG then there are no strongly compact cardinal k between β and α.

The above considerations are conected with the continuum problem. Let D be Magidor's nonregular ultrafilter over ω_3. Then $|\prod_D \omega_1| \leq \omega_3$ and $|\prod_D \omega_3| = 2^{\omega_3}$. Using the mentioned consequences we get: $2^{\omega_3} = |\prod_D \omega_3| = |\prod_D \omega_1^{++}| \leq |\prod_D \omega_1|^{++} \leq \omega_5$. Since in Magidor's model GCH holds the above is not interesting. But if D is a nonregular ultrafilter over ω_3 like Magidor's, thus $|\prod_D \omega_1| \leq \omega_3$, then $2^{\omega_2} = \omega_3$ implies $2^{\omega_3} \leq \omega_5$. It follows that the existence of ultrafilter with the cardinal function with jumps, involves bounds for the continuum function, as the above and similar examples show.

REFERENCES

(1) C. C. Chang, H. J. Keisler, Model Theory, North Holland, Amsterdam, 1973.

(2) M. Magidor, On the existence of nonregular ultrafilters and the cardinality of ultrapowers, Math. Tech Report 176, 1977.

(3). Ž. Mijajlović, Doctoral Disertation, Univ of Belgrade, Faculty of sciences, 1976.

Matematički institut,
Knez Mihajlova 35,
11000 Beograd,
Yugoslavia

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

EMBEDDING OF ALGEBRAS IN DISTRIBUTIVE SEMIGROUPS

S.Kalajdžievski

Abstract. Subalgebras of different kinds of distributive semigroups are considered in [11], [8] and [9]. Here we make corresponding investigations concerning left (right) semigroups. We also esteblish some conections between ω-subalgebras and n-subsemigroups of each of the classes of distributive semigroups, whereas ω is an n-ary operator.

0. PRELIMINARIES

Necessary preliminary definitions and results will be stated first.

An Ω-algebra $\underline{A} = (A;\Omega)$ is an Ω-subalgebra of a semigroup $\underline{S} = (S;.)$ if $A \subseteq S$ and there is a mapping $\omega \mapsto \bar{\omega}$ from Ω into S, such that

$$(1) \qquad \omega(a_1,a_2,\dots,a_n) = \bar{\omega}a_1a_2\dots a_n$$

for every $\omega \in \Omega(n)$, $a_1,a_2,\dots,a_n \in A$ ($\Omega(i)$ denotes the set of all i-ary operators in Ω).

If $\{\omega\} = \Omega(n) = \Omega$, then instead of "Ω-(sub)algebra" we say "ω-(sub)algebra". An ω-algebra $\underline{A} = (A;\omega)$ is called an n-subsemigroup of a semigroup $\underline{S} = (S;.)$ if $\omega \in \Omega(n)$, $n \geqslant 3$, $A \subseteq S$ and

$$(2) \qquad \omega(a_1,a_2,\dots,a_n) = a_1a_2\dots a_n$$

for all $a_1,a_2,\dots,a_n \in A$.

Let V be a variety of semigroups. Then $V(\Omega))(V(n))$ denotes the class of Ω-subalgebras (n-subsemigroups, resp.) of semigroups in V and $\tilde{V}V(\Omega)$ ($\tilde{V}V(n)$) denotes the variety of Ω-algebras (ω-algebras, resp.) defined by the set of all identities valid in $V(\Omega)$ ($V(n)$, resp.). If $V(\Omega)$ ($V(n)$) is a variety then clearly $\tilde{V}V(\Omega) = V(\Omega)$ ($\tilde{V}V(n) = V(n)$, resp.). But in general $V(\Omega)$ ($V(n)$) is a quasivariety [10, pg.254]. In several papers ([2], [3], [4], [6], [7], [8], [9], [11], [12], [13]) special varieties V are considered and the corresponding answers whether $V(\Omega)$ ($V(n)$) is a proper quasivariety or a variety are given. One of the first results is that $SEM(\Omega)$ is the variety of all Ω-algebras [1] , and the other is that SEM(n) is the variety of all n-semigroups [4] , whereas SEM denotes the variety of all semigroups.

Here we are dealing with the following four varieties of semigroups: The variety $\mathcal{D}^{\ell}$ ($\mathcal{D}^{r}$) of left (right, resp.) distributive semigroups, i.e. the variety defined by the left (right, resp.) distributive law

$$(3) \quad xyz = xyxz \qquad ((3') \quad xyz = xzyz) \quad ,$$

the variety $\mathcal{D} = \mathcal{D}^{\ell} \cap \mathcal{D}^{r}$ of distributive semigroups and the variety $\mathcal{D}^{c}$ of commutative distributive semigroups.

It is shown in [11] that $\mathcal{D}(n)$ is a variety and that $\mathcal{D}^{\ell}(n)$, $\mathcal{D}^{r}(n)$ are proper quasivarieties of n-semigroups. We also know ([3]) that $\mathcal{D}^{c}$ is a member of an infinite set of varieties $\mathfrak{M}$ of commutative semigroups such that $\mathfrak{M}(n)$ is a variety. Concerning Ω-subalgebras, we have ([8]) that $\mathcal{D}^{c}(\Omega)$ is a variety of Ω-algebras for any operator domain Ω and ([9]) that $\mathcal{D}(\Omega)$ is a variety iff $|\Omega \setminus \Omega(0)| \leq 1$.

In this paper we are going to prove the following theorems:

THEOREM 1. *$\mathcal{D}^{\ell}(\Omega)$ is a variety iff $\Omega = \Omega(0) \cup \Omega(1)$* .

THEOREM 2. *$\mathcal{D}^{r}(\Omega)$ is a variety iff $\Omega = \Omega(0) \cup \Omega(1)$ and $|\Omega(1)| \leq 1$.*

THEOREM 3. *Let ω be an n-ary operator ($n \geq 3$). The following relations are satisfied:*

i) $\mathcal{D}^{c}(n) = \mathcal{D}^{c}(\omega)$

ii) $\mathcal{D}(\omega) \subset \mathcal{D}(n)$, *the inclusion is strict*

iii) *if $p \in \{\ell, r\}$, then neither of the classes $\mathcal{D}^{p}(n), \mathcal{D}^{p}(\omega)$ is a subclass of the other.*

Before giving the proofs of the theorems we shall state some lemmas which are obvious or easy to prove.

LEMMA 0.1. *Let V be an arbitrary variety of semigroups. If $\Omega = \Omega(0)$, then $V(\Omega)$ is a variety. If $\Omega \neq \Omega(0)$, then $V(\Omega)$ is a variety iff $V(\Omega \setminus \Omega(0))$ is a variety.*

Further on we assume that $\Omega(0) = \emptyset$ and that $\Omega \neq \emptyset$.

LEMMA 0.2. *If $\Omega \subseteq \Omega'$ and $\mathcal{D}^{\ell}(\Omega)$ ($\mathcal{D}^{r}(\Omega)$) is a proper quasivariety, then $\mathcal{D}^{\ell}(\Omega')$ ($\mathcal{D}^{r}(\Omega')$) is a proper quasivariety.*

Let ξ be a word in an arbitrary alphabet. Denote the number of occurrences of symbols in ξ by $d(\xi)$, the set of symbols occurring in ξ by $c(\xi)$ and the i-th symbol in ξ from left to the right (the right to the left) by $\xi(i)$ ($(i)\xi$, resp.).

Two words ξ and η in an arbitrary alphabet are said to be $\mathcal{D}^{\ell}$-correlated if:

a) $c(\xi) = c(\eta)$, $\xi(i) = \eta(i)$, $i = 1,2$, $(1)\xi = (1)\eta$

b) the sequences of the first occurrences of the symbols in ξ and η are equal (whereas $\xi(i)$ is the first occurrence of the symbol $\xi(i)$ in ξ if $\xi(j) \neq \xi(i)$ for every j, $j<i$)

c) if $\xi(k) \neq (1)\xi$ for every k, $0<k\leq d(\xi)$, then $\eta(k) \neq$ $\neq (1)\eta$ for every k, $0<k\leq d(\eta)$.

A word ξ is said to be the inverse of a word η if $d(\xi) =$ $= d(\eta)$ and $\xi(i) = (i)\eta$ for every i, $0<i\leq d(\xi) = d(\eta)$.

Two words ξ and η are said to be $\mathcal{D}^{r}$-correlated if their inverses are $\mathcal{D}^{\ell}$-correlated.

LEMMA 0.3. ([11]) A semigroup identity $\xi = \eta$ is valid in $\mathcal{D}^{\ell}$ ($\mathcal{D}^{r}$) iff ξ and η are $\mathcal{D}^{\ell}$-correlated ($\mathcal{D}^{r}$-correlated).

LEMMA 0.4. An Ω-identity $\xi = \eta$ is valid in $\mathcal{D}^{\ell}(\Omega)$ ($\mathcal{D}^{r}(\Omega)$) iff ξ and η are $\mathcal{D}^{\ell}$-correlated ($\mathcal{D}^{r}$-correlated).

1. PROOF OF THEOREM 1

First, let $\Omega = \Omega(1)$.

Let $\underline{A} = (A;\Omega)$ belong to the variety $\tilde{V}\mathcal{D}^{\ell}(\Omega)$. We shall show that $\underline{A}\in\mathcal{D}^{\ell}(\Omega)$, so that $\tilde{V}\mathcal{D}^{\ell}(\Omega) = \mathcal{D}^{\ell}(\Omega)$.

Let $\bar{\Omega} = \{\bar{\omega};\omega\in\Omega\}$ be a set of symbols such that $A\cap\bar{\Omega} = \emptyset$ and $\omega\neq\tau \Rightarrow \bar{\omega}\neq\bar{\tau}$ for every $\omega,\tau\in\Omega$. Let $F(.)$ be the free semigroup in the variety $\mathcal{D}^{\ell}$ generated by the set $\bar{\Omega}\cup A$. Say that $u,v\in F(.)$ are ω-neighbours or simply neighbours if $u=u_1\cdot\bar{\omega}\cdot b\cdot u_2$, $v=u_1\cdot a\cdot u_2$, for $\omega(b)=a$ in $\underline{A}$. Let $\approx$ be the transitive and reflexive extension of the relation of neighbourhood in $F(.)$.

LEMMA 1.1. Relation $\approx$ is a congruence on $F(.)$.

Proof Let $u_1\approx v_1$ and $u_2\approx v_2$. Then $u_1u_2\approx u_1v_2\approx v_1v_2$. ::

Let $D(.) = F(.)/\approx$. We shall show that $\underline{A}$ is a subalgebra of $D(.)$.

Define a value, denoted by $[\ ]$, as a partial mapping from $F(.)$ into A by: $[\bar{\omega}_1\bar{\omega}_2 \ldots \bar{\omega}_s a] = \omega_1\omega_2 \ldots \omega_s(a)$.

It is easy to see that:

1^o. $[\ ]$ is a well defined mapping, and that

2^o. if u,v are neighbours and u is in the domain of $[\ ]$, then v is also in the domain of $[\ ]$ and $[u] = [v]$.

The set A can be considered as a subset of D. For, if $a \approx b$ for some $a,b \in A$, then there is a sequence $a=u_0,u_1,\dots,u_{t-1},u_t=b$ such that u_i,u_{i+1} are neighbours $(0 \leq i \leq t-1)$ and $a=[a]=[u_1]= \dots$ $\dots =[b]=b$.

The fact that $\omega(a)=\bar{\omega}a$ for every $\omega \in \Omega$, $a \in A$ is obvious.

Let $\Omega \neq \Omega(1)$.

If ω is an n-ary operator in Ω $(n \geq 2)$, then the quasiidentity

$$(4) \quad \omega x^n = \omega y^{n-1}x \rightarrow \omega xz^{n-1} = \omega y^{n-1}\omega xz^{n-1}$$

is valid in $\mathcal{D}^\ell(\Omega)$. Namely, for an arbitrary subalgebra $\underline{A}=(A;\Omega)$ of a semigroup S(.) belonging to $\mathcal{D}^\ell$ whose elements a,b satisfy the relation $\omega(a^n) = \omega(b^{n-1}a)$, we have: $\omega(ac^{n-1}) = \bar{\omega}.a.c^{n-1} =$ $= \bar{\omega}.a^n.c^{n-1} = (\omega(a^n)).c^{n-1} = (\omega(b^{n-1}a)).c^{n-1} = \bar{\omega}.b^{n-1}.a.c^{n-1} =$ $= \bar{\omega}.b^{n-1}.a.c^{n-1} = \bar{\omega}.b^{n-1}.\bar{\omega}.a.c^{n-1} = \bar{\omega}.b^{n-1}.(\omega(ac^{n-1})) =$ $= \omega(b^{n-1}(\omega(ac^{n-1}))$ for every $c \in A$. On the other hand, the quasiidentity (4) is not a consequence of the identities in $\mathcal{D}^\ell(\Omega)$. To prove that, consider the algebra $\underline{A}=(A;\{\omega\})$, belonging to the variety $\tilde{V}\mathcal{D}^\ell(\omega)$ and generated by the set $\{a,b,c\}$, with one defining relation between the generators: $\omega(a^n)=\omega(b^{n-1}a)$. The relation $\omega(b^{n-1}\omega(ac^{n-1})) = \omega(ac^{n-1})$ is not valid in $\underline{A}$. Roughly speaking, starting with $\omega(ac^{n-1})$, the element a remains in the second and the element c in the last place after using the identities in $\mathcal{D}^\ell(\omega)$. So, the defining relation can not be used to change the element a in the second place, because of the element c in the last.

Thus, by Lemma 0.2 we have shown Theorem 1.

2. PROOF OF THEOREM 2

Let $\Omega = \{\omega\} = \Omega(1)$. Utilizing Lemma 0.4, we see that $\xi = \eta$ is an identity in $\mathcal{D}^r(\Omega)$ iff $(1)\xi = (1)\eta$. On the other hand, the class of Ω-algebras defined by the identity of that type is precisely $\mathcal{D}(\Omega)$ (see [9]). Thus, if $\underline{A} \in \tilde{V}\mathcal{D}^r(\Omega)$, then $\underline{A} \in \mathcal{D}(\Omega)$ and because $\mathcal{D}(\Omega) \subsetneq \mathcal{D}^r(\Omega)$, $\underline{A} \in \mathcal{D}^r(\Omega)$. We can now conclude that $\mathcal{D}^r(\Omega) = \mathcal{D}(\Omega)$ and that $\mathcal{D}^r(\Omega)$ is a variety.

Let $\Omega = \{\omega,\tau\} = \Omega(1)$. The quasiidentity

$$(5) \quad \omega x = \tau x \rightarrow \omega^2 x = \tau^2 x$$

is valid in $\mathcal{D}^r(\Omega)$ (proceed as for the quasiidentity (4)). An example of an algebra $\underline{A}=(A;\{\omega,\tau\})$belonging to $\tilde{V}\mathcal{D}^r(\Omega)$ and not satisfying (5) is the following: $A = \{a,b,c\}$, $\omega(x)=b$ for every $x\in A$, $\tau(a)=b$, $\tau(b)=c=\tau(c)$. We have $\omega(a)=\tau(a)$, but $\omega^2(a)=b\neq$ $\neq c=\tau^2(a)$. The algebra $\underline{A}$ belongs to $\tilde{V}\mathcal{D}^r(\Omega)$ because every Ω-term ξ, with $d(\xi)\geqslant 3$, has an interpretation in $\underline{A}$ equal to c for $\xi(1)=\tau$ and to b for $\xi(1)=\omega$.

Finally, let $\Omega = \{\omega\} = \Omega(n)$, $n\geqslant 2$. The quasiidentity

$$(6) \quad \omega xy^{n-1} = \omega x^n \rightarrow \omega xy^{n-1} = \omega y^{n-1}x$$

is valid in $\mathcal{D}^r(\Omega)$. To check that consider an Ω-algebra $\underline{A}$ belonging to $\mathcal{D}^r(\Omega)$ and its elements a and b satisfying the relation $\omega(ab^{n-1}) = \omega(a^n)$. We have: $\omega(ab^{n-1}) = \omega(a^n) = \bar{\omega}.a^n =$ $= \bar{\omega}.a^n.a = \omega(a^n).a = \omega(ab^{n-1}).a = \bar{\omega}.a.b^{n-1}.a = \bar{\omega}.b^{n-1}.a =$ $= \omega(b^{n-1}a)$.

In order to prove that the quasiidentity (6) is not a consequence of the identities valid in $\mathcal{D}^r(\Omega)$ define an ω-algebra $\underline{A}=(A;\omega)$ as follows: $A = \{a,b,c\}$,

$$\omega(d_1,d_2,\ldots,d_n) = \begin{cases} c & \text{if } d_n=c \text{ or } d_n=d_{n-1}=b \\ a & \text{otherwise} \end{cases} .$$

We have $\omega(bc^{n-1}) = c = \omega(b^n)$ and $\omega(bc^{n-1}) = c \neq a = \omega(c^{n-1}b)$. Thus (6) is not valid in $\underline{A}$ and it is obvious that $\underline{A}\in\tilde{V}\mathcal{D}^r(\Omega)$.

Now we can use Lemma 0.2 and the proof of Theorem 2 is completed.

3. PROOF OF THEOREM 3

1°. It is easy to see that u = v is an identity in $\mathcal{D}^c$ iff $c(u) = c(v)$ and $d(u),d(v)\geqslant 3$ or it is a trivial one. Thus $\xi =$ $= \eta$ is an identity in $\mathcal{D}^c(\omega)$ or $\mathcal{D}^c(n)$ iff $c(\xi) = c(\eta)$ or it is a trivial one. So, bearing in mind that both $\mathcal{D}^c(\omega)$ and $\mathcal{D}^c(n)$ are varieties ([8],[11]) we have proved the first part of Theorem 3.

2°. An identity u = v is valid in $\mathcal{D}$ iff it is trivial or $c(u) = c(v)$, $u(1) = v(1)$, $(1)u = (1)v$ and $d(u),d(v)\geqslant 3$. Thus:

a) $\xi = \eta$ is valid in $\mathcal{D}(\omega)$ iff $c(\xi) = c(\eta)$, $(1)\xi = (1)\eta$

and $d(\xi), d(\eta) \geq 3$, or it is trivial.

b) $\xi = \eta$ is valid in $\mathcal{D}(n)$ iff $c(\xi) = c(\eta)$, $(1)\xi = (1)\eta$, $d(\xi), d(\eta) \geq 3$ and $\xi(i) = \eta(j)$ where $\xi(i)$ and $\eta(j)$ are the first variable symbols occurring in ξ and η respectively, or it is trivial.

We can see that every identity valid in $\mathcal{D}(n)$ is valid in $\mathcal{D}(\omega)$. Thus, because both classes are varieties ([9],[11]), every algebra belonging to $\mathcal{D}(\omega)$ belongs to $\mathcal{D}(n)$. The converse assertion is evidently not true. For example, the identity $\omega xy^{n-1} = \omega yxy^{n-2}$ is valid in $\mathcal{D}(\omega)$ but not in $\mathcal{D}(n)$.

3^o. For an ω-term ξ, denote by $\bar{\xi}$ the semigroup term obtained from ξ by deleting every occurrence of an operator symbol in ξ. An analogue of Lemma 0.4 is the following assertion: an identity $\xi = \eta$ is valid in $\mathcal{D}^\ell(n)$ ($\mathcal{D}^r(n)$) iff $\bar{\xi}$ and $\bar{\eta}$ are $\mathcal{D}^\ell$-correlated ($\mathcal{D}^r$-correlated, resp.). Thus, it is easy to check that:

a) The identity $\omega xy^{n-1} = \omega x^{n-1}\omega xy^{n-1}$ is valid in $\mathcal{D}^\ell(\omega)$ and not in $\mathcal{D}^\ell(n)$. Conversely, $\omega x^n = \omega^2 x^{2n-1}$ is valid in $\mathcal{D}^\ell(n)$ but not in $\mathcal{D}^\ell(\omega)$.

b) The identity $\omega x\omega yx^{2n-3} = \omega^2 yx^{2n-2}$ is valid in $\mathcal{D}^r(\omega)$ but not in $\mathcal{D}^r(n)$. Conversely, $\omega x\omega y^{2n-2} = \omega^2 xy^{2n-2}$ is valid in $\mathcal{D}^r(n)$ but not in $\mathcal{D}^r(\omega)$.

Theorem 3 is proved.

REFERENCES

1. P.M.Cohn, Universal Algebra, D.Reidel, Publ.Comp. Dordrecht, Holand 1981

2. G.Čupona, n-subsemigroups of semigroups satisfying the identity $x^r=x^{r+m}$, God.Zbor.Mat.Fak. Skopje, 30, 1979, 5-14

3. G.Čupona, n-subsemigroups of some varieties of abelian semigroups,God.Zbor.Mat.Fak. Skopje, 31, 1981

4. G.Čupona, S.Markovski, Polynomial subalgebras, Algebraic conference, Novi Sad, 1981, 1-7

5. G.Čupona, G.Vojvodić, S.Crvenković, Subalgebras of abelian torsion groups, Algebraic conference, Novi Sad, 1981, 141-148

6. G.Čupona, G.Vojvodić, S.Crvenković, Subalgebras of semilattices, Univ. u Novom Sadu Zb.Rad.Prirod.-Mat.Fak. 10, 1980, 191-195

7. G.Čupona, S.Crvenković, G.Vojvodić, Subalgebras of commutative semigroups satisfying the law $x^r = x^{r+m}$, Univ. u Novom Sadu Zb.Rad. Prirod.-Mat.Fak. 11, 1981

8. S.Kalajdžievski, Subalgebras of commutative distributive semigroups, God.Zbor.Mat.Fak. Skopje,32, 1981

9. S.Kalajdžievski, Subalgebras of distributive semigroups "n-ary structures",Skopje, 1982, 223-228

10. А.И.Мальцев, Алгебраические системы, Мир, Москва, 1980

11. С.Марковски, За дистрибутивните полугрупи, Год.Збор. Мат.Фак. Скопје,30, 1979

12. Ю.К.Ребане, О претставлений универсальних алгебр в коммутативных полугрупах, Сибирск.Мат.Ж. 7, 1966, 878-885

13. Ю.К.Ребане, О претставлении универсальних алгебр в нильпотентних полугрупах, Сибирск Мат.Ж. 10, 1969, 947-949

Математички факултет

п.ф.504

91 000 Скопје

Југославија

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

IDEMPOTENT SEPARATING CONGRUENCES ON REGULAR SEMIGROUPS

Dragica N. Krgović

At the beginning of this note we establish some properties of full subsemigroups of a semigroup S, whose set of idempotents E is nonempty. Also, we consider some equivalence relations on a regular semigroup S, contained in Green's equivalence $\mathcal{L}$ (Proposition 2). We characterize an idempotent separating congruence ρ on a regular semigroup S in several ways in terms of congruences and the $\mathcal{H}$-equivalence (Theorem 1) - analogously to Petrich's characterization of any congruence on an inverse semigroup ([8], Lemma 5.2, Corollary 5.3).

For an orthodox semigroup S we introduce the notion of a normal subsemigroup of S and obtain some idempotent separating congruences on S, contained in $\mathcal{L}$ (Theorem 2). This leads to the characterization of any idempotent separating congruence on an orthodox semigroup S (Theorem 3). Feigenbaum [2] introduced the idempotent separating congruence (K) on an orthodox semigroup S. Here we obtain some equivalent expressions for (K) (Proposition 5). One of them shows that the congruence (K) can be defined without the condition $a'b \in K$.

If S is an inverse semigroup, then some of the statements mentioned lead to the characterization of any idempotent separating congruence on S (Theorem 5).

As special cases one obtains formulae of the greatest idempotent separating congruence μ on regular, orthodox and inverse semigroups respectively (Corollary 2, Corollary 4 and Corollary 5).

Let S be a semigroup with the set of idempotents $E \neq \emptyset$. Recall that a subsemigroup K of S is <u>full</u> if $E \subseteq K$. For any element a in S, V(a) will denote the set of inverses of a and $V(K) = \{x \in S \mid (\exists a \in K)\ x \in V(a)\}$.

The next statement reguires only routine verification, and the proof is omitted.

LEMMA 1. <u>Let</u> $a, b \in S$ <u>and</u> $a' \in V(a)$, $b' \in V(b)$. <u>Then</u>

i) $a = ab \Rightarrow ba' \in V(a)$.

ii) $a = ba \Rightarrow a'b \in V(a)$.

iii) $(a = abb' \vee b = a'ab) \Rightarrow b'a' \in V(ab)$.

The statement iii) of the preceding lemma follows also from Lemma 1.1 [10] .

The proof of the following lemma is based on Lemma 1.

LEMMA 2. Let K be a full subsemigroup of a semigroup S and $a,b\in S$. The following statements are equivalent.

(i) $(\exists k\in K)(\exists k'\in K)(a = kb \wedge b = k'a)$.

(ii) $(\forall a'\in V(a))(\exists b'\in V(b))(a'a = b'b \wedge ab'\in K)$.

(iii) $(\exists a'\in V(a))(\exists b'\in V(b))(a'a = b'b \wedge ab'\in K)$.

(iv) $(\forall b'\in V(b))(\exists a'\in V(a))(a'a = b'b \wedge ab'\in K)$.

Dually, we have

LEMMA 3. Let K be a full subsemigroup of a semigroup S and let $a,b\in S$. The following statements are equivalent.

(i) $(\exists k\in K)(\exists k'\in V(k))(a = bk' \wedge b = ak)$.

(ii) $(\forall a'\in V(a))(\exists b'\in V(b))(aa' = bb' \wedge a'b\in K)$.

(iii) $(\exists a'\in V(a))(\exists b'\in V(b))(aa' = bb' \wedge a'b\in K)$.

(iv) $(\forall b'\in V(b))(\exists a'\in V(a))(aa' = bb' \wedge a'b\in K)$.

Consider now regular semigroups. The next statement may be found in [3], § .II.4.

LEMMA 4. Let S be a regular semigroup. Let $a,b\in S$ and $a'\in V(a)$. Then

(i) $a\mathcal{L}b \Leftrightarrow (\exists b'\in V(b))(a'a = b'b)$.

(ii) $a\mathcal{H}b \Leftrightarrow (\exists b'\in V(b))(a'a = b'b \wedge aa' = bb')$.

PROPOSITION 1. Let S be a regular semigroup and $a,b\in S$. Let K be a full subsemigroup of S. The following statements are equivalent.

(i) $(\exists k,h\in K)(\exists k'\in V(k))(\exists h'\in V(h))(a=kb=bh \wedge b=k'a=ah)$.

(ii) $(\forall a'\in V(a))(\exists b'\in V(b))(a'a=b'b \wedge aa'=bb' \wedge a'b,ab'\in K)$.

(iii) $(\exists a'\in V(a))(\exists b'\in V(b))(a'a=b'b \wedge aa'=bb' \wedge a'b,ab'\in K)$.

(iv) $(\forall b'\in V(b))(\exists a'\in V(a))(a'a=b'b \wedge aa'=bb' \wedge a'b,ab'\in K)$.

Proof. (i) $\Rightarrow$ (ii). Let $a'\in V(a)$. According to Lemma 2, $a = kb$ and $b = k'a$ implies $a'a = b''b$ for some $b''\in V(b)$, i.e. $a\mathcal{L}b$. By Lemma 3, $a=bh'$ and $b=ah$ implies $aa'=bb^*$ and $a'b\in K$ for some $b^*\in V(b)$, i.e. $a\mathcal{R}b$. So, we have $a\mathcal{H}b$. Then, by Lemma 4, $a'a=b'b$ and $aa'=bb'$ for some $b'\in V(b)$. Since K is a full subsemigroup of S we have $ab' = kbb'\in K$.

The implications "(ii) $\Rightarrow$ (iii)" and "(iv) $\Rightarrow$ (iii)" are trivial.

(iii) $\Rightarrow$ (i) This follows from Lemma 2 and Lemma 3.

(i) $\Rightarrow$ (iv). Let $b'\in V(b)$. According to Lemma 2, $a = kb$ and

$b=k'a$ implies $a''a=b'b$ and $ab'\in K$ for some $a''\in V(a)$, i.e. $a\mathcal{L}b$. By Lemma 3, $a=bh'$ and $b=ah$ implies $aa^*=bb'$ for some $a^*\in V(a)$, i.e. $a\mathcal{R}b$. So, we have $a\mathcal{H}b$ so, by Lemma 4, $a'a=b'b$ and $aa'=bb'$ for some $a'\in V(a)$. Also, $a'b=a'ah\in K$.

Definition 1. For an equivalence relation α on a regular semigroup S, we define the kernel and the trace of α by

$$\ker\alpha = \{a\in S \mid (\exists e\in E)\ a\alpha e\}$$
$$\operatorname{tr}\alpha = \alpha|_E$$

respectively.

The next lemma follows from Lemma 4.

LEMMA 5. Let α be an equivalence relation on a regular semigroup S. Then

i) $\alpha\subseteq\mathcal{L} \Rightarrow \ker\alpha = \{a\in S \mid (\exists a'\in V(a))\ a\alpha a'a\}$.

ii) $\alpha\subseteq\mathcal{H} \Rightarrow \ker\alpha = \{a\in S \ (\exists a'\in V(a))(a\alpha a'a \wedge a'a = aa')$.

Definition 2. Let S be a regular semigroup. A subsemigroup K of S is inverse-closed if $V(K)\subseteq K$.

PROPOSITION 2. Let K be a full inverse-closed subsemigroup of a regular semigroup S and α an equivalence relation on S such that $\alpha\subseteq\mathcal{L}$. The relation (K_α) defined on S by

$$a(K_\alpha)b \Leftrightarrow a\alpha b \wedge (\exists b'\in V(b))\ ab'\in K$$

is an equivalence relation on S for which $\ker(K_\alpha)=K\cap\ker\alpha$ and $\operatorname{tr}(K_\alpha) = \operatorname{tr}\alpha$.

Proof. The relation (K_α) is reflexive because $E\subseteq K$ and α is reflexive. Let $a(K_\alpha)b$ i.e. $a\alpha b$ and $ab'\in K$ for some $b'\in V(b)$. According to Lemma 4, $a'a=b'b$ for some $a'\in V(a)$. Then $b=ba'a$ implies, by Lemma 1, $ba'\in V(ab')$. Since K is inverse-closed we have $ba'\in K$. Thus (K_α) is symmetric. Let $a(K_\alpha)b$ and $b(K_\alpha)c$. Then $a\alpha b$ and $b\alpha c$ implies $a\alpha c$. Also, ab', $bc'\in K$ for some $b'\in V(b)$ and $c'\in V(c)$. By Lemma 4, $a\alpha b$ implies $a'a=b'b$ for some $a'\in V(a)$. Then $ab'bc'\in K$ implies $aa'ac'\in K$, i.e. $ac'\in K$. Thus $a(K_\alpha)c$, so (K_α) is transitive. Therefore (K_α) is an equivalence relation on S.

Let $a\in\ker(K_\alpha)$ i.e. $a(K_\alpha)e$ for some $e\in E$. Then $a\alpha e$ and $ae'\in K$ for some $e'\in V(e)$, so $\ker(K_\alpha)\subseteq\ker\alpha$. According to Lemma 4, $a'a=e'e$ for some $a'\in V(a)$. Then $a=a(a'a)=ae'e\in K$. Thus $\ker(K_\alpha)\subseteq K$. Therefore $\ker(K_\alpha)\subseteq K\cap\ker\alpha$.

Conversely, let $k\in K\cap\ker\alpha$. According to Lemma 5, $k\alpha k'k$ for some $k'\in K$. Since $k(k'k)=k\in K$ we have $k(K_\alpha)k'k$. Thus

$k \in \ker(K_\alpha)$. Therefore $K \cap \ker\alpha \subseteq \ker(K_\alpha)$.

Let $e, f \in E$ such that $e(K_\alpha)f$. Then $e\alpha f$. Conversely, let $e\alpha f$. Since $f \in V(f)$ and $ef \in K$ we have $e(K_\alpha)f$. Therefore $\mathrm{tr}(K_\alpha) = \mathrm{tr}\alpha$.

COROLLARY 1. Let K be a full inverse-closed subsemigroup of a regular semigroup S. The relation (K_μ) defined on S by

$$a(K_\mu)b \Longleftrightarrow (a\mu b \wedge (\exists b' \in V(b))\ ab' \in K)$$

is an idempotent separating equivalence relation on S for which $\ker(K_\mu) = K \cap \ker\mu$.

Next we consider idempotent separating congruences on a regular semigroup S.

LEMMA 6. ([4]). If S is regular, then a congruence ρ on S is idempotent separating if and only if $\rho \subseteq \mathcal{H}$.

The next proposition follows from Lemma 5 and Lemma 6.

PROPOSITION 3. Let ρ be an idempotent separating congruence on a regular semigroup S. The following statements are equivalent.

(i) $a \in \ker\rho$.

(ii) $(\exists a' \in V(a))(a\rho a'a \wedge a'a = aa')$.

(iii) $(\exists a' \in V(a))\ a\rho a'a\rho a'$.

(iv) $(\exists a' \in V(a))\ a\rho a'a$.

(v) $(\exists a' \in V(a))\ a\rho aa'$.

The following theorem describes idempotent separating congruences on a regular semigroup. The corresponding characterization of a congruence on an inverse semigroup is due to Petrich ([8], Lemma 5.2, Corollary 5.3).

THEOREM 1. Let ρ and ξ be idempotent separating congruences on a regular semigroup S such that $\rho \subseteq \xi$. The following statements are equivalent.

(i) $a\rho b$.

(ii) $a\xi b \wedge (\exists b' \in V(b))\ ab' \in \ker\rho$.

(iii) $a\mu b \wedge (\exists b' \in V(b))\ ab' \in \ker\rho$.

(iv) $a\mathcal{H}b \wedge (\exists b' \in V(b))\ ab' \in \ker\rho$.

(v) $(\exists a' \in V(a))(\exists b' \in V(b))(a'a = b'b \wedge aa' = bb' \wedge ab' \in \ker\rho)$.

Proof. (i) $\Rightarrow$ (ii). Let $a\rho b$. Then $a\xi b$ and $ab'\rho bb'$ for every $b' \in V(b)$, so that $ab' \in \ker\rho$.

(ii) $\Rightarrow$ (iii). Let $a\xi b$. Then $a\mu b$ because μ is the greatest idempotent separating congruence on S.

(iii) $\Rightarrow$ (iv) $\Rightarrow$ (v). It follows from Lemma 6 and Lemma 4.

(v) $\Rightarrow$ (i). Let $a'a = b'b$, $aa' = bb'$ and $ab' \in \ker\rho$ for some $a' \in V(a)$ and $b' \in V(b)$. Then $a'a = b'b \Rightarrow (a\mathcal{L}b \wedge a'\mathcal{R}b') \Rightarrow$ $\Rightarrow (ab'\mathcal{L}bb' \wedge aa'\mathcal{R}ab')$. Since $aa' = bb'$ we have $ab'\mathcal{H}bb'$. But, $ab' \in \ker\rho$ implies that $ab'\rho e$ for some $e \in E$. Then $ab'\mathcal{H}e$, which implies $bb' = e$. Therefore $ab'\rho bb'$ so that

$$a = aa'a = ab'b \;\rho\; bb'b = b.$$

COROLLARY 2. <u>Let</u> S <u>be</u> <u>a</u> <u>regular</u> <u>semigroup</u>. <u>The</u> <u>following</u> <u>statements</u> <u>are</u> <u>equivalent</u>.

(i) $a\mu b$.

(ii) $a\mathcal{H}b \wedge (\exists b' \in V(b))\ ab' \in \ker\mu$.

(iii) $(\exists a' \in V(a))(\exists b' \in V(b))\ a'a = b'b,\ aa' = bb',\ ab' \in \ker\mu$.

COROLLARY 3. <u>Let</u> S <u>be</u> <u>a</u> <u>regular</u> <u>semigroup</u> <u>and</u> K <u>a</u> <u>non-empty</u> <u>subset</u> <u>of</u> S <u>such</u> <u>that</u> $K \subseteq \ker\mu$. <u>The</u> <u>following</u> <u>statements</u> <u>are</u> <u>equivalent</u>.

(i) $a\mu b \wedge (\exists b' \in V(b))\ ab' \in K$.

(ii) $a\mathcal{H}b \wedge (\exists b' \in V(b))\ ab' \in K$.

(iii) $(\exists a' \in V(a))(\exists b' \in V(b))(a'a = b'b \wedge aa' = bb' \wedge ab' \in K)$.

The next proposition may be found in [2] (Theorem 3.1).

PROPOSITION 4. <u>If</u> S <u>is</u> <u>an</u> <u>orthodox</u> <u>semigroup</u> <u>then</u>

$$a\mu b \Leftrightarrow (\exists a' \in V(a))(\exists b' \in V(b))(a'a = b'b, aa' = bb', a'b, ab' \in \ker\mu).$$

Corollary 2 shows that the condition $a'b \in \ker\mu$ in Proposition 4 is not necessary.

Recall that a subsemigroup K of a regular semigroup S is <u>self-conjugate</u> if $a'Ka \subseteq K$ for all $a \in S$ and all $a' \in V(a)$.

The next lemma follows from Lemma 4.

LEMMA 7. <u>Let</u> K <u>be</u> <u>an</u> <u>inverse-closed</u> <u>self-conjugate</u> <u>subsemigroup</u> <u>of</u> <u>a</u> <u>regular</u> <u>semigroup</u> S. <u>Let</u> $a, b \in S$ <u>and</u> $a' \in V(a)$, $b' \in V(b)$. <u>Then</u>

$$(a\mathcal{L}b \wedge ab' \in K) \Rightarrow a'b \in K.$$

Let S be an orthodox semigroup and ρ a congruence on S. Then $\ker\rho$ is a full self-conjugate subsemigroup of S. Lemma 2.3, [6] shows that $\ker\rho$ is inverse-closed.

<u>Definition 3</u>. Let S be an orthodox semigroup. A subsemigroup K of S is <u>normal</u> if K is full, self-conjugate and inverse--closed.

<u>Remark</u>. If ρ is a congruence on an orthodox semigroup S then $\ker\rho$ is a normal subsemigroup of S.

THEOREM 2. Let K be a normal subsemigroup of an orthodox semigroup S and ρ a congruence on S such that $\rho \subseteq \mathcal{L}$. The relation (K_ρ) defined on S by

$$a\,(K_\rho)\,b \Leftrightarrow (a\rho b \;\wedge\; (\exists b' \in V(b))\; ab' \in K)$$

is a congruence on S for which $\ker(K_\rho) = K \cap \ker\rho$ and $\operatorname{tr}(K_\rho) = \operatorname{tr}\rho$.

Proof. According to Proposition 2, it suffices to prove that (K_ρ) is compatible. Let $a\,(K_\rho)\,b$ and $c \in S$. Then $a\rho b$ and $ab' \in K$ for some $b' \in V(b)$. According to Lemma 4, $a'a = b'b$ for some $a' \in V(a)$. Then $acc'b' = acc'b'bb' = acc'a'ab' = (acc'a')ab' \in K$. Since $c'b' \in V(bc)$ and $a\rho b \Rightarrow (ac)\rho(bc)$ we have $ac\,(K_\rho)\,bc$. Also $a\rho b \Rightarrow ca\,\rho\,cb$. Since $cab'c' \in K$ and $b'c' \in V(cb)$ we have $ca\,(K_\rho)\,cb$.

The main characterisation theorem for idempotent separating congruences on an orthodox semigroup follows.

THEOREM 3. Let S be an orthodox semigroup and K a normal subsemigroup of S such that $K \subseteq \ker\mu$. The relation (K_μ) defined on S by

$$a(K_\mu)\,b \Leftrightarrow a\mu b \;\wedge\; (\exists b' \in V(b))\; ab' \in K$$

is an idempotent separating congruence on S and $\ker(K_\mu) = K$.

Conversely, if ρ is an idempotent separating congruence on S then $\ker\rho$ is a normal subsemigroup of S, $\ker\rho \subseteq \ker\mu$ and $\rho = (K_\mu)$, where $K = \ker\rho$.

Proof. The direct part follows from Theorem 2. According to Remark and Theorem 1, the converse is true.

The following theorem is due to Feigenbaum [2].

THEOREM 4. ([2], Theorem 3.3). Let S be an orthodox semigroup, $\mathcal{K} = \{K \subseteq S \mid E \subseteq K \subseteq \ker\mu$ and K is a self-conjugate regular subsemigroup of S$\}$ and the relation (K) defined on S by

$$a(K)b \Leftrightarrow (\exists a' \in V(a))(\exists b' \in V(b))(a'a = b'b \wedge aa' = bb' \wedge ab', a'b \in K).$$

The map $K \to (K)$ is a 1 - 1 order preserving map of $\mathcal{K}$ onto the set of idempotent separating congruences on S.

According to Lemma 3, [5], we have

$$\mathcal{K} = \{K \subseteq S \mid E \subseteq K \subseteq \ker\mu \text{ and K is a normal subsemigroup of S}\}.$$

Corollary 3, Lemma 7 and Proposition 1 imply the following statement.

PROPOSITION 5. Let K be a normal subsemigroup of an orthodox semigroup such that $K \subseteq \ker\mu$. The following statements are equivalent.

(i) $a\,(K)\,b$.

(ii) $(\exists a' \in V(a))(\exists b' \in V(b))(a'a = b'b \wedge aa' = bb' \wedge ab' \in K)$.

(iii) $(\exists k,h \in K)(\exists k' \in V(k))(\exists h' \in V(h))(a = kb = bh \wedge b = k'a = ah)$.

(iv) $a\,(K_\mu)\,b$.

(v) $a \mathcal{H} b \wedge (\exists b' \in V(b))\, ab' \in K$.

COROLLARY 4. Let S be an orthodox semigroup. Then
$a\mu b \Leftrightarrow (\exists k,h \in \ker\mu)(\exists k' \in V(k))(\exists h' \in V(h))(a = kb = bh' \wedge b = k'a = ah)$.

If S is an inverse semigroup then $\ker\mu = E\zeta$, where $E\zeta$ is the centralizer of E [8]. Since $E\zeta$ is a semilattice of groups we have $aa^{-1} = a^{-1}a$ for every $a \in E\zeta$. Suppose that $K \subseteq E\zeta$ and $a,b \in S$ such that $a^{-1}a = b^{-1}b$ and $ab^{-1} \in K$. Then $aa^{-1} = aa^{-1}aa^{-1} = ab^{-1}ba^{-1} = ba^{-1}ab^{-1} = bb^{-1}bb^{-1} = bb^{-1}$, because $ab^{-1} \in E\zeta$ and $ba^{-1} = (ab^{-1})^{-1}$. Therefore, according to Theorem 3, Proposition 5 and Lemma 2, we have

THEOREM 5. Let S be an inverse semigroup and $\mathcal{K}$ the set of all normal subsemigroups contained in $E\zeta$. Let $K \in \mathcal{K}$. The relation ρ_K defined on S by

$$a\,\rho_K\,b \Leftrightarrow (\exists k \in K)\,(a = kb \wedge b = k^{-1}a)$$

is an idempotent separating congruence on S and $\ker\rho_K = K$.

Conversely, if ρ is an idempotent separating congruence on S, then $\ker\rho \in \mathcal{K}$ and $\rho = \rho_{\ker\rho}$.

Notice that the preceding theorem is also the consequence of III.3.6 Theorem [9], Theorem 4.4 [8] and Lemma 2.

COROLLARY 5. Let S be an inverse semigroup. Then

$$a\mu b \Leftrightarrow (\exists k \in E\zeta)(a = kb \wedge b = k^{-1}a).$$

REFERENCES

1. A.H. Clifford, and G.B. Preston, "The Algebraic Theory of Semigroups", Amer. Math. Soc., Providence, R.I., Vol.I, 1961; Vol. II, 1967.

2. F. Feigenbaum, Kernels of orthodox semigroup homomorphisms, J. Austral. Math. Soc. 22 (Series A) (1976), 234-245.

3. J.M. Howie, "An Introduction to Semigroup Theory", Academic Press, London/New York/San Francisco, 1976.

4. G. Lallement, Congruences et équivalences de Green sur un demi-groupe régulier, C.R. Acad. Sci. Paris, Sér.A, 262 (1966), 613-616.

5. D.R. LaTorre, Group congruences on regular semigroups, Semigroup Forum, 24 (1982), 327-340.

6. J. Meakin, Congruences on orthodox semigroups, J.Austral. Math. Soc. 12(1971).

7. M. Petrich, "Introduction to Semigroups", Merill, Columbus, 1973.

8. M. Petrich, Congruences on inverse semigroups, J.Algebra, 55 (1978), 231-256.

9. M. Petrich, "Inverse semigroups", Reprint.

10. N.R.Reilly and H.E.Scheiblich, Congruences on regular semigroups, Pacific J.Math. 23(1967), 349-360.

Matematički institut
Knez Mihajlova 35
11000 Beograd

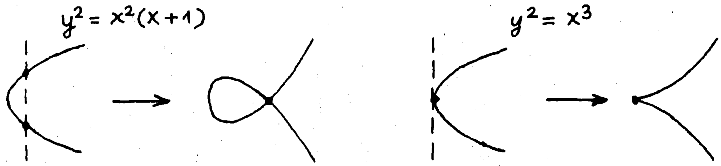
Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

ON UNIBRANCHED RINGS AND A CRITERION FOR IRREDUCIBILITY IN THE FORMAL POWER SERIES RING

Aleksandar Lipkovski

1. An important tool in classification of algebraic singularities is the process of normalisation. It is a morphism of varieties $f: X \to Y$, locally of the type $f: \mathrm{Spec}\,B \to \mathrm{Spec}\,A$ where $A \subset B$ is an extension of domains, $f(P) = P \cap A$ and the ring B is the integral closure of the ring A. A natural discrete parameter associated with a singular point $y \in Y$ is the number of points in X which lay above y. A simple example is given by normalisation of the following two plane singularities.



In the first case this number is 2, in the second 1. A singularity for which this number is 1 may be called unibranched. Since the points of the fibre $f^{-1}(y)$ correspond to the maximal ideals in the integral closure of the local ring $\mathcal{O}_y$ of the point $y \in Y$, the local ring of such a singular point must have a property that its integral closure has just one maximal ideal. This makes the following definition reasonable.

Definition 1.1. A local domain is unibranched, if its integral closure is a local ring.

This class of local rings is a natural generalisation of the class of integrally closed local rings. As far as I know, for the first time they appeared in [8](p.127). Not much is known about such rings. Here we list some of the known facts.

THEOREM 1.2. *Let A be a local domain with field of fractions*

K. A is unibranched if and only if every overring B of A contained in K, which is a finite A-module, is local (see [3]p.403, [6]p.151).

THEOREM 1.3. If $(A_\alpha, h_{\alpha\beta})$ is an inductive system of unibranched rings A_α with injective local homomorphisms $h_{\alpha\beta}$, then the direct limit ring $A = \varinjlim A_\alpha$ is unibranched (see [6]p.151).

THEOREM 1.4. Property of being unibranched is not hereditary with respect to localisation (see example in [6]p.149).

A local domain is called analytically irreducible if its completion $\widehat{A}$ (in adical topology of its maximal ideal) has no zero divisors. We say that A is a geometrical ring if it is a finite algebra over an algebraically closed field of characteristic zero. In a geometrical local domain A, the number of prime divisors of the zero ideal in $\widehat{A}$ is equal to the number of maximal ideals in the integral closure A' of A (see [10]p.135). Therefore we have the following

THEOREM 1.5. Let A be a geometrical local domain. Then, A is unibranched $\Leftrightarrow$ A is analytically irreducible (see also [7]).

In the general case only the implication " A analytically irreducible $\Rightarrow A$ unibranched" remains valid (see [3]p.403, [6] p.151).

In [8] it is mentioned one more result on unibranched rings, belonging to W.-L. Chow, but as far as I know there is no published proof of it. It may be of some interest to give it here.

THEOREM 1.6. Let $(A,\mathfrak{m})$ be a Noetherian unibranched local domain. Then the projective spectrum $Proj(GrA)$ of the ring $GrA = \bigoplus_{n\geq 0} \mathfrak{m}^n/\mathfrak{m}^{n+1}$ is connected.

Proof. Let k be the residue class field of the ring A, $S = \bigoplus_{n\geq 0} \mathfrak{m}^n$ and $Proj\,S$ the blowing up of $Spec\,A$ in the closed point $\mathfrak{m}$. There is a canonical birational projective epimorphism $f: Proj\,S \to Spec\,A$ which has a Stein factorisation (see [11] p.358) $Proj\,S \xrightarrow{g} Z \xrightarrow{h} Spec\,A$ where h is finite and $g_*\mathcal{O}_S = \mathcal{O}_Z$. Therefore h is affine, $Z = Spec\,B$ where $\widetilde{B} = f_*\mathcal{O}_S$, B is a finite A-module. Since $Spec\,A$ is irreducible, we may consider Z to be irreducible too. By extending a base to

$Spec\,k$ we get

$$P = Proj\,S \times_{Spec\,A} Spec\,k \cong Proj(Gr\,A)$$

and a diagram

$$\begin{array}{ccccc} P & \xrightarrow{p} & Spec\,B/mB & \xrightarrow{q} & Spec\,k \\ \downarrow{\scriptstyle \ell} & & \downarrow{\scriptstyle j} & & \downarrow{\scriptstyle i} \\ Proj\,S & \xrightarrow{g} & Spec\,B & \xrightarrow{h} & Spec\,A \end{array}$$

in which all the squares are products. But $g_*\mathcal{O}_S=\mathcal{O}_B$ and (see [11] p.327) $p_*\mathcal{O}_P=p_*\ell^*\mathcal{O}_S=j^*g_*\mathcal{O}_S=j^*\mathcal{O}_B=\mathcal{O}_{B/mB}$. Therefore, the morphism p has connected fibres (see [11]p.357). But A is unibranched, therefore B is local, $Spec\,B/mB$ consists of one point and the fibre above this point is exactly $P=Proj(Gr\,A)$. Q.E.D.

2. The interest for this class of rings arises also in a global situation, when investigating homeomorphisms of varieties in their Zariski topologies. In the case of curves this topology is cofinite. Therefore each two algebraic curves are homeomorphic (see [11]pp.40,52). It is another question if this homeomorphism could be achieved by an algebraic morphism and how much could such a morphism differ from an isomorphism. Yet more complicated is the situation in higher dimensions. Therefore, there is some interest in investigating morphisms $f:X\to Y$ which are homeomorphisms in Zariski topologies. In algebraic language this is equivalent to ring extensions $A\subset B$ which induce homeomorphisms of spectra $Spec\,A\approx Spec\,B$ and which therefore may be called homeomorphic extensions. In [9] the following is proved.

THEOREM 2.1. <u>If</u> A <u>and</u> B <u>are geometrical rings, a homeomorphic extension</u> $A\subset B$ <u>must be a finite extension</u>.

It can be treated somewhat more general case of ring extensions $A\subset B$ which induce a bijection of spectra. In other words, over each prime ideal in A lays exactly one prime ideal in B. In [5] such extensions are called unibranched and in [1] the case of equality $Spec\,A=Spec\,B$ is treated. In dimension 1 homeomorphisms and bijections of spectra are of course the same, but it is not so in higher dimensions (see example in [9]).

The connection between these notions and unibranched singularities is the following. If $f:X\to Y$ is the normalisation of Y and f is a bijection, then Y could have only unibranched singularities.

3. Let X be a smooth n-dimensional algebraic variety (the ambient space), $S\subset X$ a hypersurface and $y\in S$. Let $\mathcal{O}_{y,S}=\mathcal{O}_{y,X}/(f)$ be a local ring of the point y on S, $f=f(X_1,\dots,X_n)\in K[X_1,\dots,X_n]$ the local equation of S in X. By completion we get $\hat{\mathcal{O}}_{y,S}=K[[X_1,\dots,X_n]]/(f)$ where $K[[X_1,\dots,X_n]]$ is the ring of formal power series in n indeterminates over K. From the theorem 1.5. it follows that $y\in S$ is a unibranched singular point if and only if the polynomial f is irreducible in the formal power series ring (we say analytically irreducible). Therefore in the classification of such singularities it is of certain interest to find a criterion for analytical irreducibility. In the case $n=2$ such a criterion, an algorithm, exists.

LEMMA 3.1. <u>If the series $f\in K[[X,Y]]$ is irreducible, its lowest order form must be a complete power of a linear form</u> (see [4]p.11,[11]p.61).

Let now $f=\sum_{(p,q)} f_{pq}X^pY^q$ be the formal power series, $\Delta(f)$ be the set $\{(p,q)\mid p,q\in \mathbb{N}\cup\{0\},\ f_{pq}\neq 0\}$. Consider the boundary of the convex hull of the set $\Delta(f)+\mathbb{R}^2$. If $f\neq X\cdot u$ and $f\neq Y\cdot v$, this boundary consist of two halflines along the coordinate axes and a compact polygonal line. This polygonal line is called the Newton polygon for f and denoted $N(f)$ (see [2]p. 505,[4]p.89).

LEMMA 3.2. <u>If f is irreducible in $K[[X,Y]]$, its Newton polygon is a straight line segment</u> (see [4]p.90).

Set $L(f)=\sum_{(p,q)\in N(f)} f_{pq}X^pY^q$ and for an irreducible f let $N(f)$ be the segment $\overline{(m,0)(0,n)}$. We may consider $n\leq m$.

LEMMA 3.3. <u>If f is irreducible and $d=M(m,n)$, then there exist $a,b\in K\setminus\{0\}$ such that</u> $L(f)=a(Y^{n/d}-bX^{m/d})^d$ (see [4]p.91).

Let's now briefly describe the algorithm mentioned above. Suppose that n divides m. By setting $Y'=Y-bX^{m/n}$ we get a new series f' with $n'=n$ and $m'<m$. Repeating this and eventually interchanging X and Y (to have always $n\leq m$) we arrive to the case when n does not divide m. Now set $e_0=n$, $e_1=M(m,n)<e_0$

and $m'=m/e_1$, $n'=n/e_1$. Find the (unique) solution of the Diophantine equation $|rm'-sn'|=1$ with $0\leq s\leq m'/2$, $0\leq r\leq n'/2$ and set $X=U^{n'}V^{r}$, $Y=U^{m'}V^{s}$. We get a new series $f_1'(U,V)=$ $=\sum_{(p,q)} f_{T^{-1}(p,q)} U^{p-k}V^{q-\ell}$ where T is the transformation of the plane $\mathbb{N}^2$ given by $(p,q)\mapsto(pn'+qm', pr+qs)$, $k=mn/e_1$ and $\ell=\min(rm,sn)$. Now there exist $a,b\in K\setminus\{0\}$ such that $L(f_1')=a(V-b)^{e_1}$ (lemma 3.3.). Set $X=U$, $Y=V-b$. We get the series $f_1(X,Y)$ with $n=e_1$. By continuing this process we get the natural numbers $e_0>e_1>e_2>\ldots$ so the process must finish after a finite number of steps.

THEOREM 3.4. <u>If the series $f\in K[[X,Y]]$ is irreducible, the described algorithm can be completely applied</u> (see [4]p.101).

COROLLARY 3.5. Let $f(X,Y)$ be a polynomial. <u>If the described algorithm for f fails in some step, f is analytically reducible</u>.

As an illustration we give here some examples.

<u>Example</u> 3.6. The polynomial $Y^4+2X^3Y^2+X^6-X^5Y$ is analytically irreducible.

Applying the algorithm, we have $m=6$, $n=4$, $e_0=4$, $e_1=2$. Then $L(f)=(Y^2+X^3)^2$, $r=s=1$, $k=12$, $\ell=4$ and $T:(p,q)\mapsto(2p+3q,p+q)$. We get $f_1'=(V+1)^2-UV^2$, $f_1=-X+Y^2+2XY-XY^2$. The last polynomial has $m=1$, $n=2$, $e_3=1$ and this is the end of the algorithm.

<u>Example</u> 3.7. The polynomial $Y^4+2X^3Y^2+X^6-X^4Y^2$ is reducible. We get $f_1'=(V+1)^2-U^2V^2$ and $f_1=-X^2+Y^2+2X^2Y-X^2Y^2$. Now $L(f_1)=$ $=Y^2-X^2=(Y-X)(Y+X)$ and f_1 (and f too) is analytically reducible. Naturally, this could be seen easily: $f=(Y^2+X^3+X^2Y)(Y^2+X^3-X^2Y)$.

<u>Example</u> 3.8. The polynomial $Y^4+X^3Y^2+X^6-X^5Y$ is analytically reducible, despite its irreducibility.

Here it is $L(f)=Y^4+X^3Y^2+X^6\neq a(Y^2-bX^3)^2$ for any a, b and the algorithm cannot be applied. We have

$$f=\left[Y^2+\left(\tfrac{1}{2}+\tfrac{i\sqrt{3}}{2}\right)X^3-\tfrac{i}{\sqrt{3}}X^2Y+\ldots\right]\left[Y^2+\left(\tfrac{1}{2}-\tfrac{i\sqrt{3}}{2}\right)X^3+\tfrac{i}{\sqrt{3}}X^2Y+\ldots\right]$$

Any generalisation of this algorithm in the case of more than two variables would be of great interest. Regretfully, lemma 3.1. fails already in the case of three variables, as the following simple example shows.

Example 3.9. The polynomial $f(X,Y,Z) = YZ + X^3$ has a lowest degree form YZ which is a product of two nonproportional linear forms. Although, if it were $YZ+X^3 = (Y+g_2+\dots)(Z+h_2+\dots)$ we would get $g_2Z+h_2Y = X^3$. But $g_2Z+h_2Y = (aX^2+\dots)Z+(bX^2+\dots)Y$ and it could not contain the term X^3.

REFERENCES

1. D. Anderson, D. Dobbs, Pairs of rings with the same prime ideals, Can. J. Math. 32(1980), 362-384.
2. E. Brieskorn, H. Knörrer, Ebene algebraische Kurven, Birkhäuser, Basel-Boston-Stuttgart 1981.
3. Н. Бурбаки, Коммутативная алгебра, Мир, Москва 1971.
4. A. Campillo, Algebroid Curves in Positive Characteristic, Lect. Notes Math. 813(1980).
5. D. Dobbs, Divided Rings & Going Down, Pacific J. Math 67 (1976), 353-363.
6. A. Grothendieck, J. Dieudonné, Eléments de Géométrie algébrique I, 2.ed., Springer, Berlin-Heidelberg-New York 1971.
7. A.Grothendieck, J. Dieudonné, Eléments de Géométrie algébrique IV, Publ. Math. IHES 24(1965).
8. А. Гротендик, Теория когомологий абстрактных алгебраических многообразий, в сборнике Международный математический конгресс в Эдинбурге 1958, Гос.изд.физ.-мат.лит., Москва 1962.
9. А. Липковски, Гомеоморфное расширение геометрических колец пело, Publ. Inst. Mat. 32(1982), 105-107.
10. M. Nagata, Local Rings, Interscience, New York 1962.
11. Р. Хартсхорн, Алгебраическая геометрия, Мир, Москва 1981.

Institut za matematiku
Prirodno matematički fakultet
Studentski trg 16
11000 Beograd

Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

n-SUBSEMIGROUPS OF SEMIGROUPS WITH NEUTRAL PROPERTIES

Smile Markovski

In the paper [1] (this volume), G.Čupona give a sufficient condition the class of n-subsemigroups of semigroups belonging to a semigroup variety to be also a variety of n-semigroups. Here we consider some varieties of semigroups which do not satisfy the mentioned condition, but the class of their n-subsemigroups are varieties of n-semigroups as well.

1. THE VARIETY OF SEMIGROUPS $\mathcal{O}_{k,i}$. The variety of semigroups $\mathcal{O}_{k,i}$ is defined by the semigroup identity

(1.1) $$x_0 \dots x_k = x_0 \dots x_{i-1} y x_i \dots x_k,$$

where x_ν and y are variables, k and i are integers such that $k \geq 0$, $0 \leq i \leq k+1$.

<u>1.1. The semigroup equality</u>

(1.2) $$x_0 \dots x_s = y_0 \dots y_r$$

<u>is a nontrivial identity in</u> $\mathcal{O}_{k,i}$ <u>iff</u> $s,r \geq k$, $x_0=y_0,\dots,x_{i-1}=y_{i-1}$, $x_{s-k+i} = y_{r-k+i},\dots,x_s = y_r$.

It follows an easy description of the free semigroup $\underline{F}_A = (F_A,\cdot)$ in $\mathcal{O}_{k,i}$ generated by the set A. Namely, F_A consists of all nonempty sequences of elements of the set A with lengths not greater than k+1, and with an operation defined by

$$a_0 \dots a_r \cdot a_{r+1} \dots a_s = \begin{cases} a_0 \dots a_s, & \text{if } s \leq k \\ a_0 \dots a_{i-1} a_{s-k+i} \dots a_s, & \text{if } s>k. \end{cases}$$

If $\mathcal{C}$ is a class of semigroups, then by $\mathcal{C}(n)$ we denote the class of n-semigroups which are n-subsemigroups of semigroups in $\mathcal{C}$. (See [1].) Here we show that the class of n-semigroups $\mathcal{O}_{k,i}(n)$ is a variety, which is finitely axiomatizable. We denote by $[\dots]$ the n-ary operation of the n-semigroups, and x's and y's are variables.

<u>1.2. The class of n+1-semigroups</u> $\mathcal{O}_{k,i}(n+1)$ <u>is a variety defined by the identity</u>

(1.3) $[x_0 \dots x_{i-1} y_1 \dots y_{np-k} x_i \dots x_k] = [x_0 \dots x_{i-1} z_1 \dots$
$\dots z_{nq-k} x_i \dots x_k]$

<u>where</u> p,q <u>are the least positive integers such that</u> $np-k \geq 0$, $nq-k > 0$.

<u>Proof</u>: As a consequence of <u>1.1</u> we have that (1.3) is satisfied in any n+1-subsemigroup of a semigroup in $\mathcal{O}_{k,i}$ and, furthermore,

(1.4) $$[x_0 \dots x_{sn}] = [y_0 \dots y_{rn}]$$

is a nontrivial identity in the variety of n-semigroups defined by (1.3) iff $x_0=y_0, \dots, x_{i-1}=y_{i-1}, x_{ns-k+i}=y_{nr-k+i}, \dots, x_{ns}=y_{nr}$.

Now, let $\underline{A} = (A,[\dots])$ be a given n+1-semigroup which satisfy the identity (1.3). We will construct a semigroup $\underline{A}^{\wedge} \in \mathcal{O}_{k,i}$ such that $\underline{A}$ will be an n+1-subsemigroup of $\underline{A}^{\wedge}$.

Let $\underline{F}_A$ be the free semigroup in $\mathcal{O}_{k,i}$ generated by the set A. Define a relation $\vdash$ in F_A by $u = ---a--- \vdash ---a_0 \dots a_{mn}--- = v$ $(u,v \in F_A)$, where $a = [a_0 \dots a_{mn}]$ in $\underline{A}$, and let $\vdash\dashv = \vdash \cup \vdash^{-1}$. Then, the transitive extension $\approx$ of $\vdash\dashv$ is a congruence on F_A (see [1]). It is enough to show that $\approx$ separates the elements of the set A, i.e. $a,b \in A \Rightarrow (a \approx b \Rightarrow a=b)$, because in that case we can take $\underline{A}^{\wedge} = \underline{F}_A/\approx$.

An element $u \in F_A$ is said to be irreducible (reducible) if its length is less than k+1 (bigger than k). Using (1.4) we define a partial mapping [ ] of F_A into A as follows: $[u] = a$ if $u = a_0 \dots a_{mn}$ in $\underline{F}_A$ and $[a_0 \dots a_{mn}] = a$ in $\underline{A}$. Note that all reducible elements of F_A are in the domain of [ ].

Let $u,v,w_\nu \in F_A$. It is easy to check this properties:

(i) $u \vdash v$, u is in the domain of $[\,] \Rightarrow [u] = [v]$.

(ii) $u \vdash\dashv w_1 \vdash\dashv w_2 \vdash\dashv \dots \vdash\dashv w_s \vdash\dashv v$, u and v are reducible, $w_1, \dots, w_s$ are irreducible $\Rightarrow [u] = [v]$.

We will prove only the last implication. Namely, as $w_1, \dots, w_s$ are irreducible, we have that $|w_1| \equiv \dots \equiv |w_s| \pmod n$, and so there exist $w \in F_A$ such that $2|w_i| + |w| \equiv 1 \pmod n$, i.e. $w_i w w_i$ is in the domain of [ ], for i=1,2,...,s. Thus we have:

$$u \vdash\dashv w_1 \vdash\dashv \dots \vdash\dashv w_s \vdash\dashv v \Rightarrow u = uwu \vdash\dashv w_1 wu \vdash\dashv w_1 w w_1 \vdash\dashv \dots \vdash\dashv w_s w w_s \vdash\dashv v w w_s \vdash\dashv vwv = v \Rightarrow [u] = [uwu] = [w_1 w w_1] = \dots = [w_s w w_s] = [vwv] = [v].$$

Now, let $a,b \in A$ and $a \doteq b$. Then there exist $u_1,\ldots,u_r \in F_A$ such that $a \vdash\!\dashv u_1 \vdash\!\dashv u_2 \ldots \vdash\!\dashv u_r \vdash\!\dashv b$, and (i) and (ii) implies that $a=b$.

2. VARIETY OF SEMIGROUPS $\mathcal{O}_{k,i,j}$. The variety of semigroups $\mathcal{O}_{k,i,j}$ is defined by the identity

$$x_0\ldots x_k = x_0\ldots x_{i-1}y_i\ldots y_{j-1}x_j\ldots x_k,$$

where $k \geq 0$, $0 \leq i < j \leq k+1$.

<u>2.1</u>. <u>The semigroup equality</u>

$$x_0\ldots x_s = y_0\ldots y_r$$

<u>is an identity in the variety</u> $\mathcal{O}_{k,i,j}$ <u>iff it is trivial or</u> $s \geq k$, $r \geq k$ <u>and</u> $x_0=y_0,\ldots,x_{i-1}=y_{i-1},x_{s-k+j}=y_{r-k+j},\ldots,x_s=y_r$.

As a consequence of <u>1.1</u> and <u>2.1</u> we obtain:

<u>2.2</u>. $i<j \Rightarrow \mathcal{O}_{k,i} \cap \mathcal{O}_{k,j} = \mathcal{O}_{k,i,j}$.

In the same manner as in <u>1.2</u> one can prove that $\mathcal{O}_{k,i,j}(n)$ is a variety, i.e. we have:

<u>2.3</u>. <u>The class of</u> n+1-<u>semigroups</u> $\mathcal{O}_{k,i,j}(n+1)$ <u>is a variety defined by the identity</u>

$$[x_0\ldots x_{i-1}y_i\ldots y_{pn-k+j-1}x_j\ldots x_k] = [x_0\ldots x_{i-1}z_i\ldots z_{qn-k+j-1}x_j\ldots x_k]$$

<u>where</u> p,q <u>are the least integers</u> $(p,q \geq 0)$ <u>such that</u> $pn-k+j-1 \geq 0$, $qn-k+j-1 > 0$.

3. REMARKS.

1) We note that the condition (α) of [1] is not satisfied in either of the varieties $\mathcal{O}_{k,i}$ and $\mathcal{O}_{k,i,j}$. In fact, the condition (α) can be made a little more complicated such that the above varieties are in its scope, but that will not give the best posible generalization.

2) One can investigate varieties of semigroups similar to $\mathcal{O}_{k,i}$ and $\mathcal{O}_{k,i,j}$. Namely, let p be a permutation of the set $\{0,1,2,\ldots,k\}$, x's and y's are variables, and consider the semigroup identities

(3.1) $\quad x_0\ldots x_k = x_{p(0)}\ldots x_{p(i-1)}yx_{p(i)}\ldots x_{p(k)},$

(3.2) $$x_0 \ldots x_k = x_{p(0)} \ldots x_{p(i_1-1)} y_{i_1} x_{p(i_1+1)} \ldots$$

$$\ldots x_{p(i_r-1)} y_{i_r} x_{p(i_r+1)} \ldots x_{p(k)} .$$

Then one can prove that either of the varieties of semigroups defined by (3.1) or (3.2) is equal to the variety $\mathcal{O}_{k,m,M}$ for some m and M. (We assume that $p(s) \neq s$ for some s in (3.1).) Namely, let q be the least integer such that $p(q) \neq q$, and t be the biggest integer with the property $p(t) \neq t$. Then we have $m=\min\{i,s\}$ and $M=\max\{i,t+1\}$ for (3.1), and $m=\min\{q,i_1\}$, $M=\max\{i_r+1,t+1\}$ for (3.2).

3) The results of this paper are generalizations of the results obtained in [2].

R E F E R E N C E S

1 G.Čupona, A set of semigroup n-varieties, this volume

2 С.Марковски, За една класа полугрупи, Мат. Билтен 2(XXVIII), 1978, 29-36

Smile Markovski
Matematički fakultet
p.f. 504
91000 Skopje
Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

ON THE EMBEDDING PROPERTY OF MODELS

Žarko Mijajlović

0. INTRODUCTION

In this paper we are interested in those classes of models which admit the embedding property (abbreviated by EP). However, in most cases we shall assume that the class is elementary. In the first part we state several properties which are equivalent to EP. In the second part we apply these results to consider the amalgamation property (abbr. AP) of models. We recall that the importance of this notion arises from the study of homogeneous-universal models.

Now we introduce some terminology. A first order language is denoted by L, the language of a theory T by L(T), and of a model $\underline{A}$ by L($\underline{A}$). If not stated otherwise, it is assumed that L(T) is countable. Universes of models $\underline{A}$, $\underline{B}$, $\underline{C}$, ... are denoted by A, B, C, ... respectively, and the cardinal number of A by A . The class of all models of a theory T is denoted by $\mathcal{M}(T)$. Concerning other basic notions and definitions, we shall use them as they are introduced, for example, in [1].

Robinson forcing (finite and infinite) will be one of the tools used here. We shall follow the notation introduced in [4]. Therefore, $\mathcal{P}(\mathcal{M})$ denotes the set of finite pieces (i.e. conditions) of a class of models $\mathcal{M}$. If $\underline{A}$ is a model then $\mathcal{P}(\underline{A})$ stands for $\mathcal{P}(\{\underline{A}\})$. If $\mathcal{P}$ is a set of conditions, and $p \in \mathcal{P}$, then C(p) denotes the set of all new constant symbols which appear in p, i.e. symbols in p which belong to C, C is the set of new constant symbols added to L, and used in the notion of forcing. We recall that T^f denotes the finite forcing companion, and T^F denotes the infinite forcing companion (cf. [3]).

A class of models $\mathcal{M}$ is said to have the embedding property iff for all $\underline{A},\underline{B} \in \mathcal{M}$ there is a model $\underline{C} \in \mathcal{M}$ in which $\underline{A},\underline{B}$ are embedded. If $\mathcal{M} = \mathcal{M}(T)$ and $\mathcal{M}$ has the embedding property, then, by definition, T has EP also.

1. THE EMBEDDING PROPERTY

In this part we state and prove several properties equivalent to EP. It should be observed that most results may be simplified if it is assumed that T is universal, i.e. if $T = T_\forall$ ($T_\forall$ denotes the set of all universal consequences of T). This assumption is made in [6a], for example. The theorem below is applied to an arbitrary theory in a countable language. Many of the listed equivalences are known as stated in the theorem, or in a similar form, but having all of them at one place and some new proofs as well, might be of interest.

THEOREM 1.1. Let T be a theory in a countable language. Then the following are equivalent:

1. T has EP.
2. $T_\forall$ has EP.
3. If φ, ψ are $\sum_1^0$ sentences of L, then the consistency of theories $T+\varphi$, $T+\psi$ implies the consistency of $T+\varphi+\psi$.
4. The class of all countable models of T has EP.
5. The class of all finitely generated submodels of T has EP.
6. T has EP for arbitrary set of models of T, i.e. for any family $\underline{A}_i$, $i \in I$, of models of T there is $\underline{C} \models T$ in which all $\underline{A}_i$'s are embedded.
7. For each cardinal number k, the theory T has a k-universal model. (If $\underline{A}$ is a such a model, then it may be assumed $|A| \leq 2^k$; for an arbitrary language L, $|A| \leq 2^{\max(k, \|L\|)}$).
8. For all conditions $p, q \in \mathcal{P}(\mathfrak{M})$ if $C(p) \cap C(q) = \emptyset$, then $p \cup q \in \mathcal{P}(\mathfrak{M})$.
9. T^f is a complete theory.
10. T^F is a complete theory.
11. There is a model $\underline{A}$ of T such that $\mathcal{P}(\mathfrak{M}) = \mathcal{P}(\underline{A})$.
12. There is a submodel $\underline{M}$ of T such that all models of T are embedded into an elementary extension of $\underline{M}$.

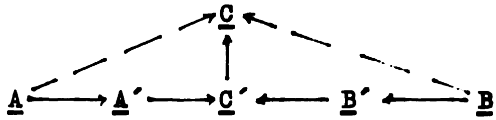
<u>Proof</u> In several cases we shall use (implicitly or explicitly) the following well-known theorem

(*) $\underline{A}$ is a model of $T_\forall$ iff $\underline{A}$ is a submodel of T.

With this theorem we can transfer arrow-diagrams between theories. In that manner we obtain the following consequence:

(**) If T and T′ are theories of a language L such that $T = T'$ then T has EP iff T′ has EP.

The proof of this fact can be seen on the displayed commutative diagram:



$\underline{A},\underline{B},\underline{C} \models T$

$\underline{A}',\underline{B}',\underline{C}' \models T$

arrows stand for embeddings.

Given $\underline{A},\underline{B} \models T$ and assuming that T′ has EP, models $\underline{A}',\underline{B}'$, $\underline{C}'$ and embeddings are obtained using (*) and EP of T′.

One important case of the application of (**) is when the theory T′ is complete, as in this case T′ has EP.

By the way, Claim (**) gives us a proof of ($1\leftrightarrow 2$). Now we proceed to the proof of the rest of Theorem.

($1\leftrightarrow 3$) Assume (3), and let $\underline{A},\underline{B}$ be models of T, and assume they cannot be embedded in a model of T. Then the theory $T+\Delta_A+\Delta_B$ is inconsistent, so there are finite pieces $p(\vec{c})\subseteq\Delta_A$, $q(\vec{d})\subseteq\Delta_B$, $\vec{c},\vec{d}\in C$, so that T+p+q is inconsistent. We may assume that $\{c_1,\dots,c_m\}\cap\{d_1,\dots,d_n\}=\emptyset$. Taking $\varphi(\vec{c})=\bigwedge p$, $\psi(\vec{d})=\bigwedge q$, we have $T\vdash(\varphi(\vec{c})\rightarrow\neg\psi(\vec{d}))$. As $\vec{c},\vec{d}$ do not belong to L, it follows $T\vdash\forall\vec{x}\,\forall\vec{y}\,\neg(\varphi(\vec{x})\wedge\psi(\vec{y}))$. Therefore, $T\vdash\neg(\exists\vec{x}\,\varphi(\vec{x})\wedge\exists\vec{y}\,\psi(y))$ and $\underline{A}\models\exists\vec{x}\,\varphi(\vec{x})$, $\underline{B}\models\exists\vec{y}\,\psi(\vec{y})$, contradicting our hypothesis.

($4\leftrightarrow 1$) This equivalence follows immediately by the equivalence ($1\leftrightarrow 3$) and downward Löwenheim-Skolem theorem.

($5\leftrightarrow 1$) Similarly to ($1\leftrightarrow 4$). Observe that if φ is a Σ_1^0 sentence which holds on $\underline{A}$, then φ holds on some finitely generated submodel of $\underline{A}$.

($1\rightarrow 6$) If T has EP, then obviously any finite set of models of T can be embedded into a model of T. So let $\underline{A}_i$, $i\in I$, be models of T, let T′ be the theory which consists of T and diagrams of models $\underline{A}_i$. As it was observed, T′ is finitely consistent, therefore, by compactness argument T′ has a model $\underline{C}$. In that model all $\underline{A}_i$'s are embedded.

($6\rightarrow 7$) One may choose a collection of all nonisomorphic models of T of the cardinality $\leq k$.

($7\rightarrow 1$) If $\underline{A},\underline{B}$ are models of T and $k=\max(|A|,|B|)$, then $\underline{A},\underline{B}$ can be embedded into a k-universal model of T.

(1 → 8) If $p,q \in \mathcal{P}(\mathfrak{M})$ then there are $\underline{A},\underline{B} \in \mathfrak{M}$ such that their simple expansions $\underline{A}',\underline{B}'$ satisfy p,q. By EP there is $\underline{C}$ so that $\underline{A},\underline{B}$ are embedded into $\underline{C}$. Thus, simple expansions of $\underline{C}$ satisfy $p \cup q$.

(8 → 4) Assume $\underline{A},\underline{B}$ are countable models of T, and let Δ_A, Δ_B be diagrams of $\underline{A},\underline{B}$ respectively, so that constant symbols in Δ_A are c_{2i}'s, and in Δ_B they are c_{2i+1}'s, $i \in \omega$. Further, let

$$X = \{p \cup q:\ p \subseteq \Delta_A, q \subseteq \Delta_B,\ |p \cup q| < \aleph_0\}.$$

Then the following set is generic

$$G = \{r \in \mathcal{P}(\mathfrak{M}):\ \text{for some } s \in X,\ r \leq s\}.$$

To prove that assertion, it suffices to check the following conditions

(i) $p \in G$ and $q \leq p$ implies $q \in G$.

(ii) If $p,q \in G$ then there exists $r \in G$ such that $p \leq r$ and $q \leq r$.

(iii) For each sentence φ in $L \cup C$ there exists $p \in G$ such that either $p \Vdash \varphi$ or $p \Vdash \neg\varphi$.

The first two claims trivially hold. To verify the third one, let φ be any sentence of $L \cup C$. There cannot exist conditions p,q such that $p \Vdash \varphi$ and $q \Vdash \neg\varphi$, as otherwise $p \cup q$ would force both φ and $\neg\varphi$. Therefore, $\emptyset \Vdash \neg\varphi$ or $\emptyset \Vdash \neg\neg\varphi$, and consequently there is $s \in \mathcal{P}$ such that $s \Vdash \varphi$ or $s \Vdash \neg\varphi$.

Let $\underline{M}$ be a generic model generated by G. Then $\underline{M}$ is a model of T^f, and as $T^f_\forall = T_\forall$ it follows $\underline{M} \models T_\forall$. Further, if $\theta \in \Delta_A$ then $p = \{\theta\}$ is a condition, p belongs to G and $p \Vdash \theta$. Hence, $\underline{M} \models \theta$ and therefore $\underline{M}$ is a model of Δ_A. Thus $\underline{A}$ is embedded in $\underline{M}$. In a similar way we can prove that $\underline{B}$ is embedded in $\underline{M}$. By (*) $\underline{M}$ is a submodel of T, thus $\underline{A}$ and $\underline{B}$ are embedded in a model of T.

(8 → 9) The theory T^f is the set of all sentences forced by $\emptyset$, so by the proof of (iii) in (8 → 4), we have $\emptyset \Vdash \neg\varphi$ or $\emptyset \Vdash \neg\neg\varphi$ for any sentence φ, hence $\neg\varphi \in T^f$ or $\neg\neg\varphi \in T^f$.

(9 → 1) If T^f is complete then T^f has EP. As $T_\forall = T^f_\forall$ the implication holds by (**).

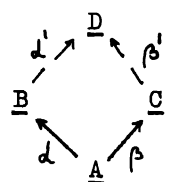
(10 → 1) Similarly to the proof of (8 ↔ 1).

(7 → 11) Let $\underline{A}$ be an $\aleph_0$-universal model. If $p \in \mathcal{P}(\mathfrak{M})$, then all sentences from p are true in some simple expansion of a countable model $\underline{B}$ of T. As $\underline{B}$ is embedded in $\underline{A}$, it follows that $\bigwedge p$ holds in a simple expansion of $\underline{A}$, i.e. $p \in \mathcal{P}(\underline{A})$, so $\mathcal{P}(\underline{A}) = \mathcal{P}(\mathfrak{M})$.

(11 → 8) If $C(p) \cap C(q) = \emptyset$ then obviously $p,q \in \mathcal{P}(\underline{A})$ implies $p \cup q \in \mathcal{P}(\underline{A})$.
(9 → 12) As T^f is complete, then for any model $\underline{A}$ of T^f we have $T^f = Th(\underline{A})$, hence $T_\forall = Th(\underline{A})$. Thus, for any model $\underline{B}$ of T there is a model $\underline{C}$ of $Th(\underline{A})$ in which $\underline{B}$ is embedded. As $\underline{C} \equiv \underline{A}$ there is $\underline{D}$ in which $\underline{A}$ and $\underline{C}$ are elementary embedded.
(12 → 1) If all models of T are embedded into a submodel $\underline{M}$ of T then $T = Th(\underline{M})$. The theory $Th(\underline{M})$ is complete, so it has EP. Therefore, the implication holds by (**).

2. THE AMALGAMATION PROPERTY

A class of models $\mathcal{M}$ is said to have the amalgamation property iff for all $\underline{A},\underline{B},\underline{C} \in \mathcal{M}$ and embeddeings $\alpha:\underline{A} \longrightarrow \underline{B}$, $\beta:\underline{A} \longrightarrow \underline{C}$ there is a model $\underline{D}$ and embeddings $\alpha':\underline{B} \longrightarrow \underline{D}$, $\beta':\underline{C} \longrightarrow \underline{D}$ such that the displayed diagram commutes.

(δ) 

If the class of all models of a theory T has AP, then it is said that T has AP.

Therefore, the amalgamation property of a class $\mathcal{M}$ is a localization of the embedding property at every model A of $\mathcal{M}$. This property has been studied in general cases (cf. [5a], [5c], [6b], [7], etc) as well as in some concrete cases (groups, semigroups, Boolean algebras, etc.). We shall make a few additional remarks. First, we observe the following fact which might be operative in proving that some classes have EP.

PROPOSITION 2.1. A theory T has AP iff for every model $\underline{A}$ of T and all Σ^0_1 sentences φ,ψ of $L \cup \{\underline{a}: a \in A\}$, the consistency of $T+\Delta_A+\varphi$, $T+\Delta_A+\psi$ implies the consistency of $T+\Delta_A+\varphi+\psi$.

This proposition is an immediate consequence of Theorem 1.1. As in case of EP some weaker assumption on elementary classes of models can be made in order to have AP.

PROPOSITION 2.2. A theory T has AP iff T has AP for countable models $\underline{A}'$ in diagram (δ).

Proof We shall use the criteria given by Proposition 2.1. So suppose $T+\Delta_A+\varphi$, $T+\Delta_A+\psi$ are consistent theories, where $A \models \Gamma$.

Assume that $T+\Delta_A+\varphi+\psi$ is inconsistent. Then there is $\Sigma\subseteq\Delta_A$ such that $T+\Sigma+\varphi+\psi$ is inconsistent. Let $\underline{A}'\prec\underline{A}$ be such that $\underline{A}'$ contains all a's which occur in Σ, and $|A'|\leq\aleph_0$. Then $T+\Delta_{A'}+\varphi+\psi$ is inconsistent, contradicting the fact that A' is countable, and that theories $T+\Delta_{A'}+\varphi$, $T+\Delta_{A'}+\psi$ are consistent.

<u>Example 2.3.</u> Amalgamation of Boolean algebras.

We show that the class of Boolean algebras has AP by use of the technique considered in the paper. The main tool will be the criteria given by Proposition 2.1. So let $\underline{A}$ be a Boolean algebra, and assume $T+\Delta_A+\varphi$, $T+\Delta_A+\psi$ are consistent theories, where T is the theory of Boolean algebras, and φ,ψ re Σ^0_1 sentences. Let $\Sigma\subseteq\Delta_A$ be a finite set and $\underline{B}\subseteq\underline{A}$ subalgebra generated by elements with names in $\Sigma\cup\{\varphi,\psi\}$. Further, let $\underline{D},\underline{C}$ be finite Boolean algebras so that $\underline{B}\subseteq\underline{C}$ and $\underline{B}\subseteq\underline{D}$, and

$$\underline{C}\models T+\Sigma+\varphi,\quad \underline{D}\models T+\Sigma+\psi.$$

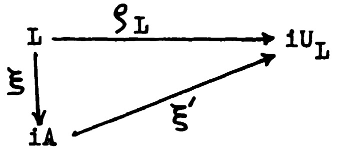
As $\underline{D},\underline{C}$ are finite Boolean algebras, there are embeddings $\alpha:\underline{C}\longrightarrow\Omega$, $\beta:\underline{D}\longrightarrow\Omega$, where Ω is a countable atomless Boolean algebra. If α', β' are restrictions of α,β respectively, then by the homogeneity of Ω(v.s. [5b]) there is $\lambda\in\mathrm{Aut}\,\Omega$ so that $\lambda\circ\alpha'=\alpha$. Thus, for some simple expansion Ω' of Ω we have $\Omega'\models T+\Sigma+\varphi+\psi$. Hence $T+\Delta_A+\varphi+\psi$ is finitely consistent.

In some cases it is possible to transfer the diagram $\underline{B}\xleftarrow{\alpha}\underline{A}\xrightarrow{\beta}\underline{C}$ into some other class of models, to complete there and to transfer back to the original class. This situation is described best in the language of categories. By an elementary category of models we mean a category $\mathcal{L}$ so that $\mathrm{Ob}(\mathcal{L})=\mathcal{M}(T)$ for some theory T, and morphisms of $\mathcal{L}$ are all embeddings bemodels of $\mathcal{M}(T)$. If T has AP then we shall say that $\mathcal{L}$ has AP also. The terminology we shall use is according to [2].

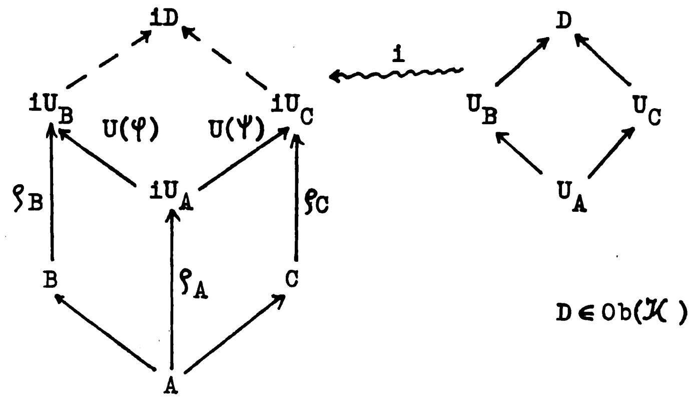
A uniform transfer of diagrams between categoties exists if some universal constructions are given. This is the content of the following assertion.

THEOREM 2.4. Let $\mathcal{K},\mathcal{L}$ be elementary categories of models. Assume that $\mathcal{K}$ is subordinate to $\mathcal{L}$, i.e. there is a faithful functor $i:\mathcal{K}\rightarrow\mathcal{L}$. Further, assume that there is a universal functor U under the representation F of the category $\mathcal{L}$ in $\mathcal{K}$ given by $F(\underline{L},\underline{A})=\mathrm{Hom}(L,iA)$, $F(\varphi,\alpha):\xi\longmapsto(i\alpha)\xi\varphi$, $L\in\mathrm{Ob}(\mathcal{L})$, $\underline{A}\in\mathrm{Ob}(\mathcal{K})$. Then we have: if $\mathcal{K}$ has AP then $\mathcal{L}$ has AP also.

<u>Proof</u> If $L \in \mathcal{L}$ let (U_L, ρ_L) be the corresponding universal pair. Then by definition of a universal pair, for each $\xi: L \longrightarrow iA$ there is $\xi': iU_L \longrightarrow iA$ so that the displayed diagram commutes.



Therefore, if $\underline{A}, \underline{B}, \underline{C} \in Ob(\mathcal{L})$ and $\varphi: \underline{A} \longrightarrow \underline{B}$, $\psi: \underline{A} \longrightarrow \underline{C}$, then by the universality of U we have the following commutative diagrams:



The right amalgam exists by the assumption that $\mathcal{K}$ has AP. Using functor i we can transfer that diagram into the category $\mathcal{L}$.

The previous theorem may be applied in many situations. The most important case is when the functor i is forgetful. It means that it associates to each $\underline{A} \in \mathcal{K}$ a reduct of that model.

<u>Example 2.5.</u> Let $\mathcal{K}$ be the elementary category of Boolean algebras and let $\mathcal{L}$ be the elementary category of distributive lattices with end-points. If $i: \mathcal{K} \longrightarrow \mathcal{L}$ is the forgetful functor, then the representation of $\mathcal{L}$ in $\mathcal{K}$ in the above Theorem has a universal functor U. For each distributive lattice L, the object U_L is the least Boolean algebra in which L is embedded. It is well known that such a Boolean algebra exists (it is easily constructed by the use of Stone representation theorem for distributive lattices). Therefore, the class of distributive lattices has AP.

REFERENCES

1. C.C.Chang, H.J.Keisler, Model Theory, North Holland, Amsterdam 1973.

2. P.M.Cohn, Universal Algebras, Reidel Publ. Co, Dordrecht 1981.

3. J.Hirschfeld, W.Wheeler, Forcing, Arithmetic, Division rings, Springer Verlag, Berlin 1975.

4. H.J.Keisler, Forcing and omitting types theorems, in: Studies in Model Theory, MAA, Buffalo, N.Y., pp. 96-133, 1973.

5. Ž.Mijajlović, a) Homogeneous-universal Models of Theories Which Have Model-Completions, in: Symp. Set Theory, Found. of Math., Beograd 29.08-2.09.1977, Rec. d. trav. Inst. Math. t.2(10), pp. 87-97, 1977. b) Saturated Boolean algebras with ultrafilters, Publ. Inst. Math. t.26(40), pp.175-197, 1979 c) Completion of Models and Galois Theory, Proc. Algebraic Conference, Novi Sad 1981, pp.19-26.

6. P.Krauss, a) Universally Complete Universal Theories, Zeit. f. Math. Logik und Grundlagen d. Math., Bd.17, pp.351-370, 1971. b) Homogeneous Models of Universal Theories, ibid. Bd. 23, pp. 415-426, 1977.

7. M.Yasuhara, The Amalgamation Property, The Universal-Homogeneous Models and Generic Models, Math. Scand. 34, pp.5-26, 1974.

Prirodno-matematički fakultet

Beograd

Studentski trg 16

Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

ON C^{n+1} -SYSTEMS AND $[n,m]$ -GROUPOIDS

Mirko Polonijo

0. Let Q be a nonvoid set, n and m positive integers and $f:Q^n \longrightarrow Q^m$. Then $Q(f)$ is an $[n,m]$ -groupoid. The component operations of f are n-ary operations $f_1,f_2,\dots,f_m:Q^n \longrightarrow Q$ defined by the equivalence

$$f(x_1,\dots,x_n) = (y_1,\dots,y_m) \Longleftrightarrow (\forall i \in \{1,\dots,m\})$$

$$y_i = f_i(x_1,\dots,x_n)$$

and we write $f = (f_1,f_2,\dots,f_m)$. $Q(f)$ will be called proper $[n,m]$ -groupoid if $n,m,|Q| \geqslant 2$ hold.

An $[n,m]$ -groupoid $Q(f)$ is said to be $[n,m]$ -quasigroup (multiquasigroup) ([2],[3]) iff it has the following property: for any n-tuple $(a_1,\dots,a_n) \in Q^n$ and any injection $\varphi:N_n \longrightarrow N_{n+m}$, $N_n = \{1,\dots,n\}$, there is a unique (n+m)-tuple $(b_1,\dots,b_{n+m}) \in Q^{n+m}$ such that $b_{\varphi(i)} = a_i$, for $i = 1,2,\dots,n$ and $f(b_1,\dots,b_n) = (b_{n+1},\dots,b_{n+m})$.

1. An $[n,m]$ -groupoid $Q(f)$ is said to be totally symmetric (briefly TS) iff for any permutation φ on N_{n+m} and for all $x_1,\dots,x_{n+m} \in Q$ the equality $f(x_1,\dots,x_n) = (x_{n+1},\dots,x_{n+m})$ implies $f(x_{\varphi(1)},\dots,x_{\varphi(n)}) = (x_{\varphi(n+1)},\dots,x_{\varphi(n+m)})$, (cf. [8]). Obviously, the components of a TS-$[n,m]$ -groupoid are TS. Moreover, it is easy to see that any TS-$[n,m]$-groupoid is a multiquasigroup. But if $Q(f)$ is a TS-$[n,m]$ -quasigroup, then $|Q| = 1$, which was proved in [8], Corollary 2.2. Therefore, we introduce the notion of weak total symmetry by the following definition:

An $[n,m]$ -groupoid $Q(f)$ is said to be weakly totally symmetric (briefly WTS) iff all its components are totally symmetric.

Now we shall list some obvious facts for WTS - $[n,m]$ -groupoids:

1.1. If $|Q| = 1$, then any $[n,m]$ -groupoid $Q(f)$ is a WTS - $[n,m]$-quasigroup.

1.2. An $[1,m]$ -groupoid $Q(f)$, $f = (f_1,\dots,f_m)$, is WTS iff all f_i , $i = 1,\dots,m$, are permutations and $f_i = f_i^{-1}$.

Hence, WTS -$[1,m]$ -groupoid is an $[1,m]$ -quasigroup.

1.3. Any WTS - $[n,1]$ -groupoid is an n-quasigroup.

2. For an $[n,m]$ -groupoid $Q(f)$, $f = (f_1,\dots,f_m)$, and an $n \times p$ array $X = (x_{ij})$ on Q we define an $m \times p$ array $C_f(X) = (y_{ij})$, by

$$y_{ij} = f_i(x_{1j}, x_{2j},\dots,x_{nj}) ,$$

$i = 1,\dots,m$, $j = 1,\dots,p$ (cf. [7]).

Analogously, for an $r \times n$ array $X = (x_{ij})$ on Q we define an $r \times m$ array $R_f(X) = (z_{ij})$ by

$$z_{ij} = f_j(x_{i1}, x_{i2},\dots,x_{in}) ,$$

$i = 1,\dots,r$, $j = 1,\dots, m$.

An $[n,m]$ -groupoid $Q(f)$ is said to be bisymmetric iff for any permutation γ on $N_n \times N_n$ and for all $n \times n$ arrays $X = (x_{ij})$ holds

$$C_f R_f(X) = C_f R_f(X^{\gamma}) ,$$

where $X^{\gamma} = (x_{ij})^{\gamma} = (x_{\gamma(i,j)})$.

Obviously, the components of a bisymmetric $[n,m]$-groupoid are bisymmetric. But, from the bisymmetry of the components, the bisymmetry of an $[n,m]$ -groupoid does not follow. Namely, we have the following example:

2.1. <u>Example</u>. Let be $Q = \{a_1, a_2, a_3, \dots\}$, $|Q| \geqslant 3$ and

$$f_1(x_1,\dots,x_n) = \begin{cases} a_1 & \text{for } x_1 = a_1,\ x_2 = x_3 = \dots = x_n = a_2 \\ a_3 & \text{otherwise} \end{cases}$$

$$f_2(x_1,\dots,x_n) = \begin{cases} a_1 & \text{for } x_1 = a_1,\ x_2 = x_3 = \dots = x_n = a_3 \\ a_2 & \text{otherwise .} \end{cases}$$

Since $C_{f_1}R_{f_1}(X) = a_3$, $C_{f_2}R_{f_2}(X) = a_2$, for all $n \times n$ arrays X , it follows that $Q(f_1)$ and $Q(f_2)$ are bisymmetric n-groupoids. For any m-2 bisymmetric n-groupoid operations $f_3,\dots,f_m$ on Q , $Q(f)$, $f = (f_1,f_2,\dots,f_m)$, is a non-bisymmetric $[n,m]$-groupoid with bisymmetric components. Namely,

$$C_{f_1}R_{f_2}(X) = f_1(a_1,a_2,\dots,a_2) = a_1 \quad ,$$

$$C_{f_1}R_{f_2}(X^T) = f_1(a_2, a_2,\dots, a_2) = a_3 \ ,$$

for $\quad X = (x_{ij}),\ x_{ij} = \begin{cases} a_3 & \text{for } i = 1 \ ;\ j = 2,\dots,n \\ a_1 & \text{otherwise .} \end{cases}$

At the same way, we have shown that there are such bisymmetric n-groupoids which are not commutative. But it does not hold for n-quasigroups.

2.2. PROPOSITION. <u>A bisymmetric multiquasigroup is commutative.</u>

<u>Proof</u>. Obviously, any $[1,m]$-groupoid is bisymmetric and commutative. Let $Q(f)$ be a bisymmetric $[n,m]$-quasigroup, $n \geqslant 2$. For $x_1,\dots,x_n \in Q$ and a permutation φ on N_n , put $X = (x_{uv})$, $Y = (y_{uv})$, where $x_{1v} = x_v$, $y_{1v} = x_{\varphi(v)}$, for $v = 1,\dots,n$, and $x_{uv} = y_{uv}$, for $u = 2,\dots,n$, $v = 1,\dots,n$. Since $C_fR_f(X) = C_fR_f(Y)$, it follows

$$f_i(f_j(x_{11},x_{12},\dots,x_{1n}),f_j(x_{21},x_{22},\dots,x_{2n}),\dots,f_j(x_{n1},x_{n2},\dots,x_{nn})) =$$
$$= f_i(f_j(y_{11},y_{12},\dots,y_{1n}),f_j(y_{21},y_{22},\dots,y_{2n}),\dots,f_j(y_{n1},y_{n2},\dots,y_{nn}))$$

i.e.

$$f_i(f_j(x_1,x_2,\dots,x_n),f_j(x_{21},x_{22},\dots,x_{2n}),\dots,f_j(x_{n1},x_{n2},\dots,x_{nn})) =$$
$$= f_i(f_j(x_{\varphi(1)},x_{\varphi(2)},\dots,x_{\varphi(n)}),f_j(x_{21},x_{22},\dots,x_{2n}),\dots,f_j(x_{n1},x_{n2},\dots,x_{nn}),$$

for $i,j = 1,\dots,m$. But $Q(f_i)$ is an n-quasigroup, which implies

$$f_j(x_1,x_2,\dots,x_n) = f_j(x_{\varphi(1)},x_{\varphi(2)},\dots,x_{\varphi(n)})$$

and therefore $Q(f)$ is commutative.

Since there is no proper commutative multiquasigroup, we have the following corollary:

2.3. COROLLARY. <u>For</u> $n,m, |Q| \geqslant 2$, <u>a bisymmetric</u> $[n,m]$ <u>-quasigroup does not exist</u>.

3. In [4] a notion of C^{n+1}-system was introduced, inspired by certain geometrical models. C^{n+1}-system is defined as a totally symmetric and bisymmetric n-groupoid (Cf.[5]). Therefore, if $Q(f)$ is a C^{n+1}-system, then there are an abelian group $Q(+)$ and $w \in Q$, such that $f(x_1,\dots,x_n) = - \sum_{i=1}^{n} x_i + w$, for all $x_1,\dots,x_n \in Q$ ([4],[5],[6]) .

Taking into account the previous definitions and results, weakly totally symmetric and bisymmetric (briefly WTSB) $[n,m]$ -groupoids are natural generalization of C^{n+1}-systems. For $|Q| = 1$, any $[n,m]$ -groupoid is WTSB, and for $n = 1$, any WTS -$[1,m]$ -groupoid is bisymmetric. For $n, |Q| \geqslant 2$ we have the following proposition

3.1. PROPOSITION. <u>An</u> $[n,m]$ <u>-groupoid</u> $Q(f)$, $n,|Q|\geqslant 2$, $f = (f_1,\dots,f_m)$, <u>is WTSB iff there are an abelian group</u> $Q(+)$ <u>and</u> $w_i \in Q$, $i = 1,\dots,m$, <u>such that</u>

$$f_i(x_1,\ldots,x_n) = -(x_1+\ldots+x_n) + w_i$$

<u>for all</u> $i = 1,\ldots,m$.

<u>Proof</u>. For $m = 1$ the statement is true ([4],[5],[6]). Therefore, let be $m \geq 2$.

Necessity. Since $Q(f_1)$, $Q(f_i)$, $i = 2,\ldots,m$, are TSB - n- groupoids, there are abelian groups $Q(+)$, $Q(\oplus)$ and $w,v \in Q$ such that

$$f_1(x_1,\ldots,x_n) = -(x_1+\ldots+x_n) + w$$

$$f_i(x_1,\ldots,x_n) = \ominus\ (x_1 \oplus \ldots \oplus x_n) \oplus v$$

for all $x_1,\ldots,x_n \in Q$. Let $e,f \in Q$ be the zeros of $Q(+)$, $Q(\oplus)$ respectively. For all $n \times n$ arrays $X = (x_{ij})$, $X^{\curlyvee} = (y_{ij})$ such that $x_{11} = y_{11} = -x$, $x_{22} = y_{12} = -y$, $x_{12} = x_{21} = y_{21} = y_{22} = w$, and $x_{ij} = y_{ij} = e$ otherwise, where $x, y \in Q$, we get

$$C_{f_i}R_{f_1}(X) = f_i(x,y,w,\ldots,w) = $$
$$= \ominus (x \oplus y \oplus w \oplus \ldots \oplus w) \oplus v \quad ,$$

$$C_{f_i}R_{f_1}(X^{\curlyvee}) = f_i(x+y+w,-w,w,\ldots,w) = $$
$$= \ominus ((x+y+w) \oplus (-w) \oplus w \oplus \ldots \oplus w) \oplus v \ .$$

Since $Q(f)$ is bisymmetric, it follows $C_{f_i}R_{f_1}(X) = C_{f_i}R_{f_1}(X^{\curlyvee})$ and therefore

$$x \oplus y = (x+y+w) \oplus (-w) \quad .$$

Hence $x = x \oplus f = (x+f+w) \oplus (-w)$, implying

$$(x+y+w) \oplus (-w) = ((x \oplus y) + f + w) \oplus (-w) \ ,$$

i.e.

$$x \oplus y = x+y-f \quad .$$

Thus we have

$$f_i(x_1,\ldots,x_n) = -(x_1+\ldots+x_n) + u \quad ,$$

where $u = n \cdot f + v$.

Sufficiency. Let $Q(+)$ be an abelian group, $w_i \in Q$, $i = 1,\dots,m$, and

$$f_i(x_1,\dots,x_n) = -(x_1+\dots+x_n) + w_i \quad ,$$

$i = 1,\dots,m$. Then $Q(f)$, $f = (f_1,\dots,f_m)$ is WTS and it is bisymmetric, because

$$C_{f_i} R_{f_j}(X) = \sum_{k,h=1}^{n} x_{kh} - n \cdot w_j + w_i \quad .$$

for any $n \times n$ array $X = (x_{kh})$ and all $i,j = 1,\dots,m$.

REFERENCES:

1. V.D.Belousov, n-arnye kvazigruppy, Štiinca, Kišinev, 1972.
2. G.Čupona, J.Ušan, Z.Stojaković, Multiquasigroups and some related structures, Prilozi MANU I 2 (1980), 5-12.
3. G.Čupona, Z.Stojaković, J.Ušan, On finite multiquasigroups, Publ. Inst. Math. Beograd, t.29(43), 1981, 53-59.
4. P.De Vito, F.Zirilli, Curve ellitiche normali e C^{n+1}-sistemi, Ricerche Mat. 27 (1978), 319-332.
5. M.Polonijo, Structure theorem for C^{n+1}-systems, Glasnik Mat. 17(37) (1981), 211-217.
6. M.Polonijo, Abelian totally symmetric n-quasigroups, Proc. Symp. on "n-ary structures", Skopje 1982, 185-193.
7. M.Polonijo, Medial multiquasigroups, MANU Contributions, to appear.
8. Z.Stojaković, Đ.Paunić, Identities on multiquasigroups, Proc. Symp. on "n-ary structures", Skopje 1982, 195-200.
9. K.Stojmenovski, Za [m,n] -kvazigrupite, God. Zb. Mat. fak. Skopje, 28 (1977), 33-37.

Prirodoslovno-matematički fakultet

p.p. 187

41001 Zagreb

Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

EMBEDDING OF A RING IN A RING WITH UNITY

Slaviša B. Prešić

1. As it is well known an arbitrary ring R without unity can be embedded in a ring S with unity. Namely, if we take S=RxZ and define addition and multiplication as follows

$$(1)\qquad \begin{aligned}(a,i) + (b,j) &= (a+b, i+j)\\ (a,i)\ (b,j) &= (ab+ib+ja, ij)\end{aligned}$$

we obtain such a ring S. However, this construction is not <u>reproductive</u>, for if the ring R already has a unity, e say, then the ring S is not isomorphic to R. In this paper we state one reproductive construction by which any ring can be embedded in a ring with unity.

2. Now let R be a given ring. Ring axioms can be expressed as follows

$$(2)\qquad \begin{aligned} x+y &= y+x \\ (x+y)+z &= x+(y+z) \qquad (x\cdot y)\cdot z = x\cdot(y\cdot z)\\ x+0 &= x\\ x+(-x) &= 0 \end{aligned}$$

$$x\cdot(y+z) = x\cdot y+x\cdot z,\quad (y+z)\cdot x = y\cdot x+z\cdot x$$

These axioms are in the language $L=\{+, \ , -, 0\}$. Supose now that there is at least one ordered pair (a,i), where $a\in R$, $i\in Z$ such that the equalities

$$(3)\qquad a\cdot x = ix,\quad x\cdot a = ix$$

hold for any $x\in R$. Such pairs (a,i) will be called <u>pre-characteristic</u>. Let P be the set of all pre-characteristic pairs. Obviously the implication

$$(a_1,i_1)\in P,\ (a_2,i_2)\in P \Rightarrow (k_1a_1+k_2a_2, k_1i_1+k_2i_2)\in P$$

$$(k_1,k_2\in Z)$$

is true. Consequently there are pairs $(a,\lambda)\in P$, $\lambda\geqslant 0$ whose number λ is the smallest one. Such pairs (a,λ) will be called <u>characteristic</u>.

Any two characteristic pairs (a_1, λ_1), (a_2, λ_2) must have the same numbers λ_1, λ_2. Besides that if (a, λ) is a characteristic pair and A is an annihilator[1] of the ring R then

- any characteristic pair is of the form $(a+n, \lambda)$ with $n \in A$
- any pre-characteristic pair is of the form $(ka+n, k\lambda)$ with $n \in A$, $k \in Z$

The notion of characteristic pairs includes that of unity, characteristic and zero elements of a ring. Namely, if a characteristic pair is one of the form

$$(0, \lambda), \quad (a,1), \quad (a,0)$$

then λ is the characteristic, a is a unity of R and a is an element of A, respectively.

For instance, let R be the ring determined by the tables

(4)

+	0	r
0	0	r
r	r	0

•	0	r
0	0	0
r	0	0

	−
0	0
r	r

This ring has two characteristic pairs

(5) $\qquad (r,2), \quad (0,2)$

The number 2 is the caracteristic of this ring.

3. Now we are going to state our construction. Let $e \notin R$ be a new element and let Term (R,e) denote the set of all terms built up by e, elements of R and symbols +, •, −, i.e. Term (R,e) is the smallest sot satisfying the following conditions

$$R \subset \text{Term}(R,e), \quad e \in \text{Term}(R,e)$$

$$x,y \in \text{Term}(R,e) \Longrightarrow (x+y),\ (x \cdot y),\ -x \in \text{Term}(R,e)$$

In connection with it let

(6) $\qquad (2)_{\text{Term}(R,e)}$

be the set of all formulas which one obtains from the axioms (2) by replacing the variables x,y,z by members of Term (R,e) in all possible ways.

Finally let $\mathcal{F}$ be the union of the set (6) and the set of all formulas of the following forms

(7)(i) $\quad a+b=\text{res}(a+b),\ a \cdot b=\text{res}(a \cdot b),\ -a=\text{res}(-a) \qquad (a,b \in R)$

(ii) $\quad a \neq b$ (a and b are different elements of R)

(iii) $\quad x \cdot e=x,\ e \cdot x=x \qquad (x \in \text{Term}(R,e))$

[1] i.e. the set of all $n \in R$ such that $(\forall x \in R)nx=xn=0$

The symbol <u>res</u> is a short form of the word <u>result</u>, so for instance res (a+b) represents that element $c \in R$ which is equal to a+b and similarly.

As a matter of fact, the set (i) $\cup$ (ii) is logically equivalent to the diagram of R. It is clear that any model M of $\mathcal{F}$, whose elements are some elements of Term (R,e), determines a certain ring S which has the unity e and contains the ring R as a subring. As a matter of fact such a model M is <u>generated</u> by R and e.

In order to simplity the condidtions $\mathcal{F}$ we first derive some logical consequences of $\mathcal{F}$. So, it is easy to conclude that each $t \in$ Term (R,e) is equal to one of the terms of the form[1)]

(8) $$a + ie \qquad (a \in R,\ i \in Z)$$

About these terms one can easily prove the following equalities

(9) $$\begin{aligned}(a+ie) + (b+je) &= res(a+b) + (res(i+j))e\\ (a+ie) \cdot (b+je) &= res(ab+ib+ja) + (res(i \cdot j))e\\ -(a+ie) &= res(-a) + (res(-i))e\end{aligned}$$

(10) $$a + 0e = a, \quad 0 + 1e = e$$

Deonote by $\mathcal{F}_1$ the union 7(i) $\cup$ 7(ii) $\cup$ (9) $\cup$ (10). This set of formulas, as we have remarked, is a logical censequence of the set $\mathcal{F}$, i.e. the implication $\mathcal{F} \Rightarrow \mathcal{F}_1$ is valid. It is important that the converse implication $\mathcal{F}_1 \Rightarrow \mathcal{F}$ is also true. Indeed, if t is any element of Term (R,e) then using (9) $\cup$ (10) one concludes that t is equal to some term of the form (8). Conseqently to prove ring axioms (2) and the formula $x \cdot e = x$ it suffices to prove this under assumption x,y,z are terms of the form (8). So, for instance, we have

$$\begin{aligned}x \cdot e = (a+ie) \cdot e &= (a+ie) \cdot (0+1e)\\ &= res(a \cdot 0 + i0 + 1a) + (res(i \cdot 1))e\\ &= a + ie = x\end{aligned},$$

and the formula $x \cdot e = x$ is proved. The ring axioms (6) can be proved similarly.

In such a way our problem is reduced to the problem of constructing models of the set $\mathcal{F}_1$ (more precizely said, of those <u>models which</u> are generated by R and e).

[1)] It is supposed by convention that the terms 0e, 1e, 2e,..., (-1)e, (-2)e,... stand for 0,e,(e+e),...,-e,-(e+e),..., respectively.

Such a model, in fact the ring S determined by (1) at the very beginning, can be described as follows. Let $\sim$ be the equivalence relation of the set $R \cup (R \times Z)$ whose classes either are singletons of the form $\{(x,i)\}$ where $x \in R$, $i \in Z$, $i \neq 0$, or are two - element sets of the form $\{x, (x,0)\}$ where $x \in R$. For sake of simplicity we shall denote classes shortly by (x,i), where $x \in R$, $i \in Z$. Accordingly to (9), (10), the operations +, $\cdot$, $-$, 0, e are defined by

$$(a,i) + (b,j) = (\text{res}(a+b), \text{res}(i+j))$$
$$(a,i) \cdot (b,j) = (\text{res}(a \cdot b + ib + ja), \text{res}(i \cdot j)$$
$$-(a,i) = (\text{res}(-a), \text{res}(-i))$$
$$0 = (0,0), \qquad e = (0,1)$$

We denote this model by $R \vartriangle Z$. In it any two different pairs (a_1,i_1), (a_2,i_2) are different elements of $R \vartriangle Z$. In other words this ring satisfies the following equivalence [1)]

$$a_1 + i_1 e = a_2 + i_1 e \Longleftrightarrow a_1 = a_2,\ i_1 = i_2$$

However, in any other model M of $\mathcal{F}_1$ some equalities of the form

(11) $\qquad a_1 + i_1 e = a_2 + i_2 e \quad \text{with} \quad (a_1,i_1) \neq (a_2,i_2)$

may hold. Consequently such a model M is a certain homomorphic image of $R \vartriangle Z$, i.e. M is, up to the isomorphism, of the form

$$R \vartriangle Z /\sim$$

where $\sim$ is some congruence relation of $R \vartriangle Z$ which <u>separates</u> the set R, i.e. satisfies the condition

(12) $\qquad x,y \in R,\ x \sim y \Longrightarrow x = y$

We describe now all such congruence relations. Let r be a binary relation of the set $R \vartriangle Z$ and denote by $\bar{r}$ the corresponding smallest congruence relation of the ring $R \vartriangle Z$, which contains the relation r and separates the set R, if such a relation $\bar{r}$ exists.

If $(a_1,i_1)\bar{r}(a_2,i_2)$ i.e. $(a_1+i_1e)\ \bar{r}\ (a_2+i_2e)$ then we have $\text{res}(a_1+(-a_2))\ \bar{r}\ (\text{res}(i_1+(-i_2))e$ which for some $a \in R$, $i \in Z, i \geq 0$ yields

$$a\ \bar{r}\ i\ e$$

1) Any element $(a,i) \in R \vartriangle Z$ can be expressed in the form a+ie.

Consider all such pairs (a,i) and denote by λ the smallest i. Because of (12) the corresponding element <u>a</u> must also be unique. Denote now by r′ the relation defined by the set $\{(a,0),(0,\lambda)\}$. It is easy to prove the equality

$$\bar{r}' = \bar{r}$$

i.e. r may be replaced by r′.

In such a way in the sequel we can confine our attention to the congruence relations $\bar{r}$ generating by the relations r of the form

$$\{(a,0),\ (0,\lambda)\}$$

with some fixed $a \in R$, $x \in Z$, $\lambda \geq 0$. The problem is when such a relation $\bar{r}$ separates the set R. If λ is 0 then obviously a must be 0 as well. About the other cases we have the following lemma.

LEMMA. <u>The congruence relation $\bar{r}$ generated by the relation of the form</u>

$$\{(a,0),\ (0,\lambda)\} \qquad (a \in R,\ \lambda \in Z)$$

<u>with</u> $\lambda > 0$ <u>separates the set</u> R <u>if and only if the pair</u> (a, λ) <u>is a pre-characteristic pair of the ring</u> R.

<u>Proof</u>. <u>Only if-part</u>. If $\bar{r}$ separates R then from $a\ \bar{r}\ \lambda e$ multiplying by $x \in R$ one obtains

$$ax\ \bar{r}\ \lambda x,\quad x \cdot a\ \ \bar{r}\ \lambda x$$

Hence by (12) if follows that

$$ax = \lambda x,\quad xa = \lambda x \qquad (x \in R)$$

i.e. (a, λ) is a pre-characteristic pair.

<u>If - part</u>. The relation $\bar{r}$ satisfyies the condition

$$a\ \bar{r}\ \lambda e$$

For that reason any $x_1 + i_1 e \in R \Delta Z$ is equivalent (i.e. is in the relation $\bar{r}$) to some element of the form

$$x + ie$$

where $x \in R$, $0 \leq i \leq \lambda - 1$. Additionally for such elements it can be easily proved the following equivalences

$$(13) \quad \begin{aligned} &[(x+ie)+(y+je)]\ \bar{r}\ [res(x+y+(q(i+j))a)+(r(i+j))e] \\ &[(x+ie)\cdot(y+je)]\ \bar{r}\ [res(xy+iy+jx+(q(i\cdot j))a)+(r(i\cdot j))e] \\ &-(x+ie)\ \bar{r}\ [res(-x+(q(-i))a)+(r(-i))e] \\ &x+0e\ \bar{r}\ x, \quad 0+1e\ \bar{r}\ e \end{aligned}$$

$$(x,y \in R, 0 \leq i,j \leq \lambda-1)$$

where $q(m)$, $r(m)$ with $m \in Z$ denote the quotient and the rest of dividing m by λ.

Accordingly to (13) we define an algebra $R \Delta L$, where $L := \{0, \ldots, \lambda - 1\}$, as follows. Similarly to the definition of $R \Delta Z$ the set $R \Delta L$ consists of elements of the form (x,i), where $x \in R$, $i \in L$ and additionally the equalities

$$(x,0) = x \qquad (x \in R)$$

are supposed. Operations $+$, $\cdot$, $-$, 0, e are defined by

$$(14) \quad \begin{aligned} (x,i)+(y,j) &= (res(x+y+(q(i+j))a),\ r(i+j)) \\ (x,i)\cdot(y,j) &= (res(xy+iy+jx+(q(i\cdot j))a,\ r(i\cdot j)) \\ -(x,i) &= (res(-x+(q(-i))a,\ r(-i)) \\ 0 = (0,0),\ e &= (0,1) \end{aligned} \qquad (x,y \in R, 0 \le i,j \le \lambda-1)$$

Essentially using the assumption

$$(\forall x \in R)(ax = \lambda x \ \wedge \ xa = \lambda x)$$

it is not difficult to prove that the algebra $R \Delta L$ is a ring with the unity (0,1) and that the ring R is its subring. Just on the ground of that fact it follows that the relation $\bar{r}$ separates the set R which completes the proof.

Finally we can describe our construction. Denote by $\mathcal{R}_e$ the class of all rings with a unity e which contains the ring R as a subring and which are generated by R and e. The ring $R \Delta Z$ is a member of that class. This ring is a maximal member of the class $\mathcal{R}_e$ in the sense that any other member of that class is some homorphich image of $R \Delta Z$. Besides $R \Delta Z$ any member of $\mathcal{R}_e$ is a ring of the form

$$R \Delta L$$

constructed on the proof of the lemma. Each such an element corresponds to some pre-characteristic pair (a, λ). The minimal elements of the class $\mathcal{R}_e$ are determined by the corresponding characteristic pairs.

For instance, the ring R given by (4) has two characteristic pairs (5) and therefore there are just two minimal elements of the corresponding class $\mathcal{R}_e$. One of them is the well-known ring Z_4.

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

A NOTE ON NORMED DIRECTED MULTIGRAPHS AND UNARY ALGEBRAS

A.Samardžiski, N.Celakoski

A class of normed directed multigraphs derived by unars or associated to K-unars is considered in this note with an aim to „translate" some notions and results on unary algebras from the paper [1] in terms of multigraphs.

Let A be a nonempty set and $\alpha \subseteq A \times \mathbb{N} \times A$, where $\mathbb{N}$ is the set of positive integers. The pair $\mathcal{G} = (A;\alpha)$ is called a *normed directed multigraph*. Any element of A is called a *vertex* and $(a,n,b) \in \alpha$ an *arc* of $\mathcal{G}$. The positive integer n is called the *norm*, the element a - the beginning and b - the end of the arc (a,n,b). Any sequence

$$(a,n_1,a_1),(a_1,n_2,a_2),\ldots,(a_{k-1},n_k,b) \in \alpha$$

is called a *path* of a to b, which we denote by $(a,n_1,\ldots,n_k,b)$, and the sum $n_1+\ldots+n_k$ is called the *length* of the path. A path with the length n will be denoted by Π_n or more precisely $a\Pi_n$ if it starts from a vertex a. (Note that a path is not determined uniquely by the symbols $(a,n_1,\ldots,n_k,b)$ or $a\Pi_n$.)

We are interested in special normed directed multigraphs which could be derived from the graph of a transformation, i.e. from a unar.

Let (B;f) be a unar (i.e. $f:x \mapsto f(x)$ is a transformation of B) and let K be a nonempty subset of $\mathbb{N}$. If A_o is a nonempty subset of B, and if

$$A_{i+1} = \{g^n(a)\,|\,a \in A_i, n \in K\}, \quad i=0,1,2,\ldots; \; A=\bigcup_{i\geq 0} A_i,$$

then we can construct a normed directed multigraph $(A;\alpha)$ in the following way

$$(a,n,b) \in \alpha \iff n \in K \quad \text{and} \quad b = f^n(a). \tag{1}$$

Then we say that $(A;\alpha)$ is a *K-subgraph* of the unar (B;f) generated by A_o.

It is easy to show that:

PROPOSITION 1. _If a normed directed multigraph_ $(A;\alpha)$ _is a K-subgraph of a unar, then the following propositions hold_:

M1. $\alpha \subseteq A\times K\times A$.

M2. $(\forall a\in A)(\forall n\in K)(\exists b\in A) \quad (a,n,b)\in\alpha$.

M3. _If two paths with the same length start from a vertex_ a, _then they terminate in the same vertex_ b.

M4. _Let_ $a\Pi_m$, $a\Pi_{m+p}$, $b\Pi_n$ _and_ $b\Pi_{n+p}$ _be paths in_ $(A;\alpha)$. _If_ $a\Pi_m$ _and_ $b\Pi_n$ _terminate in the same vertex_ c, _and_ $a\Pi_{m+p}$ _terminates in a vertex_ d, _then there is a path_ $b\Pi_{n+p}$ _with end_ d (Fig. 1). □

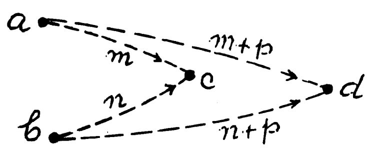


Fig. 1

PROPOSITION 2. _Each of the propositions_ Mi $(i=2,3)$ is independent of the others.

M1 _is independent of_ M2, M3, M4 _if and only if_ $K \neq \mathbb{N}$.

M4 _is independent of_ M1, M2, M3 _if and only if the least element_ k_0 _of_ K _is not a divisor of all the elements of_ K.

Proof. Below we give four examples of multigraphs $(A;\alpha_1)$, $(A;\alpha_2)$, $(A;\alpha_3)$, $(A;\alpha_4)$ such that $(A;\alpha_i)$ does not satisfy the proposition Mi, although it satisfies Mj for any $j \neq i$.

1) Clearly, if $K = \mathbb{N}$, then M1 is satisfied. Assume that $\emptyset \subset K \subset \mathbb{N}$. Let $(A;f)$ be a unar and define α_1 by

$$(a,n,b)\in\alpha_1 \iff f^n(a) = b \quad \& \quad n\in\mathbb{N}.$$

Then the multigraph $(A;\alpha_1)$ has the properties M2-M4 and does not have M1.

2) $A \neq \emptyset$, $K \neq \emptyset$, $\alpha_2 = \emptyset$.

3) $A \neq \emptyset$, $K \neq \emptyset$, $\alpha_3 = A\times K\times A$.

4) Let a normed directed multigraph $(A;\alpha)$ satisfy M1, M2 and M3, and let k_0, the least element of K, be a divisor of any element of K. If (a,n,c) is an arc and if $n=k_0 s$, then there exists a path $(a,\underbrace{k_0,\dots,k_0}_{s},c)$. Thus, any path $(a,n_1,\dots,n_p,c)$ can be replaced by a path $(a,\underbrace{k_0,\dots,k_0}_{s},c)$ with the same length as the given one. If $(a,\underbrace{k_0,\dots,k_0}_{s},c)$, $(b,\underbrace{k_0,\dots,k_0}_{t},c)$ and if $(a,\underbrace{k_0,\dots,k_0}_{s},\underbrace{k_0,\dots,k_0}_{r},d)$, $(b,\underbrace{k_0,\dots,k_0}_{t},\underbrace{k_0,\dots,k_0}_{r},d')$ are paths, then $(c,\underbrace{k_0,\dots,k_0}_{r},d)$, $(c,\underbrace{k_0,\dots,k_0}_{r},d')$ are also paths and this, by M3, implies that $d=d'$. Thus, M4 is satisfied.

Assume now that there is an element of K which is not divisible by k_0, and let $m\in K$ be the least such a number. Let $A=\{a,b,c\}$ and let $\alpha_4\subseteq A\times K\times A$ be defined in the following way:

$\alpha_4 = \{(x,n,a)\,|\,x\in\{a,b\},n\in K\}\cup\{(c,n,a)\,|\,n\in K\setminus\{m\}\}\cup\{(c,m,b)\}$.

It is easy to show that $(A;\alpha_4)$ satisfies M1,M2 and M3. Now, we will show that M4 does not hold. Let $m=qk_0+r$, $q>0$, $0<r<k_0$. Then:

$$(a,\underbrace{k_0,\dots,k_0}_{q},a),\quad (c,\underbrace{k_0,\dots,k_0}_{q},a),\quad (a,m,a),\quad (c,m,b)$$

are paths; moreover, (a,m,a), (b,m,a) and (c,m,b) are the unique paths with length m. □

A normed directed multigraph $(A;\alpha)$ is called a K-graph if $\emptyset\subset K\subseteq \mathbb{N}$ is such that M1,M2 and M3 hold.

The proposition M4 for a K-graph can be stated (because of M3) in the following way:

M4′. Let a path $a\Pi_m$ and a path $b\Pi_n$ terminate in the same vertex c. If a path $a\Pi_{m+p}$ terminates in a vertex d, then any path $b\Pi_{n+p}$ terminates in d.

The notion of a K-graph is closely connected with the notion of a K-unar ([1]) as we will see below.

Let A be a nonempty set and $\emptyset\subset K\subseteq\mathbb{N}$. If a mapping $(n,a)\mapsto na$ from $K\times A$ into A is defined such that

$$n_1,\dots,n_r,\ m_1,\dots,m_s \in K,\ n_1+\dots+n_r = m_1+\dots+m_s \Longrightarrow$$
$$(\forall x\in A)\ n_1(n_2(\dots(n_{r-1}(n_r x))\dots)) = m_1(m_2\dots(m_{s-1}(m_s x))\dots)), \qquad (2)$$

then we say that a structure of K-unar is built on A, i.e. that (A;K) is a K-*unar*. (This notion is defined in [1], where it is written $a^{[n]}$ instead of na.)

PROPOSITION 3. *If* $(A;\alpha)$ *is a* K-*graph and if a mapping* $(n,a)\mapsto na$ *is defined by*

$$b = na \iff (a,n,b)\in\alpha, \qquad (3)$$

then we obtain a K-*unar* (A;K).

Conversely, if a K-*unar* (A;K) *is given, and if* α *is defined by* (3), *then* $(A;\alpha)$ *is a* K-*graph*. □

All the propositions which will be stated below are „translations" of corresponding propositions for K-unars.

PROPOSITION 4. *Every* K-*graph is a* K-*subgraph of a unar iff the least element of* K *is a divisor of any element of* K. ([1;2.5, p.78]). □

A K-graph $(A;\alpha)$ is said to be *injective* if the following condition is satisfied: if two paths with the same length start from distinct vertices, then they terminate to distinct vertices; $(A;\alpha)$ is said to be *surjective* if every vertex is an end of an arc. A K-graph which is both injective and surjective is said to be *bijective*.

PROPOSITION 5. *Every injective* K-*graph is a* K-*subgraph of a unar*. ([1;3.2, p.80]). □

PROPOSITION 6. *A surjective* K-*graph is a* K-*subgraph of a unar if and only if* M4 *is satisfied*. ([1;3.6, p.82]). □

Examples

1. Let $B = \{a_1,a_2,a_3,a_4,a_5,a_6,a_7,a_8\}$ and

$$f = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 \\ a_3 & a_3 & a_5 & a_5 & a_6 & a_7 & a_8 & a_5 \end{pmatrix}.$$

If $K=\{2,3\}$ and $A_0=\{a_1,a_2\}$, then the K-subgraph $(A;\alpha)$ of the unar (B;f) generated by A_0 is given by Fig. 2.

The K-graph given on Fig. 3 is not a K-subgraph of a unar $(B;f)$, for if it were, then we would have

$$b = f^3(c) = f(f^2(c) = f(f^2(a)) = f^3(a) = a.$$

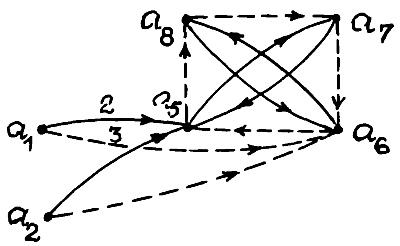


Fig. 2

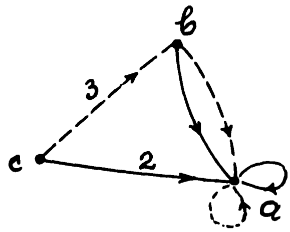


Fig. 3

2. Let $A=\{a_1,a_2,\dots,a_{10}\}$ and $K=\{3,4\}$. The K-graph given on Fig. 4 is not a K-subgraph of a unar (although it satisfies M4).

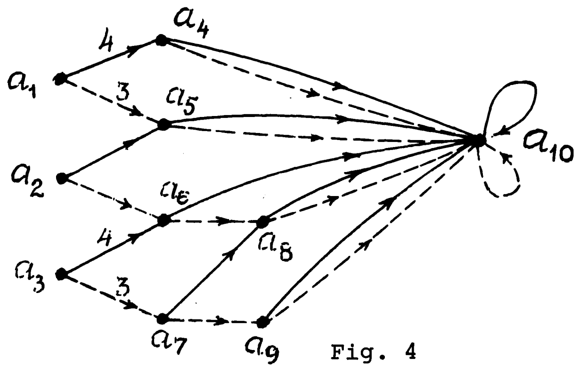


Fig. 4

For, if this K-graph were a K-subgraph of a unar $(B;f)$, then we would have:

$$a_4 = f^4(a_1) = f(f^3(a_1) = f(f^4(a_2)) =$$
$$= f^2(f^3(a_2)) = f^2(f^4(a_3)) = f^6(a_3) =$$
$$= a_9.$$

3. Let $K=\{3,4\}$. Choosing the symbols $a_0,a_1,\dots,a_n,\dots;$ $b_0,b_1,\dots,b_n,\dots$ and putting

$$(a_{n+1},3,a_n),\quad (b_{n+1},3,b_n)\in\alpha,\quad n=0,1,2,\dots$$

$$(a_0,3,z),\quad (b_0,3,z)\in\alpha,$$

a K-graph $\mathcal{G}$ can be generated, part of which is given on Fig. 5. $\mathcal{G}$ is surjective, but it does not satisfy M4, since

$(a_0,3,z)$, $(b_0,3,z)$, $(a_0,4,u)$, $(b_0,4,v)$ α and $u \neq v$. Thus, by Proposition 6, $\mathcal{G}''$ is not a K-subgraph of a unar.

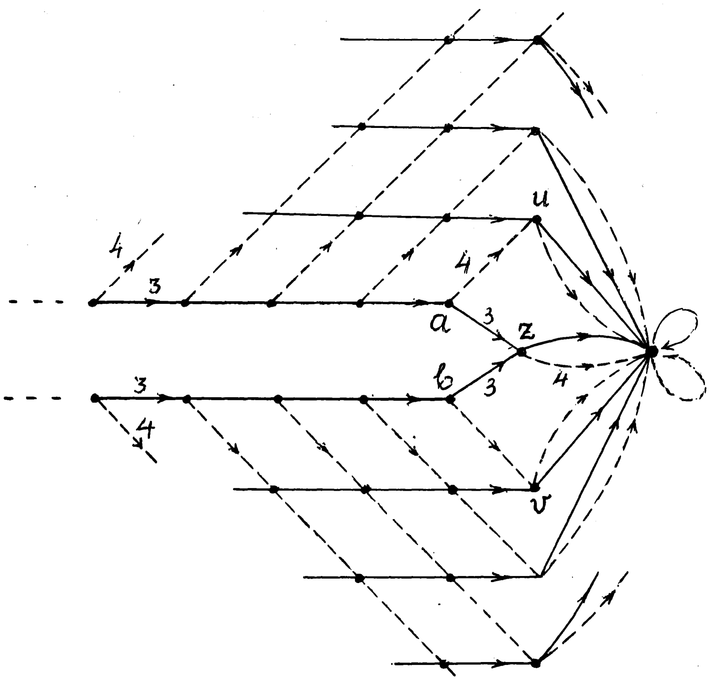


Fig. 5

Remarks

1. For any nonempty subset K of $\mathbb{N}$ there exists a unique finite nonempty subset K_0 of K with the following properties:

(i) Each element $n \in K$ is a sum of elements of K_0, $n=n_1+\ldots+n_r$.

(ii) If $k \in K_0$, then k is not a sum of the elements of $K_0 \setminus \{k\}$.

We say that K_0 is the base of K ([2]).

If $(A;\alpha)$ is a K-graph, and if α_0 is defined by: $\alpha_0=\alpha \cap A\times K_0\times A$, then we obtain a K_0-graph $(A;\alpha_0)$ which is called the best refinement of $(A;\alpha)$. It is easy to see that $(A;\alpha)$ is a K-subgraph of a unar $(B;f)$ iff $(A;\alpha_0)$ is a K_0-subgraph of $(B;f)$.

2. The K-graph on Fig. 4 is not a K-subgraph of a unar, although it satisfies M4. This suggests the problem of finding the family Φ of subsets of $\mathbb{N}$ sush that

$K \in \Phi \Leftrightarrow$ every K-graph which satisfies M4 is a K-subgraph of a unar.

3. It is conceivalble to look for necessary and sufficient conditions a K-graph $(A;\alpha)$ to be a K-subgraph of a unar $(A;f)$. We note that this problem is not solved even in the case when K is a one-element set, $K=\{n\}$. Namely, a convenient solution is given in [3] in the case $n=2$ when A is finite, and if $(A;\alpha)$ is an $\{n\}$-graph of a permutation, a solution is given in [4] for any $n \in \mathbb{N}$ and any A.

REFERENCES

[1] G.Čupona, N.Celakoski, A.Samardžiski, Post theorems for unary algebras, Proc. Symp. n-ary Structures, Skopje 1982, 71-84

[2] D.Dimovski, Additive semigroups of integers, (in Macedonian), MANU, Contributions IX-2 (1977), 21-26

[3] M.Snowden, J.M.Howie, Square roots in finite full transformation semigroups, Glasgow Math. J. 23 (1982), 137-149

[4] G.Čupona, A.Samardžiski, N.Celakoski, Roots of permutations, Proc. Symp. n-ary Structures, Skopje 1982, 85-95

Matematički fakultet, p.f. 504
91000 Skopje, Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

SEMISIMPLE RINGS

Srboljub Srećković

In this paper the Artinian semisimple rings (or the classical semisimple rings) have been considered. These rings have a series of interesting and marked characteristics. They may be represented as finite direct sums of minimal left ideals. However, it is certainly the most important property that they may be represented by finite direct sums of Artinian simple rings. From this property and the Wederburn - Artin theorem follows that the Artinian semisimple rings are isomorphic to finite direct sums of complete matrix rings over some skewfields.

In consideration of the fact that the properties of rings influence the properties of modules over these rings and vice-versa for the characterization of Artinian semisimple rings a reciprocal connection between the properties of the rings and the properties of the modules over these rings is used. By this characterization an equivalence of some properties of rings and some properties of modules over these rings has been established. Both the projective and the injective modules play an important role in the previously mentioned characterization. Such a ring characterization, as well as some more important notions in connection with it, present the subject matter of this paper.

Some more important characteristics of the projective and injective modules have been proved in [4, Ch.I, Section 2 and 3]. It is certainly the most remarkable property of injective module. This property has been proved in [4, Ch.I, Theorem 3.3]. A simpler proof of this property is given in [1]. In that proof a definition of the full module is used as well as the property of the Z-module stated by Lemma 1 of this paper.

Definition 1. The left module A over the ring R will be called full if $rA=A$ for all nonzero $r\in R$.

LEMMA 1. Each Z-module is injective if and only if it is full.

In [4, Ch.VII, Section 1] the above mentioned lemma has been generalized on the integral domain, and in this paper a generalization to the noncommutative rings was made by the following theorem.

THEOREM 2. Each R-module over the ring R of the principal left ideals without zero divisors is injective if and only if it is full.

Proof. Let Q be the injective R-module. Since $r'r_1=r''r_1$, if and only if $r'=r''$ for each $r_1\neq 0$, the map $f:Rr_1\to Rx$ defined by the equality $f(rr_1)=rx$ for any $r\in R$ and $x\in Q$ is R - homomorphism and may be extended to the homomorphism $g:R\to Q$. Then $x=f(r_1)=g(r_1)=r_1g(1)$. Therefore $r_1Q=Q$ for all $r_1\neq 0$, that is Q is the full module.

Reversely, let Q be the full R-module,and Rr_1 arbitrary left ideal of the ring R and $f:Rr_1\to Q$ arbitrary R-homomorphism. Then $f(rr_1)=rf(r_1)$. Since Q is the full module, there exists $g\in Q$ so that $f(r_1)=r_1g$ from which $f(rr_1)=(rr_1)g$ is obtained. Consequently, R-module Q is injective.

If R-module M is submodule of R-module N, the module N will be called the extension of module M. The module M, as so-called trivial extension, belongs to the set of all extensions of module M. Each module M can be embedded into an injective module N. Then we say that the module N is an injective extension of module M. The module N is the minimal injective extension of module M if it is not a nontrivial injective extension of no one injective extension of module M.

The extension N of module M will be called the essential extension if each nonzero submodule of module N has a nonzero intersection with M. Then we say that M is the essential submodule of the module N. The notation $N\overset{\prime}{\supset}M$ signifies that the module N is the essential extension of the module M. The module M, as so-called trivial essential extension of the module M, belongs to the set of all essential extensions of the module M as well. If the module M_1 is an extension of module M, and M_2 an extension of M_1, then, evidently, M_2 is the essential extension of the module M, if and only if M_2 is the essential extension of module M_1 and M_1 the essential extension of module M.

The essential extension N of module M will be called maximal if N has no nontrivial essential extensions. The set of all essential extensions of the module M has been partially ordered by inclusion. The union V of the ascending chain $M \subset M_1 \subset \ldots$ of the essential extensions of the module M is the essential extension because from $H \subset V$ and $H \cap M = 0$ it follows $(H \cap M_1) \cap M = 0$, that is, $H \cap M_1 = 0$ and $H = 0$. In this way, in the set of all essential extensions of the module M there exist the maximal essential extensions.

If N is an injective extension and N_1 an essential extension of the module M, then the monomorphism $j: M \to N$ may be extended to the homomorphism $\bar{j}: N_1 \to N$. Since N_1 is the essential extension of the module M and $M \cap \mathrm{Ker}(\bar{j}) = 0$, then $\mathrm{Ker}(\bar{j}) = 0$, that is, the module N_1 is embedded into the module N by $\bar{j}$. Consequently, any essential extension of the module M can be embedded into each injective extension of the module M. When the module is injective, then it has no nontrivial essential extensions.

In [1] the following theorem has been proved.

THEOREM 3. <u>The following three statements are equivalent for any module</u> M:

(a) M <u>is an injective module</u>,

(b) M <u>has no nontrivial essential extensions</u>,

(c) M <u>is the direct summand of each extension</u>.

The maximal essential extension $\bar{M}$ of the module M has no nontrivial essential extension and therefore it is the injective module. Since $\bar{M}$ is contained in each injective extension of the module M, then $\bar{M}$ is the minimal injective extension of the module M. Consequently, the minimal injective extension of the module M is unique to the isomorphism.

Let M be the left module over the ring R. Let us mark with $x^R = \{r \in R : rx = 0\}$ the order of element $x \in M$. Evidently, x^R is the left ideal of the ring R. Using the left ideals x^R for $x \in M$ we define the submodule $Z(M)$ of the module M by equality $Z(M) = \{x \in M : R \,'\!\supset x^R\}$. And so $Z(M)$, evidently, is the Abelian group. According to the following proposition one can conclude that the implication $x\in Z(M)\Rightarrow rx\in Z(M)$ is valid for each $r\in R$ and $x\in Z(M)$, that is, that $Z(M)$ is the submodule of the module M.

PROPOSITION 4. <u>If</u> $R\,'\!\supset x^R$, <u>then</u> $R\,'\!\supset (rx)^R$ <u>for each</u> $r\in R$.

<u>Proof</u>. It is sufficiently to prove $x^R\,'\!\supset (rx)^R$. Let I_1 be the arbitrary ideal which is contained in x^R. Then the ideal $I_1 r$ has a nonzero intersection with the ideal x^R. Therefore $I_1\cap (rx)^R\neq 0$. Consequently, $x^R\,'\!\supset (rx)^R$ and $R\,'\!\supset (rx)^R$ for each $r\in R$ because $R\,'\!\supset x^R$.

Evidently, Z(R) is an ideal of the ring R because it is the left ideal and $(xr)^R\supset x^R$ for each $x,r\in R$.

The maximal essential extension of the submodule of a module is not unique. However, in [3, Lemma 2] it has been proved that all the submodules of the module M with the property $Z(M)=0$ have their unique maximal essential extensions.

<u>Definition</u> 2. The ring R can be called regular if there exists $x\in R$ for each $r\in R$, so that $rxr=r$.

PROPOSITION 5. <u>If</u> R <u>is the regular ring, then</u> $Z(R)=0$.

<u>Proof</u>. If $e^2=e\in R$ and $x\in e^R\cap Re$, then $x=xe=0$. Therefore $e^R\cap Re=0$ and Z(R) does not contain nonzero idempotents.

If the ring R is regular, then for each $r\in R$ there exists $x\in R$, so that $rxr=r$. Then xr is nonzero idempotent because $(xr)(xr)=x(rxr)=xr$. Therefore each nonzero left ideal of the ring R contains an nonzero idempotent. Since Z(R) does not contain nonzero idempotents then $Z(R)=0$.

The classical semisimple rings have been characterized by the following theorem.

THEOREM 6. <u>For any ring</u> R <u>the following statements are equivalent</u>:

(a) R <u>is classical semisimple ring</u>,

(b) R <u>is semisimple as the left</u> R-<u>module</u>,

(c) <u>every left ideal of the ring</u> R <u>is the direct summand</u>,

(d) <u>every left ideal of the ring</u> R <u>is injective as the left</u> R-<u>module</u>,

(e) <u>all left</u> R-<u>modules are semisimple</u>,

(f) <u>all the exact sequences</u> $0\to A'\to A\to A''\to 0$ <u>of the left</u> R-<u>modules are direct</u>,

(g) <u>every left</u> R-<u>module is projective</u>,

(h) <u>every left</u> R-<u>module is injective</u>,

(i) *every finitely generated left* R-*module is injective*,

(j) *every cyclic left* R-*module is injective*,

(k) *every submodule of the arbitrary left* R-*module is its direct summand*,

(l) *the order of each nonzero element of the arbitrary* R-*module is the intersection of the finite number of the maximal left ideals of the ring* R,

(m) *the left annihilator of each nonzero element of the ring* R *is the intersection of the finite number of the maximal left ideals of the ring* R,

(n) *every maximal independent system of elements of the arbitrary left module is the basis of this module*,

(o) *every maximal independent system of elements of the ring* R *is the basis of* R,

(p) *every finitely generated left* R-*module is projective*,

(q) *every cyclic left* R-*module is projective*.

Proof. (a) $\Rightarrow$ (c). Every left ideal of the classical semisimple ring is generated by an idempotent and therefore it is the direct summand of the ring R.

(b) $\Leftrightarrow$ (c) and (e) $\Leftrightarrow$ (k). Proved in [4, Ch.I, Proposition 4.1].

(f) $\Leftrightarrow$ (k). Trivial.

(f) $\Leftrightarrow$ (h). Proved in [4, Ch.I, Proposition 3.4].

(h) $\Rightarrow$ (d). Trivial.

(d) $\Rightarrow$ (c). If the left ideal I of the ring R is injective, then the sequence $0 \to I \to R \to R/I \to 0$ is exact and direct. Therefore the ideal I is the summand of the ring R.

(c) $\Rightarrow$ (h). If every left ideal I is the direct summand of the R-module R, then it is for every homomorphism $f: I \to A$, for the arbitrary R-module A, and every $r \in I$

$$f(r)=f(re)=rf(e),$$

where e is idempotent by which the ideal I was generated. According to [4, Ch.I, Theorem 3.2] the module A is injective.

(h) $\Rightarrow$ (i) $\Rightarrow$ (j) and (g) $\Rightarrow$ (p) $\Rightarrow$ (q). Trivial.

(q) $\Rightarrow$ (n). Let $\{a_i\}$ be the maximal independent system of the elements of the R-module M. The system of elements $\{a_i\}$ generates a submodule N of the module M. For each $x \in M$

the sequence $0 \to (x+N)^R \to R \to R(x+N) \to 0$ is exact and direct because the cyclic submodule $R(x+N)$ of the module M/N is projective. Therefore the left ideal $(x+N)^R$ is the direct summand of the ring R and was generated by an idempotent e and also $ex \in N$. If $r \notin (x+N)^R$, then $r(x-ex) \notin N$ because $rx \notin N$ and $r(ex) \in N$. Therefore $R(x-ex) \cap N=0$ and the element x-ex is independent of the system $\{a_i\}$. Since $\{a_i\}$ is the maximal independent system of elements, then $(x+N)^R=R$. Then $r(x-ex)=$ $=rx-(re)x=rx-rx=0$, that is $x=ex \in N$. Consequently, the module M has been generated by the system of elements $\{a_i\}$.

(j)$\Rightarrow$(a). If (j) is valid, then the ring R is selfinjective because it is generated by the unity 1. For the arbitrary $a \in R$ the left ideal Ra is injective. The ideal Ra is the direct summand of the ring R and is generated by some idempotent e, that is Ra=Re. Therefore $e=r_1a$ and also $a=r_2e$ for some elements $r_1, r_2 \in R$. Then $a=r_2e=(r_2e)e=ae=ar_1a$. Consequently, the ring R is regular and selfinjective. Every left ideal of the ring R contains a nonzero idempotent. If $e \in J(R)$ is an idempotent, then $R(1-e)=R$ because J(R) is quasi-regular ideal of the ring R. Since $Re \cap R(1-e)=0$, then e=0. Therefore J(R)=0 and the ring R is semisimple. According to [3, Lemma 5] the ring R does not contain an infinite set of orthogonal idempotents. Let $I_1 \supset I_2 \supset \ldots$ be a descending chain of left ideals. Every of ideals is finitely generated because it does not contain an infinite set of orthogonal idempotents. Therefore the ideals of the chain are injective and the equalities $I_1=I_1'+I_2=I_1'+I_2'+I_3=\ldots$ are valid. Since I_1 can be represented in the form of finite direct sum, then the descending chain of left ideals must be finite. Therefore, R is the classical semisimple ring.

(l)$\Rightarrow$(m). Trivial.

(m)$\Rightarrow$(a). If (m) is valid, then R contains the maximal ideal J which is not the essential submodule of the ring R because R has the unity. The ideal J has no nontrivial essential extensions and therefore it is injective. The ring R can be presented in the form of direct sum R=J+I. The ideal I is simple submodule because J is maximal one. Every ideal different from I, which contains I, has a nonzero intersection with J. Therefore I has no nontrivial essential extensions. The ring R is selfinjective because it is presented in the form of the direct sum R=J+I of the injective left ideals. Since J(R) is contained in every maximal left ideal of the ring R, the ring R has the unity as well, then the ring R is semisimple.

If $x \in Z(R)$ and if $x \neq 0$, then $(1+x)^R = 0$ because $x^R \cap (1+x)^R = 0$. Therefore $R(1+x) \approx R$ is the direct summand in R because R(1+x) is an injective module. Evidently, x^R is contained in R(1+x) because if $r \in x^R$, then $r = r(1+x)$. Therefore R(1+x)=R, that is, x is a quasi-regular element in R. From this we can conclude that Z(R) is a quasi-regular ideal in R and therefore Z(R)=0.

Let $x \neq 0$ and $x \in R$. Then x^R is not the essential submodule in R because Z(R)=0. Therefore the maximal submodule $I \neq 0$ of the module R exists which has a zero intersection with x^R. Then $x^R + I$ is the essential submodule of the module R. R-homomorphism $f: I \to R$ defined with $f(r) = rx$ is the monomorphism. Let $f^{-1}: f(I) \to I$ be inverse to the isomorphism f. Then $f^{-1}(rx) = r$ and according to [4, Ch.I, Theorem 3.2] in R exists the element r_1 such a one that $f^{-1}(rx) = rxr_1$. Then $rxr_1 = r$ and $rxr_1x = rx$ or $r(xr_1x - x) = 0$. The last equality is satisfied for all $r \in x^R + I$. Therefore $(xr_1x - x)^R$ is the essential submodule in R and therefore $xr_1x - x = 0$. Consequently, R is a regular ring.

The proof that the ring R is classical semisimple is derived in the same way as in the proof of the implication (j) ⟹ (a).

(b) ⟹ (l). Let the module M be the direct sum of simple modules $\{A_n\}$. Then every element can be presented in the form of the sum $x = a_{n_1} + \dots + a_{n_k}$ $(0 \neq a_{n_i} \in A_{n_i})$. Since $A_{n_i} \approx R/a_{n_i}^R$, then $a_{n_i}^R$ are maximal ideals. In that case $x^R = a_{n_1}^R \cap \dots \cap a_{n_k}^R$. Consequently, x^R is an intersection of the finite number of the maximal left ideals of the ring R.

(c) ⟹ (n). For every submodule N of the module M and for every $x \in M$ the sequence $0 \to (x+N)^R \to R \to R(x+N) \to 0$ is exact and direct because the left ideal $(x+N)^R$ is the direct summand of the ring R. In all the other cases the proof of this implication is identical to the proof of the implication (q) ⟹ (n).

(n) ⟹ (o). Trivial.

(c) $\Rightarrow$ (c). Let I be the arbitrary left ideal of the ring R and $\{a_i\}$ the maximal independent system in I. Let us complete this system with the elements $\{b_j\}$ in such a way to get a maximal independent system S in R. Then S is the basis of the ring R and $R=\sum Ra_i+\sum Rb_j$. Let x be an arbitrary element in I. The element x is a linear combination of elements from S in which combination the elements from $\{b_j\}$ can not participate because in this case the sum whose summands are of the form $r_k b_k$ of this linear combination would belong to the ideal I and the system $\{a_i\}$ would not be maximal. Therefore I is the direct summand of the ring R.

REFERENCES

1. B. Eckmann and A. Schöpf, Über injektive Moduln, Archiv der Mathematik 4(1953), 75-78.
2. A. Kertész, Modules and semisimple rings, Publ. Math. 3(1954), 289-296.
3. B. L. Osofsky, Rings all of whose finitely generated modules are injective, Pacific J. Math. 14(1964), 646-650.
4. А. Картан, С. Эйленберг, Гомологическая алгебра, "Наука", Москва, 1960
5. Ч. Кэртис, И. Райнер, Теория представлений конечных групп и ассоциативных алгебр, "Наука", Москва, 1969
6. Л. А. Скорняков, Гомологическая классификация колец, Мат. весник 4(19)(1967), 415÷434

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

ON A CLASS OF BISYMMETRIC $[n,m]$-GROUPOIDS

Zoran Stojaković

ABSTRACT. Bisymmetric $[n,m]$-groupoids were introduced in [4] (as a generalization of C^{n+1}-systems [2],[3]) and they were also studied in [5]. In this paper a class of bisymmetric $[n,m]$-groupoids is considered. It is shown that if a component operation of a bisymmetric $[n,m]$-groupoid is an n-groupoid with unity, then this component is an n-semigroup. It is also proved that this n-semigroup is an n-group with unity if there is another component operation which is an n-quasigroup. The structure of a bisymmetric $[n,m]$-groupoid the components of which are either n-groupoids with unity or n-quasigroups is described.

First we give some basic definitions. Notions from the general theory of n-quasigroups can be found in [1].

Instead of $x_p, x_{p+1}, \dots, x_q$ we shall write $\{x_i\}_{i=p}^q$ or x_p^q. If $p > q$, then x_p^q will be considered empty. The sequence $x, x, \dots, x$ (n times) will be denoted by $\overset{n}{x}$.

Let $Q(f)$ be an n-groupoid. An element $e \in Q$ is called a unity of $Q(f)$ iff

$$f(\overset{i-1}{e}, x, \overset{n-i}{e}) = x,$$

for all $x \in Q$ and every $i=1,\dots,n$.

An n-groupoid $Q(f)$ is called (i,j)-associative iff the following identity holds

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

If $Q(f)$ is an (i,j)-associative n-groupoid for all $i,j \in N_n = \{1,\dots,n\}$, then it is called an n-semigroup.

An n-quasigroup with unity is called an n-loop.

An n-semigroup which is an n-quasigroup is called an n-group.

An n-groupoid $Q(f)$ is called commutative iff the following identity holds

$$f(x_1^n) = f(x_{\phi(1)}^{\phi(n)})$$

for any permutation ϕ of N_n.

Let Q be a nonempty set, n and m positive integers and $f : Q^n \to Q^m$. Then $Q(f)$ is called an $[n,m]$-groupoid. The n-ary operations defined by

$$f_i(x_1^n) = y_i \iff (\exists y_1^{i-1}, y_{i+1}^m)(y_1^m) = f(x_1^n), \ i=1,\dots,m,$$

are called the component operations of f and this is denoted by $f = (f_1,\dots,f_m)$.

An $[n,m]$-groupoid $Q(f)$ is commutative ([6]) iff

$$f(x_1^n) = f(x_{\phi(1)}^{\phi(n)})$$

holds for all $x_i \in Q$, $i=1,\dots,n$ and any permutation ϕ of N_n. Obviously, an $[n,m]$-groupoid is commutative iff all its component operations are commutative n-groupoids.

Let $Q(f)$ be an $[n,m]$-groupoid, $f = (f_1,\dots,f_m)$. If $X = [x_{ij}]$ is an $n \times p$ array of elements from Q, then an $m \times p$ array $C_f(X) = [y_{ij}]$ is defined by

$$y_{ij} = f_i(x_{1j}^{nj}), \quad i=1,\dots,m, \quad j=1,\dots,p.$$

If $X = [x_{ij}]$ is an $r \times n$ array of elements from Q, then an $r \times m$ array $R_f(X) = [z_{ij}]$ is defined by

$$z_{ij} = f_j(x_{i1}^{in}), \quad i=1,\dots,r, \quad j=1,\dots,m.$$

An $[n,m]$-groupoid $Q(f)$ is said to be bisymmetric ([4]) iff for all $n \times n$ arrays $X = [x_{ij}]$ and every permutation ϕ of $N_n \times N_n$

$$C_f R_f(X) = C_f R_f(X^\phi),$$

where $X^\phi = [x_{\phi(i,j)}]$, holds.

In [4] it is shown that there are bisymmetric $[n,m]$-groupoids which are not commutative. But in [5] it is proved that a bisymmetric $[n,m]$-groupoid $Q(f)$, $f = (f_1,\dots,f_m)$, such that there is a component operation f_k for which $Rf_k = Q$ must be commutative (by Rf_k we denote the range of f_k).

THEOREM 1. *Let* $Q(f)$ *be a bisymmetric* $[n,m]$*-groupoid* $f=(f_1,\dots,f_m)$. *If* f_k *is an* n-*groupoid with unity, then* f_k *is an* n-*semigroup*.

Proof. Since $Q(f)$ is bisymmetric it follows that for every permutation ϕ of $N_n \times N_n$ the following identity holds

$$f_k(\{f_k(x_{i1}^{in})\}_{i=1}^{n}) = f_k(\{f_k(x_{\phi(i,1)}^{\phi(i,n)})\}_{i=1}^{n}) .$$

If e is a unity of f_k, $j \in N_n$, then

$$f_k(f_k(x_1,\overset{n-1}{e}),\dots,f_k(x_{j-1},\overset{n-1}{e}),\ f_k(x_j^{j+n-1}), f_k(x_{j+n},\overset{n-1}{e}),\dots$$
$$\dots,\ f_k(x_{2n-1},\overset{n-1}{e})) = f_k(f_k(x_1^n),\ f_k(x_{n+1},\overset{n-1}{e}),\ \dots$$
$$\dots,\ f_k(x_{2n-1},\overset{n-1}{e})),$$

i.e.

$$f_k(x_1^{j-1}, f_k(x_j^{j+n-1}),\ x_{j+n}^{2n-1}) = f_k(f_k(x_1^n),\ x_{n+1}^{2n-1}),$$

which means that f_k is $(1,j)$-associative for all $j \in N_n$. Hence, f_k is an n-semigroup.

THEOREM 2. *Let* $Q(f)$ *be a bisymmetric* $[n,m]$*-groupoid*, $f=(f_1,\dots,f_m)$. *If* f_j *is an* n-*quasigroup and* f_k *is an* n-*groupoid with unity, then* f_k *is an* n-*group with unity and there exists an Abelian group* $Q(+)$ *such that*

$$f_k(x_1^n) = \sum_{i=1}^{n} x_i$$

and

$$f_j(x_1^n) = \alpha \sum_{i=1}^{n} x_i$$

where α *is a permutation of* Q.

Proof. By the preceding theorem f_k is an associative operation.

Because of the bisymmetry of $Q(f)$ we have

$$f_j(\{f_k(x_i,\overset{n-1}{e})\}_{i=1}^{n}) = f_j(f_k(x_1^n),\ \overset{n-1}{\{f_k(\overset{n}{e})\}}) ,$$

where e is a unity of f_k, and

$$f_j(x_1^n) = f_j(f_k(x_1^n), \overset{n-1}{e}) .$$

If we define $\alpha : x \mapsto f_j(x, \overset{n-1}{e})$, then, since f_j is an n-quasigroup, α is a permutation of Q. Hence,

$$f_j(x_1^n) = \alpha f_k(x_1^n) .$$

From the last equality it follows that f_k is an n-quasigroup, so f_k is an n-group with unity. Then there exists ([1]) a group $Q(\cdot)$ such that

$$f_k(x_1^n) = x_1 \cdot x_2 \cdot \ldots \cdot x_n .$$

But f_k is an n-quasigroup and $Rf_k = Q$, so by Theorem 1 from [5] we get that f_k is a commutative n-group. If 0 is the unity of the group $\cdot$, then

$$x_1 \cdot x_2 \cdot 0 \cdot \ldots \cdot 0 = x_2 \cdot x_1 \cdot 0 \cdot \ldots \cdot 0$$

and $\cdot$ is an Abelian group.

THEOREM 3. *Let $Q(f)$ be a bisymmetric $[n,m]$-groupoid, $f = (f_1, \ldots, f_m)$. If component operations f_{j_ℓ}, $\ell = 1, \ldots, p$ are n-quasigroups, $\{j_1, \ldots, j_p\} \neq \emptyset$, and f_{k_i}, $i = 1, \ldots, q$ are n-groupoids with unity, then all operations f_{k_i}, $i = 1, \ldots, q$ are isomorphic n-groups with unity and there exist an Abelian group $Q(+)$, elements a_{j_ℓ}, $a_{k_i} \in Q$, $\ell = 1, \ldots, p$, $i = 1, \ldots, q$ and automorphisms α_{j_ℓ}, $\ell = 1, \ldots, p$ of the group $+$ such that*

$$f_{j_\ell}(x_1^n) = \alpha_{j_\ell} \sum_{s=1}^{n} x_s + a_j , \quad \ell = 1, \ldots, p;$$

$$f_{k_i}(x_1^n) = \sum_{s=1}^{n} x_s + a_{k_i} , \quad i = 1, \ldots, q .$$

Proof. From Theorem 2 it follows that every operation f_{k_i}, $i = 1, \ldots, q$ is an n-group with unity, and from the same theorem we get that they are all mutually isotopic. Since every n-loop which is isotopic to n-group with unity is isomorphic to that n-group ([1]), it follows that all operations

f_{k_i}, $i=1,\dots,q$ are isomorphic n-groups with unity.

By Theorem 4 from [5] it follows that there exist an Abelian group $Q(+)$, elements a_{j_ℓ}, $a_{k_i} \in Q$, $\ell=1,\dots,p$, $i=1,\dots,q$, and automorphisms α_{j_ℓ}, α_{k_i}, $\ell=1,\dots,p$, $i=1,\dots,q$ of the group $+$ such that

$$f_{j_\ell}(x_1^n) = \alpha_{j_\ell} \sum_{s=1}^{n} x_s + a_j \,, \quad \ell=1,\dots,q \,,$$

$$f_{k_i}(x_1^n) = \alpha_{k_i} \sum_{s=1}^{n} x_s + a_k \,, \quad i=1,\dots,q \,.$$

Since f_{k_i} is an n-group with unity e from the preceding equalities we obtain that for all $x \in Q$

$$\alpha_{k_i}(x+(n-1)e) + a_{k_i} = x.$$

Putting here $x=0$ (where 0 is the neutral element of the group $+$) gives $\alpha_{k_i}((n-1)e) + a_{k_i} = 0$, and this implies $\alpha_{k_i} x = x$ for all $x \in Q$. Hence, α_{k_i}, $i=1,\dots,q$ are identity mappings of Q.

R E F E R E N C E S

1. Белоусов В.Д., n-арные квазигруппы, Штиинца, Кишинев, 1972.
2. De Vito P., Zirilli F., Curve ellitiche normali e C^{n+1} - sistemi, Ricerche Mat. 27(1978), 319-332.
3. Polonjo M., Structure theorem for C^{n+1}-systems, Glasnik Mat. 16(36) (1981), 211-217.
4. Polonijo M., On C^{n+1}-systems and [n,m]-groupoids, Algebraic Conference, Beograd, 1982.
5. Stojaković Z., On bisymmetric [n,m]-groupoids, Univerzitet u Novom Sadu, Zbornik radova Prirodno-matematičkog fakulteta 12 (1982).
6. Paunić Dj., Stojaković Z., Identities on multiquasigroups, Proc. Symp. on n-ary structures, Skopje, 1982, 195-200.

Institut za matematiku, Dr Ilije Djuričića 4,

21000 Novi Sad, Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

S-БАЗИСЫ ДЛЯ ОДНОЙ МОДИФИКАЦИИ АЛГЕБРЫ ЛОГИКИ

Иван Стойменович

РЕЗЮМЕ. В работе определяются симметрические функции для каждого от 9 типов алгебры ϕ^{O} (одной модификации алгебры логики). Найдены также числа двухчленных, трехчленных и четырехчленных S-базисов, состоящихся из n-местных симметрических функций, и числа S-базисов, состоящихся из функций, зависящих от не более n аргументов.

В.М.Глушков предложил рассматривать алгебры, которые являются модификациями алгебр Поста [2] и связаны с операцией композиции $\otimes$, определяемой тождеством

$$(f\otimes g)(x_1,x_2,\dots,x_{m+n-1}) = f(g(x_1,x_2,\dots,x_n), g(x_2,x_3,\dots,x_{n+1}),\dots,g(x_m,x_{m+1},\dots,x_{m+n-1})) ,$$

где f,g-произволяные m-местная и n-местная функции. Эти алгебры находят приложения при рассмотрении логических структур ЭЦВМ, Пусть ϕ^{O} алгебра булевских функций система операций которой в отличие от алгебр Поста вместо суперпозиции содержит операцию $\otimes$.

<u>Определение.</u> Конечная система функций $K\subseteq\phi^{O}$. Называется базисом, если:

1. Каждая функция из ϕ^{O} получается из функций системы К путем отождествления аргументов, их перестановки, приписывания фиктивного аргумента и применения операции композиции $\otimes$.
2. Никакая из ее подсистем не обладает свойством 1.

Целью настоящей статьи является исследование всех базисов алгебры ϕ^{O}, состоящих из симметричных функций. Подобную проблему для алгебры логики исследовал Р.Тошич |4|.
Симметричные функции находят приложения в теории контактных схем.

НЕКОТОРЫЕ ОБОЗНАЧЕНИЯ

Дальше нам понадобятся нижеследующие множества:

$T_{ij} = \{f \mid f\in\phi^{O}, f(0,\dots,0)=i,\ f(1,\dots,1)=j\},\ 0\le i,j\le 1,$

$V = \{f \mid f\in\phi^{O}, f(x_1,x_2,\dots,x_n) = f'(x_1',x_2',\dots,x_n')\}$,

т.е. множество всех самодвойственных булевских функций.

$M_1 = \{f \mid f\in\phi^{O},\ \forall(a,b)\, a\le b \Rightarrow f(a)\le f(b)\}$, где $a=(a_1,a_2,\dots,a_n)$, $b=(b_1,b_2,\dots,b_n)$ и $a\le b$ если $a_i\le b_i$ $(1\le i\le n)$,

$$M_2 = \{f \mid f \in \phi^o,\ f' \in M_1\},$$

т.е. множества всех изотонных и антитонных булевских функций.

$$A = T_{oo} \cup T_{o1} \cup T_{11},\ B = T_{00} \cup T_{11} \cup V,\ C = T_{00} \cup T_{11} \cup M_1 \cup M_2,$$
$$D = T_{01} \cup T_{10} \cup \{0,1\}.$$

Для каждого $K \subseteq \phi^o$ пусть $K' = \phi^o \setminus K$..

ТЕОРЕМА (Цейтлина ([5]) Для того чтобы система функций $K \subseteq \phi^o$ была базой, необходимо и достаточно чтобы:

1^o в К содержались:

-по крайней мере одна функция, не принадлежащая А,

-по крайней мере одна функция, не принадлежащая В,

-по крайней мере одна функция , не принадлежащая С,

-по крайней мере одна функция , не принадлежащая D.

2^o Никакая из ее подсистем не обладала свойством 1^o.

НЕКАТОРЫЕ СВОЙСТВА СИММЕТРИЧНЫХ ФУНКЦИЙ

Определение: n-местная функция $f(x_1,\dots,x_n)$ алгебры логики называется симметрической если $f(x_1,\dots,x_n) = f(y_1,\dots,y_n)$, где $(y_1,\dots,y_n)$-любая перестановка $(x_1,\dots,x_n)$.

ЛЕММА 1. ([1] , п. 178.) Если среди членов дизъюнктивной совершенной нормальной формы (ДСНФ) n-местной симметрической функции есть член, в который входят m букв с отрицаниями, то в ДСНФ обязательно входят все возможные члены с m отрицаниями над буквами.

Определение. Фундаментальной симметрической функцией индекса m называется такая функция алгебры логики, у которой все члены, входящие в ДСНФ этой функции, имеют ровно m букв без отрицания. Фундаментальную симметричную n-местную функцию индекса m мы будем обозначать как S^n_m .

ЛЕММА 2. ([1],п. 178) Любая симметричная функция есть дизъюнкция фундаментальных симметричных функций, индекс которых определяется однозначно заданной симметричной функцией.

Определение. $S^n_{K_1,\dots,K_m} = S^n_{K_1} \vee \dots \vee S^n_{K_m}$ $(n \geq 1)$.

Определение. $S^n_L = S^n_{K_1,\dots,K_m}$ если $L = \{K_1,\dots,K_m\}$.

Пусть S_n множество всех симметричных n-местных функций алгебры логики. Если $k(X)$ обозначает число всех функций множества X, то $k(S_n) = 2^{n+1}$.

Определение. S-базисом алгебры логики называется базис, который содержит только симметричные функции.

ЛЕММА 3. ([4]) Число n-местных симметричных функций без фиктивных переменных равно $2^{n+1}-2$. Только функции 0 и 1 вырожденные.

ЛЕММА 4. Эсли $H=\{1,2,\dots,n-1\}$ и $\{k_1,\dots,k_m\}\subseteq H$, то

$$S^n_{k_1,\dots,k_m}\in T_{00}\cap S_n;\quad S^n_{k_1,\dots,k_m,n}\in T_{01}\cap S^n;$$

$$S^n_{0,k_1,\dots,k_m}\in T_{10}\cap S_n;\quad S^n_{0,k_1,\dots,k_m,n}\in T_{11}\cap S_n.$$

Доказательство. Пусть $S^n_L=f(x_1,\dots,x_n)$. Лемма следует из следующих фактов: $f(0,\dots,0)=1 \Leftrightarrow 0\in L$ и $f(1,\dots,1)=1\Leftrightarrow n\in L$.

Из леммы 4 вытекает:

ЛЕММА 5. $k(T_{00}\cap S_n)=k(T_{01}\cap S_n)=k(T_{10}\cap S_n)=k(T_{11}\cap S_n)=2^{n-1}$.

Следующие две леммы доказаны в [4].

ЛЕММА 6. Эсли n четное число, то $S_n\cap V=\phi$.

ЛЕММА 7. Число n-местных изотонных симметрчных функций равно $n+2$. Это функции $S^n_{0,1,\dots,n}$, $S^n_{1,2,\dots,n};\dots;S^n_n$; $S^n_\phi=0$.

Для четного n $M_1\cap S_n\cap V=\phi$. Для нечетного $n=2m+1$ только функция $S^{2m+1}_{m+1,\dots,2m,2m+1}$ изотонна и самодвойственна.

ЛЕММА 8. Эсли n нечетное число $(n=2m+1)$, то $k(S_n\cap V)=2^{\frac{n+1}{2}}$ и $S_n\cap V=\{S_{k_0,k_1,\dots,k_m}\}$, где ровно одно из чисел $i,n-i$ $(0\le i\le m)$ принадлежит множеству $\{k_0,\dots,k_m\}$.

Доказательство содержится в доказательстве теоремы 1 ([4]).

ЛЕММА 9. Эсли $0\le k_i\le n$, $L=\{k_1,\dots,k_m\}$ и $L'=\{0,1,\dots,n\}\setminus L$, то

$$(S^n_L)'=S^n_{L'}.$$

Доказательство. Легко проверить равенства $S^n_L\vee S^n_{L'}=1$, $S^n_L\wedge S^n_{L'}=0$.

ЛЕММА 10. $S_n\cap M_2=S^n_{0,1,\dots,n}=1$, $S^n_{0,1,\dots,n-1}$, $S^n_{0,1,\dots,n-2}$, ... S^n_0, $S^n_\emptyset=0$, $k(S_n\cap M_2)=n+2$, $S_n\cap M_2\cap V=\emptyset$ для $n=2m$ $S_n\cap M_2\cap V=\{S^n_{0,1,2,\dots,m}\}$ для $n=2m+1$.

Доказательство. Первое утверждение вытекает из определения M_2, леммы 7 и леммы 9, а последнее следует из леммы 8.

4. ТИПЫ СИММЕТРИЧНЫХ ФУНКЦИЙ АЛГЕБРЫ ϕ^o

Эсли функция f принадлежит классу X (X $\in$ {A,B,C,D}), будем говорить , что она имеет свойство X. Эсли функция обладает, например, свойствами A,C и не обладает свойствами B,D, будем говорить что это функция типа A,C и обозначим ее через /A,C/. Две функции, обладающие одними и теми же свойствами будем называть функциями, одного и того же типа.

ЛЕММА 11. Число различных типов функций из ϕ^o равно 9:

1. /A,B,C,D/,	4. /A,C,D/,	7. /B,D/ ,
2. /A,B,C/,	5. /B,C,D/ ,	8. /C,D/,
3. /A,B,D/,	6. /A,D/ ,	9. /D/ .

Лемму доказал Р.Тошич [3] .

Пусть, например, $k/A,C,D/_S(n)$ число n-местных симметричных функций типа /A,C,D/, а $k/A,C,D/_S(\leq n)$ число симметричных функций типа /A,C,D/ , зависящих от не более чем n аргументов. В силу следующей теоремы каждый от 9 типов содержит симметричные функции.

ТЕОРЕМА 1.

1. $k/A,B,C,D/_S(n) = \begin{cases} 2 & \text{для } n=2m \\ 3 & \text{для } n=2m+1 \end{cases}$. Этом типу принадлежат константы 0 и 1. Для n=2m+1 этом типу принадлежит и функция $S^{2m+1}_{m+1,\dots,2m+1}$.

2. $k/A,B,C/_S(n)=2^n-2$. Этом типу принадлежат функции $S^n_{k_1,\dots,k_m}$ и $S^n_{0,k_1,\dots,k_m,n}$, $\{k_1,\dots,k_m\}\subseteq H$, за исключением констант 0 и 1.

3. $k/A,B,D/_S(n) = \begin{cases} 0 & \text{для } n=2m \\ 2^{\frac{n-1}{2}}-1 & \text{для } n=2m+1. \end{cases}$ Для n=2m+1 этот тип содержит функции $S^n_{k_1,\dots,k_m,2m+1}$, $k_i \in \{i,n-i\}$, $1 \leq i \leq m$, за исключением функции $S^{2m+1}_{m+1,\dots,2m+1}$.

4. $k/A,C,D/_S(n) = \begin{cases} n & \text{для } n=2m \\ n-1 & \text{для } n=2m+1 \end{cases}$. Этом типу принадлежат $S^n_{1,2,\dots,n}, S^n_{2,\dots,n}, S^n_{3,\dots,n};\dots;S^n_n$. Для n=2m+1 исколючается

самодвойственная функция $S^{2m+1}_{m+1,\ldots,2m+1}$.

5. $k/B,C,D/_S(n) = \begin{cases} 0 & \text{для } n=2m \\ 1 & \text{для } n=2m+1 \end{cases}$. Единственная функция этого типа $S^n_{0,\ldots,m}$ для $n=2m+1$.

6. $k/A,D/_S(n) = \begin{cases} 2^{n-1}-n & \text{для } n=2m \\ 2^{n-1} - 2^{\frac{n-1}{2}} - n+1 & \text{для } n=2m+1 \end{cases}$. Этот тип содержит функции $S^n_{k_1,\ldots,k_m,n}$, $\{k_1,\ldots,k_\ell\} \subseteq H$, за исключением функций $S^n_{1,2,\ldots,n}$; $S^n_{2,\ldots,n}$; $S^n_{3,\ldots,n}$; ...; S^n_n. Для $n=2m+1$ исключаются и функции $S^{2m+1}_{k_1,\ldots,k_m,n}$, $k_i \in \{i,n-i\}$, $1 \le i \le m$.

7. $k/B,D/_S(n) = \begin{cases} 0 & \text{для } n=2m \\ 2^{\frac{n-1}{2}}-1 & \text{для } n=2m+1. \end{cases}$ Для нечетного $n=2m+1$ этом типу принадлежат функции $S^{2m+1}_{0,k_1,\ldots,k_m}$; $k_i \in \{i,n-i\}$, $1 \le i \le m$, за исключением функции $S^n_{0,1,\ldots,m}$.

8. $k/C,D/_S(n) = \begin{cases} n & \text{для } n=2m \\ n-1 & \text{для } n=2m+1 \end{cases}$. Этот тип содержит функции $S^n_{0,1,\ldots,n-1}$; $S^n_{0,1,\ldots,n-2}$; ...; S^n_0. Для $n=2m+1$ исключается функция $S^n_{0,1,\ldots,m}$.

9. $k/D/_S(n) = \begin{cases} 2^{n-1}-n & \text{для } n=2m \\ 2^{n-1}-2^{\frac{n-1}{2}}-n+1 & \text{для } n=2m+1 \end{cases}$. Этом типу принадлежат функции $S^n_{0,k_1,\ldots,k_\ell}$, $\{k_1,\ldots,k_\ell\} \subseteq H$, за исключением функций $S^n_{0,1,\ldots,n-1}$; $S^n_{0,1,\ldots,n-2}$; ...; $S^n_{0,1}$; S^n_0 .

Для $n=2m+1$ исключаются и функции $S^{2m+1}_{0,k_1,\ldots,k_m}$, $k_i \in \{i,n-i\}$, $1 \le i \le m$.

Доказательство. В доказательстве пользуются равенства между множествими доказаные в |3|.

1. $A \cap B \cap C \cap D = (T_{01} \cap V \cap M_1) \cup \{0,1\}$. Вытекает из лемм 4 и 7.
2. $A \cap B \cap C \cap D' = (T_{00} \cup T_{11}) \setminus \{0,1\}$. Вытекает из леммы 4.
3. $A \cap B \cap C' \cap D = (T_{01} \cap V) \setminus M_1$. Вытекает из леммы 6 для $n=2m$. Для $n=2m+1$ вытекает из лемм 8,9 и 6.
4. $A \cap B' \cap C \cap D = M_1 \setminus (\{0,1\} \cup (T_{01} \cap V))$. Следует из леммы 7.

5. $A' \cap B \cap C \cap D = T_{10} \cap V \cap M_2$. Для $n=2m$ следует из леммы 6, а для $n=2m+1$ следует из лемм 4 и 10.

6. $A \cap B' \cap C' \cap D = T_{01} \setminus ((T_{01} \cap V) \cup M_1)$. Следует из лемм 4, 6 и 7. Для $n=2m+1$ пользуется и лемма 8.

7. $A' \cap B \cap C' \cap D = (T_{10} \cap V) \setminus M_2$. Для $n=2m$ следует из леммы 6. Для $n=2m+1$ следует из лемм 4, 8 и 10.

8. $A' \cap B' \cap C \cap D = M_2 \setminus (\{0,1\} \cup (T_{10} \cap V))$. Следует из лемм 4 и 10.

9. $A' \cap B' \cap C' \cap D = T_{10} \setminus ((T_{10} \cap V) \cup M_2)$. Следует из лемм 4,10,6 и 8.

В силу теоремы 1 и леммы 3 суммируя соответственные выражения легко получается

ТЕОРЕМА 2. 1. $k/A,B,C,D/_S(\le n) = \left[\frac{n+5}{2}\right]$.

2. $k/A,B,C/_S (\le n) = 2^{n+1}-2\,(n+1)$.

3,7. $k/A,B,D/_S (\le n) = k/B,D/_S (\le n) = 2^{\left[\frac{n+1}{2}\right]} - \left[\frac{n+3}{2}\right]$.

4,8. $k/A,C,D/_S (\le n) = k/C,D/_S (\le n) = \left[\frac{n^2}{2}\right]$.

5. $k/B,C,D/_S (\le n) = \left[\frac{n+1}{2}\right]$.

6,9. $k/A,D/_S (\le n) = k/D/_S (\le n) = 2^n - 2^{\left[\frac{n+1}{2}\right]} - \left[\frac{n^2}{2}\right]$.

СИМЕТРИЧНЫЕ БАЗИСЫ АЛГЕБРЫ Φ^0

Тип каждого базиса алгебры Φ^0 определяется типами принадлежащих функций этого базиса. Следующая лемма доказана в [3].

ЛЕММА 12. Число различных типов базисов в Φ^0 равно 8:

I Двухчленные типы базисов: {/A,B,C/,/D/} .

II Трехчленные типы базисов: {/A,B,C/,/C,D/,/A,B,D/} , {/A,B,C/,/C,D/,/A,D/}, {/A,B,C/,/C,D/,/B,D/}, {/A,B,C/,/B,D/,/A,C,D/}, {/A,B,C/,/B,D/,/A,D/}, {/A,B,C/,/A,D/,/B,C,D/} .

III Четырехчленные типы базисов:{/A,B,C/,/A,B,D/,/A,C,D/, /B,C,D/}. Пусть N_i^n и $N_i^{(\le n)}$ число всех i-членных S-базисов, состоящихся только из n-местных функций, соответственно из функций зависящих от не более, чем от n переменных.

Используя теоремы 1 и 2 и лемму 12 можно легко проверить равенства в следующей теореме.

<u>ТЕОРЕМА 3.</u> 1. $N_2^0 = N_3^0 = N_4^0 = 0$. <u>В остальных равенствах</u> $n > 0$.

2. $$N_2^n = \begin{cases} 2\,(2^{n-1}-1)(2^{n-1}-n) & \text{для } n=2m, \\ 2(2^{n-1}-1)(2^{n-1}-2^{\frac{n-1}{2}}-n+1) & \text{для } n=2m+1\,. \end{cases}$$

3. $$N_3^n = \begin{cases} 2n(2^{n-1}-1)(2^{n-1}-n) & \text{для } n=2m \\ 2(2^{n-1}-1)(3(n-1)(2^{\frac{n-1}{2}}-1)+(2^{n-1}-2^{\frac{n-1}{2}}-n+1)(n-1+2^{\frac{n-1}{2}})) & \text{для } n \neq 2m. \end{cases}$$

4. $$N_4^n = \begin{cases} 0 & \text{для } n=2m \\ 2(2^{n-1}-1)(2^{\frac{n-1}{2}}-1)(n-1) & \text{для } n=2m+1\,. \end{cases}$$

5. $$N_2^{(\le n)} = (2^{n+1}-2(n+1))(2^n-2^{[\frac{n+1}{2}]}-[\frac{n^2}{2}]).$$

6. $$N_3^{(\le n)} = (2^{n+1}-2(n+1))(3[\frac{n^2}{2}](2^{[\frac{n+1}{2}]}-[\frac{n+3}{2}]) + (2^n-2^{[\frac{n+1}{2}]}-[\frac{n^2}{2}])\cdot(2^{[\frac{n+1}{2}]}-1+[\frac{n^2}{2}]))\,.$$

7. $$N_4^{(\le n)} = (2^{n+1}-2(n+1))(2^{[\frac{n+1}{2}]}-[\frac{n+3}{2}])\,[\frac{n^2}{2}]\,[\frac{n+1}{2}]\,.$$

<u>СЛЕДСТВИЕ 1.</u> $N_2^1 = N_3^1 = N_4^1 = N_2^2 = N_3^2 = N_4^2 = N_2^{(\le 2)} = N_3^{(\le 2)} = N_4^{(\le 2)} = 0$.

S-базис не может содержаться только из функций, зависящих от не более двух переменных.

<u>СЛЕДСТВИЕ 2.</u> $N_2^3 = 0$, $N_3^3 = 36$, $N_4^3 = 12$, $N_2^{(\le 3)} = 0$, $N_3^{(\le 3)} = 96$, $N_4^{(\le 3)} = 64$.

Например, функции трех переменных определяют 12 четырехчленных S-базисов:

$\{S_1^3, S_{1,3}^3, S_{1,2,3}^3, S_{0,1}^3\}$, $\{S_1^3, S_{1,3}^3, S_3^3, S_{0,1}^3\}$,

$\{S_2^3, S_{1,3}^3, S_{1,2,3}^3, S_{0,1}^3\}$, $\{S_2^3, S_{1,3}^3, S_3^3, S_{0,1}^3\}$,

$\{S_{1,2}^3, S_{1,3}^3, S_{1,2,3}^3, S_{0,1}^3\}$, $\{S_{1,2}^3, S_{1,3}^3, S_3^3, S_{0,1}^3\}$,

$\{S_{0,3}^3, S_{1,3}^3, S_{1,2,3}^3, S_{0,1}^3\}$, $\{S_{0,3}^3, S_{1,3}^3, S_3^3, S_{0,1}^3\}$,

$\{S_{0,1,3}^3, S_{1,3}^3, S_{1,2,3}^3, S_{0,1}^3\}$, $\{S_{0,1,3}^3, S_{1,3}^3, S_3^3, S_{0,1}^3\}$,

$\{S_{0,2,3}^3, S_{1,3}^3, S_{1,2,3}^3, S_{0,1}^3\}$, $\{S_{0,2,3}^3, S_{1,3}^3, S_3^3, S_{0,1}^3\}$.

По аналогичному способу можно получить все S-базисы каждого типа.

<u>СЛЕДСТВИЕ 3.</u> Наименьшее n для которого существуют двухчленные

базисы состоящиеся из n-местных функций есть $4 (N_2^4 = 56)$. Пример двухчленного базиса: $\{S_1^4, S_{0,2}^4\}$.

ЛИТЕРАТУРА

[1] V.M.Gluškov, Sinteza cifarskih automata, Beograd, 1967.

[2] А.И.Мальцев, Итеративные алгебры и многообразия Поста, сб. "Алгебра и логика", Т.5, в п. 2, Новосибирск, 1965.

[3] Р.Тошич, Типи базисов для одной модификации алгебры логики, Zbornik radova PMF, serija za matematiku, 11(1981) 287-295.

[4] R.Tošić, S-bases of propositional algebra, Publ. Inst.Math. 14(28)(1972), 139-148, Beograd.

[5] Г.Е.Цейтлин, Вопросы функциональной полноты для одной модификации алгебры логики, Кибернетика, 4(1969).

Ivan Stojmenović
Institut za matematiku
dr Ilije Djuričića 4,
21000 Novi Sad
Jugoslavija

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

MONOTONE MAPPINGS OF ORDERED SETS

Milán R. Tasković

1. **Introduction.** An map f of a partially ordered set P to itself has a *fixed point* if there exists an element ξ in P such that $f(\xi) = \xi$. An ordered pair (u, v) is called a *fixed edge* of f if $f(u) = v$ and $f(v) = u$, where $u \leqslant v$ ($u, v \in P$). In a noted paper [TA] Tarski has shown that every order-preserving (isotone or increasing) map of a complete lattice into itself has a fixed point. Davis [DA] proved the converse: Every lattice, with the fixed point property is complete. Order-reversing (antitone or decreasing) maps, on the other hand, may or may not have fixed points. In a noted papers [KJ] Klimeš and [TM] Tasković has shown that every antitone map of a complette lattice into itself has a fixed edge. The analogous problems for *conditionally complete* partially ordered sets has remained largely unexplored.

Let (P, $\leqslant$) be partially ordered set. For $x, y \in P$ and $x < y$, the set (x, y) is defined by

$$(x, y) = [t : t \in P \text{ and } x < t < y].$$

We begin with a statements for **conditionally complete sets** (that is, every nonempty subset of P with upper bound has its supremum).

Lemma 1. *Let* (P, $\leqslant$) *be a partially ordered set and* f *an isotone mapping from* P *into* P *such that:*

(A) f *has a* fork i.e. $a \leqslant f(a) \leqslant f(b) \leqslant b$ *for some* $a, b \in P$, and

(B) *The set* (a, b) *(or* P*) is a conditionally complete.*

Then the set $P(f) := [x \in P : f(x) = x]$ *is nonempty.*

Lemma 2. (Fixed Edge Lemma). *Let* (P, $\leqslant$) *be a conditionally complete partially ordered set and* f *an antitone mapping from* P *into* P *such that* f *has a fork type*

(C) $a \leqslant f(b) \leqslant f(a) \leqslant b$ *for some* $a, b \in P$.

Then there exists a fixed edge (u, v) *of* f *and there exists an* u *with the least element in* P *such that* (u, f(u)) *is the fixed edge of* f.

2. **The main results and corollaries.** With the help of Lemmas we now obtain the main results of this paper:

Theorem 1. *Let* (P, $\leqslant$) *be a partially ordered set. For set* (a, b) or P *to be conditionally complete it is necessary and sufficient that every isotone function* $f: P \rightarrow P$ with *fork have a fixed point.*

Theorem 2. *Let* (P, $\leqslant$) *be a partially ordered set. For set* (a, b) or P *to be conditionally complete it is necessary and sufficient that every antitone function* f:P → P *with fork (C) have a fixed edge.*

Special cases of Theorem 1. have been discussed by Davis [DA] and some others.

Corollary 1. (A. Davis [DA]) *For a lattice* (L, $\leqslant$) *to be complete it is necessary and sufficient that every isotone function* f: L → L *have a fixed point.*

Corollary 2. *Let* (P, $\leqslant$) *be a partially ordered set. For a maximal chain* L = (a, b) ⊂ P *to be conditionally complete it is necessary and sufficient that every increasing function* f:P → P *such* that (A) *have a fixed point.*

Corollary 3. If (P, $\leqslant$) *is a partially ordered sets and if every isotone function* f:P → P *has a fixed point, then every maximal chain of* P *is a complete set.*

The proofs of these results with a more detailed discussion and some examples will be published in [TM].

But the main question is open.

Problem: Let P be a nonempty ordered set and f:P → P. Solve the following functional equation $f^2(x) := f(f(x)) = g(x)$, where g:P → P is given arbitrary function.

References

[DA] **A.C.Davis**, A Characterization of complete lattices, Pacific J. Math. 5 (1955), 311-319.

[BG] **Birkhoff G.**, Lattice theory, Amer. Math. Soc. Colloq. Publ. vol. 25, New York, 1948.

[KĐ] **Kurepa Đ.**, Fixpoints of monotone mappings of ordered sets, Glasnik Math. fiz. astr. 19 (1964), 167–173.

[KJ] **Klimeš J.**, Fixed edge theorems for complete lattices, Arch. Math. 4. scripta, 17 (1981), 227–234.

[TA] **Tarski A.**, A lattice theoretical fixpoint theorem and its applications, Pacific J. Math. 5 (1955), 285–309.

[TM] **Tasković M.**, Characterization of conditionally complete sets (to appear).

M. Tasković
Prirodno-matematički fakultet
11.000 Beograd
p. p. 550
Yugoslavia

THIRD ALGEBRAIC CONFERENCE
Beograd, 3-4 December 1982

ON A QUASIIDENTITY IN n-ARY QUASIGROUPS

J.Ušan, K.Stojmenovski

Abstract. A generalization of the Reidemeister condition for n-ary quasigroups is considered. (A generalization of this condition for ternary nets is given in [1].)

First we will give some definitions.

Let Q be a nonempty set, Q^n the Cartesian n-th power of Q and $A: Q^n \to Q$ a mapping. The ordered pair (Q,A) is called an n-quasigroup if for any $(a_1,\dots,a_{i-1},a_{i+1},\dots,a_n,b) \in Q^n$ and $i \in \{1,\dots,n\}$ the equation

$$A(a_1,\dots,a_{i-1},x,a_{i+1},\dots,a_n) = b \qquad (1)$$

has a unique solution.

Further on we will denote the sequence $(a_1,\dots,a_n) \in Q^n$ shortly by $\bar{a}$, and the sequence $(a_1,\dots,a_{i-1},a_{i+1},\dots,a_n)$ by $i(\bar{a})$.

If $\bar{a}$ is any fixed element of Q^n and $i \in \{1,\dots,n\}$, then the mapping

$$L_{i(\bar{a})}: x \to A(a_1,\dots,a_{i-1},x,a_{i+1},\dots,a_n)$$

is called a translation of the n-quasigroup (Q,A) [2]. We note that any translation of (Q,A) is a permutation of the set Q. The n-ary operation B on Q, defined by:

$$B(x_1,\dots,x_n) = A(L^{-1}_{1(\bar{a})}x_1,\dots,L^{-1}_{n(\bar{a})}x_n), \qquad (2)$$

where $\bar{a}$ is a given element of Q^n, is called an LP-isotop of the n-quasigroup (Q,A). So, any fixed element $(a_1,\dots,a_n) \in Q^n$ determines an LP-isotop of (Q,A) by (2).

It can be shown that (Q,B) is an n-quasigroup with an identity element $e = A(a_1,\dots,a_n)$, i.e. (Q,B) is an n-loop.

We can write the equality (2) in the following form:

$$A(x_1,\dots,x_n) = B(L_{1(\bar{a})}x_1,\dots,L_{n(\bar{a})}x_n). \qquad (2')$$

We will investigate some properties of LP-isotops when the n-quasigroup (Q,A) satisfies a special condition.

Let (Q,A) be an n-quasigroup. Consider the quasiidentity

$$
\begin{aligned}
&A(x_1^1,\ldots,x_n^1) = A(x_1^3,\ldots,x_n^3)\\
&\bigwedge_{i=1}^{n} A(x_1^1,\ldots,x_{i-1}^1,x_i^2,x_{i+1}^1,\ldots,x_n^1) = \\
&= A(x_1^3,\ldots,x_{i-1}^3,x_i^4,x_{i+1}^3,\ldots,x_n^3)\\
&\Rightarrow A(x_1^2,\ldots,x_n^2) = A(x_1^4,\ldots,x_n^4),
\end{aligned}
\tag{3}
$$

where $x_1,\ldots,x_n$ are variables. If n=2, i.e. A is a binary operation, then (3) is the Reidemeister condition [1].

THEOREM. The condition (3) in an n-quasigroup (Q,A) holds if and only if any two LP-isotops of (Q,A) with a (given in advance) common identity element are equal.

Proof. Let (Q,C) and (Q,D) be LP-isotops of an n-quasigroup (Q,A). By (2´) we obtain

$$A(x_1,\ldots,x_n) = C(L_{1(\bar{x})}x_1,\ldots,L_{n(\bar{x})}x_n), \tag{4}$$

$$A(x_1,\ldots,x_n) = D(L_{1(\bar{y})}x_1,\ldots,L_{n(\bar{y})}x_n), \tag{5}$$

where $\bar{x} = (x_1^1,\ldots,x_n^1)$ and $\bar{y} = (x_1^3,\ldots,x_n^3)$ are fixed elements of Q^n, $A(\bar{x})$ adn $A(\bar{y})$ are identity elements of (Q,C) and (Q,D) respectively.

Let the following condition

$$e_C = e_D \Rightarrow C = D \tag{6}$$

be satisfied. By the hypothesis $e_C=e_D$ it follows that

$$A(x_1^1,\ldots,x_n^1) = A(x_1^3,\ldots,x_n^3).$$

Substituing $x_1=x_1^2,\ldots,x_n=x_n^2$ in (4), $x_1=x_1^4,\ldots,x_n=x_n^4$ in (5) and using the assumption that the condition on the left-hand side of the implication (3) holds and C=D, we obtain

$$A(x_1^2,\ldots,x_n^2) = A(x_1^4,\ldots,x_n^4),$$

which means that (3) is satisfied.

Conversely, suppose that (3) holds in an n-quasigroup (Q,A) and let $e_C=e_D$ be an identity element of the LP-isotops of (Q,A), defined by (4) and (5). It is necessary to show that C=D. By the equalities

$$A(x_1^2,x_2^1,x_3^1,\dots,x_n^1) = A(x_1^4,x_2^3,x_3^3,\dots,x_n^3) = t_1,$$
$$A(x_1^1,x_2^2,x_3^1,\dots,x_n^1) = A(x_1^3,x_2^4,x_3^3,\dots,x_n^3) = t_2, \quad (7)$$
$$\vdots$$
$$A(x_1^1,\dots,x_{n-1}^1,x_n^2) = A(x_1^3,\dots,x_{n-1}^3,x_n^4) = t_n,$$

where $t_1,\dots,t_n$ are arbitrarily chosen elements of Q, we conclude that the elements $x_1^2,\dots,x_n^2,x_1^4,\dots,x_n^4$ are uniquele determined. By (3), (4), (5) it follows that

$$C(t_1,\dots,t_n) = A(x_1^2,\dots,x_n^2) = A(x_1^4,\dots,x_n^4) = D(t_1,\dots,t_2),$$

i.e. C=D. The proof of the Theorem is completed.

COROLLARY 1. _If an n-quasigroup (Q,A) satisfies condition (3), then the number of their LP-isotops is not greater than_ $|Q|$.

Namely, let $a \in Q$. For any solution of the equation $A(x_1,\dots,x_n) = a$ we obtain an LP-isotop of (Q,A), determined by (2). All of them have a common identity element e=a, and thus they are equal.

Let (Q,A) be an n-quasigroup. If we substitute the variables $x_{i_1},\dots,x_{i_{n-2}}$ by arbitrary fixed elements of Q, then we will obtain a binary quasigroup (a binary retract) $(Q,\cdot)$ of the n-quasigroup (Q,A).

COROLLARY 2. _If an n-quasigroup (Q,A) satisfies (3) then any of its binary retracts is isotopic with a group._

Namely, if n-2 variables in (3) are fixed, then the Reidemeister condition for the binary retracts of the n-quasigroup (Q,A) is satisfied, and thus any binary retract is isotopic with a group [3].

REFERENCES

1. F.Radó, _Eine Bedingung für die Regularität der Gewebe_, Mathematica 2(25) (1960), 325-334

2. В.Д.Белоусов, _n-арные квазигруппы_, Штиинца, Кишинев (1972)

3. В.Д.Белоусов, _Основы Теории квазигрупп и луп_, Наука, Москва (1967)

Institut za Matematiku, PMF
21000 Novi Sad, Jugoslavija

Matematički fakultet
91000 Skopje, Jugoslavija