INSTITUTE OF MATHEMATICS
UNIVERSITY OF NOVI SAD

PROCEEDINGS OF THE CONFERENCE "ALGEBRA AND LOGIC" CETINJE

1986.

NOVI SAD
1987

PROCEEDINGS OF THE CONFERENCE
"ALGEBRA AND LOGIC", CETINJE 1987
published by
INSTITUTE OF MATHEMATICS
FACULTY OF SCIENCE
UNIVERSITY OF NOVI SAD
DR ILIJE DJURIČIĆA 4
21000 NOVI SAD, YUGOSLAVIA

This publication was supported by the Self-Management Community of Interest for Scientific Research of SAP Vojvodina.

Printed by: "Prepisi - umnožavanja", Vidosav Novaković, Beograd, M. Tolbuhina bb.

Number of copies: 400

P R E F A C E

The Fifth Yugoslav Algebraic Conference "Algebra and Logic" took place in Cetinje, June 12-14, 1986 and was organized by the Institute of Mathematics and Physics, Titograd and the Society of Mathematicians and Physicists of SR Crna Gora.

This volume contains most of the papers presented at the Conference. It is the seguel to the four volumes containing proceedings of the previous Algebraic Conferences, the first one published by the Matematički fakultet, Skopje and others by the Institute of Mathematics, Novi Sad.

We would like to thank all the contributors for responding to our invitation and for their contribution to this volume. All papers were refereed and we would like to extend our thanks to the referees for their effort.

Zoran Stojaković

C O N T E N T S

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

ON LATTICES OF SOME CONGRUENCES ON REGULAR SEMIGROUPS

Branka P.Alimpić and Dragica N.Krgović

Abstract. In this paper E-unitary and E-reflexive congruences on a regular semigroup S are considered. The set $\mathcal{U}(S)$ of all E-unitary congruences and the set $\mathcal{R}(S)$ of all E-reflexive congruences on S, ordered by inclusion, are complete lattices. A complete homomorphism of the lattice $\mathcal{U}(S)$ onto the lattice of all group congruences, and a complete $\vee$-homomorphism of the lattice $\mathcal{R}(S)$ onto the lattice of all Clifford congruences on S are obtained.

Throughout this paper, S stands for an arbitrary regular semigroup, and E(S) denotes the set of idempotents of S. It is known that a congruence ρ on a regular semigroup S is uniquely determined by its kernel $\ker\rho = \{x \in S \mid (\exists e \in E(S)) x \rho e\}$ and trace $\mathrm{tr}\,\rho = \rho|_{E(S)}$ [2]. Let Con S be the congruence lattice of S, K and T equivalences on Con S defined by

$$\rho K \xi \iff \ker\rho = \ker\xi \quad \text{and} \quad \rho T \xi \iff \mathrm{tr}\,\rho = \mathrm{tr}\,\xi .$$

It is known that K-classes $[\rho_K, \rho^K]$ and T-classes $[\rho_T, \rho^T]$ are intervals on Con S ([7],[9]).

Let $\rho \in$ Con S. If $\mathcal{C}$ is a class of semigroups, and $S/\rho \in \mathcal{C}$, then ρ is a $\mathcal{C}$-congruence on S. In the paper, σ and ν denote respectively the least group and the least Clifford congruence on S, and ω denotes the universal congruence $S \times S$ on S. For undefined notations or terminology see [3],[8].

RESULT 1.[5]. For any family $\mathcal{F} \subseteq$ Con S,

$$\Big(\bigvee_{\rho\in\mathcal{F}} \rho\Big)_T = \bigvee_{\rho\in\mathcal{F}} \rho_T, \qquad \Big(\bigcap_{\rho\in\mathcal{F}} \rho\Big)^T = \bigcap_{\rho\in\mathcal{F}} \rho^T.$$

RESULT 2. [4;5]. For any family $\mathcal{F} \subseteq$ Con S,

$$\ker \bigcap_{\rho\in\mathcal{F}} \rho = \bigcap_{\rho\in\mathcal{F}} \ker\rho .$$

This paper is in final form and no version of it will be submitted for publication elsewhere.

A regular semigroup S is E-unitary if, for any $a \in S$ and $e \in E(S)$, $ae \in E(S)$ implies $a \in E(S)$.

RESULT 3. [1]. The following statements for a congruence ρ on S are equivalent

(i) ρ is E-unitary.

(ii) $ae \in \ker\rho \Rightarrow a \in \ker\rho$, $\quad (a \in S,\ e \in E(S))$.

(iii) $\ker\rho = \ker(\rho \vee \sigma)$.

(iv) $\rho^K = \rho \vee \sigma$.

(v) ρ^K is a group congruence.

Let $\mathcal{U}(S)$ denotes the set of all E-unitary congruences on a regular semigroup S.

LEMMA 1. For any family $\mathcal{F} \subseteq \mathrm{Con}\, S$,

$$\mathcal{F} \subseteq \mathcal{U}(S) \Rightarrow \wedge\mathcal{F} \in \mathcal{U}(S).$$

Proof. Let $\mathcal{F} \subseteq \mathcal{U}(S)$, and $a \in S$, $e \in E(S)$. Then

$$\begin{aligned} ae \in \ker \bigwedge_{\rho\in\mathcal{F}} \rho &\Longleftrightarrow (\forall \rho \in \mathcal{F}) ae \in \ker\rho && \text{(by Result 2)} \\ &\Rightarrow (\forall \rho \in \mathcal{F}) a \in \ker\rho && \text{(since } \rho \in \mathcal{U}(S)) \\ &\Longleftrightarrow a \in \ker \bigwedge_{\rho\in\mathcal{F}} \rho\ . && \text{(by Result 2).} \end{aligned}$$

Hence, according to Result 3 $\wedge\mathcal{F}$ is an E-unitary congruence.

Let $\rho \in \mathrm{Con}\, S$. The existence of the least E-unitary congruence $\pi(\rho)$ containing ρ follows from Lemma 1.
Hence, for $\mathcal{F} \subseteq \mathcal{U}(S)$, $\pi(\vee\mathcal{F})$ is the least E-unitary congruence containing $\vee\mathcal{F}$, i.e. the family $\mathcal{F}$ has the join $\pi(\vee\mathcal{F})$ in $\mathcal{U}(S)$. We summarize this observation and Lemma 1 in a theorem as follows.

THEOREM 1. The set $\mathcal{U}(S)$ of all E-unitary congruences on a regular semigroup S ordered by inclusion is a complete lattice, and a complete $\wedge$-subsemilattice of Con S.

Let $\rho \in \mathrm{Con}\, S$. Since $\rho\vee\sigma$ is the least group congruence $\sigma(\rho)$ containing ρ, and $\rho \subseteq \pi(\rho) \subseteq \sigma(\rho) = \rho\vee\sigma$, we obtain $\rho\vee\sigma \subseteq \pi(\rho)\vee\sigma \subseteq \rho\vee\sigma$.

We have therefore established the following.

LEMMA 2. For any $\rho \in \mathrm{Con}\, S$,

$$\rho \vee \sigma = \pi(\rho) \vee \sigma .$$

THEOREM 2. Let S be a regular semigroup. The mapping

$$\phi : \rho \to \rho \vee \sigma \qquad (\rho \in \mathcal{U}(S))$$

is a complete homomorphism of the lattice $\mathcal{U}(S)$ of all E-unitary congruences onto the lattice $[\sigma, \omega]$ of all group congruences on S.
The classes of the complete congruence induced by this homomorphism are K-classes.

Proof. Obviously, ϕ maps $\mathcal{U}(S)$ onto $[\sigma,\omega]$. Let $\mathcal{F}$ be any family of E-unitary congruences on S. Then by Theorem 1 $\pi(\vee\mathcal{F})$ is the join of $\mathcal{F}$ in $\mathcal{U}(S)$. Thus we have

$$(\pi(\bigvee_{\rho\in\mathcal{F}}\rho))\phi = \pi(\bigvee_{\rho\in\mathcal{F}}\rho)\vee\sigma = (\bigvee_{\rho\in\mathcal{F}}\rho)\vee\sigma \qquad \text{(by Lemma 2)}$$

$$\bigvee_{\rho\in\mathcal{F}}(\rho\vee\sigma) = \bigvee_{\rho\in\mathcal{F}}(\rho\phi).$$

Further, since $\wedge\mathcal{F} \in \mathcal{U}(S)$, we obtain

$$\begin{aligned} \ker((\bigwedge_{\rho\in\mathcal{F}}\rho)\vee\sigma) &= \ker \bigwedge_{\rho\in\mathcal{F}}\rho && \text{(by Result 3)} \\ &= \bigcap_{\rho\in\mathcal{F}} \ker\rho && \text{(by Result 2)} \\ &= \bigcap_{\rho\in\mathcal{F}} \ker(\rho\vee\sigma) && \text{(by Result 3)} \\ &= \ker \bigwedge_{\rho\in\mathcal{F}} (\rho\vee\sigma) && \text{(by Result 2)} \end{aligned}$$

On the other hand, $\mathrm{tr}((\bigwedge_{\rho\in\mathcal{F}}\rho)\vee\sigma) = \mathrm{tr}\bigwedge_{\rho\in\mathcal{F}}(\rho\vee\sigma) = \omega_{E(S)}$

so we have $(\bigwedge_{\rho\in\mathcal{F}}\rho)\phi = \bigwedge_{\rho\in\mathcal{F}}(\rho\phi)$.

From Result 3 we have, for any $\rho, \xi \in \mathcal{U}(S)$, $\rho\vee\sigma = \xi\vee\sigma \Leftrightarrow \ker\rho = \ker\xi$. So we have $\rho\phi = \xi\phi \Leftrightarrow \rho^K\xi$.

From this theorem and Result 3 it follows

COROLLARY. Let $\mathcal{F} \subseteq \mathcal{U}(S)$. Then

(i) $(\bigwedge_{\rho\in\mathcal{F}}\rho)^K = \bigwedge_{\rho\in\mathcal{F}}\rho^K$

(ii) $(\pi(\bigvee_{\rho\in\mathcal{F}}\rho))^K = \bigvee_{\rho\in\mathcal{F}}\rho^K$.

A regular semigroup S is called E-reflexive if, for any $a,b \in S$ and $e \in E(S)$, $eab \in E(S)$ implies $eba \in E(S)$.

RESULT 4. [1]. The following statements concerning a congruence ρ on Con S are equivalent

(i) ρ is E-reflexive.

(ii) ρ^K is a Clifford congruence.

(iii) $\ker\rho = \ker(\rho\vee\nu)$.

Let $\mathcal{R}(S)$ denotes the set of all E-reflexive congruences on S. By Lallement's Lemma, for any $\rho \in \mathrm{Con}\, S$ we have $\rho \in \mathcal{R}(S)$ if and only if

$$eab \in \ker\rho \Rightarrow eba \in \ker\rho \qquad (a,b \in S,\ e \in E(S)).$$

Therefore, the proof of the following lemma is similar to the proof of Lemma 1.

LEMMA 3. For any family $\mathcal{F} \subseteq \mathrm{Con}\, S$

$$\mathcal{F} \subseteq \mathcal{R}(S) \Rightarrow \cap\mathcal{F} \in \mathcal{R}(S).$$

Let $\rho \in \mathrm{Con}\, S$. The existence of the least E-reflexive congruence $\lambda(\rho)$ on S containing ρ follows from Lemma 3.

Hence, for $\mathcal{F} \subseteq \mathcal{R}(S)$, $\lambda(\vee\mathcal{F})$ is the least E-reflexive congruence on S containing $\vee\mathcal{F}$, i.e. it is the join of the family $\mathcal{F}$ in $\mathcal{R}(S)$.

So we have the following result for E-reflexive congruences corresponding to the result for E-unitary congruences given in Theorem 1.

THEOREM 3. The set $\mathcal{R}(S)$ of all E-reflexive congruences on a regular semigroup S ordered by inclusion is a complete lattice and a complete $\cap$-subsemilattice of Con S.

Let $\rho \in \mathrm{Con}\, S$. Since $\rho \vee \nu$ is the least Clifford congruence $\nu(\rho)$ containing ρ, and $\lambda(\rho) \subseteq \nu(\rho)$, it follows

LEMMA 4. Let $\rho \in \mathrm{Con}\, S$. Then

$$\rho \vee \nu = \lambda(\rho) \vee \nu.$$

THEOREM 4. Let S be a regular semigroup and

$$\Psi : \rho \to \rho \vee \nu \qquad (\rho \in \mathcal{R}(S)).$$

Then

(i) The mapping Ψ is a complete $\vee$-homomorphism of the lattice $\mathcal{R}(S)$ of all E-reflexive congruences onto the lattice $[\nu, \omega]$ of all Clifford congruences on S.

(ii) $\ker((\bigcap_{\rho\in\mathcal{F}} \rho)\Psi) = \ker \bigcap_{\rho\in\mathcal{F}} (\rho\Psi)$ and

$$(\bigcap_{\rho\in\mathcal{F}} \rho)\Psi \subseteq \bigcap_{\rho\in\mathcal{F}} (\rho\Psi), \qquad (\mathcal{F} \subseteq \mathcal{R}(S)).$$

Moreover, $\rho\Psi = \xi\Psi \Rightarrow \rho K \xi$ $(\rho, \xi \in \mathcal{R}(S))$.

Proof. (i) According to Result 4, any Clifford congruence is E-reflexive. Hence, Ψ maps $\mathcal{R}(S)$ onto the lattice $[\nu, \omega]$ of all Clifford congruences on S. Let $\mathcal{F}$ be any family of E-reflexive congruences on S. Then by Theorem 3 $\lambda(\bigvee_{\rho\in\mathcal{F}} \rho)$ is the join of

$\mathcal{F}$ in $\mathcal{R}(S)$. Thus we have

$$(\lambda(\bigvee_{\rho\in\mathcal{F}} \rho))\Psi = \lambda(\bigvee_{\rho\in\mathcal{F}} \rho) \vee \nu = (\bigvee_{\rho\in\mathcal{F}} \rho) \vee \nu \qquad \text{(by Lemma 4)}$$

$$\bigvee_{\rho\in\mathcal{F}} (\rho \vee \nu) = \bigvee_{\rho\in\mathcal{F}} (\rho\Psi).$$

(ii) Obviously $(\bigcap_{\rho\in\mathcal{F}} \rho) \vee \nu \subseteq \bigcap_{\rho\in\mathcal{F}} (\rho \vee \nu)$, for any $\mathcal{F} \subseteq \mathcal{R}(S)$.

Since $\bigcap_{\rho\in\mathcal{F}} \rho \in \mathcal{R}(S)$, we have

$$\begin{aligned}
\ker((\bigcap_{\rho\in\mathcal{F}} \rho) \vee \nu) &= \ker \bigcap_{\rho\in\mathcal{F}} \rho && \text{(by Result 4)}\\
&= \bigcap_{\rho\in\mathcal{F}} \ker\rho && \text{(by Result 2)}\\
&= \bigcap_{\rho\in\mathcal{F}} \ker(\rho \vee \nu) && \text{(by Result 4)}\\
&= \ker \bigcap_{\rho\in\mathcal{F}} (\rho \vee \nu) && \text{(by Result 2).}
\end{aligned}$$

From Result 4 we have, for any $\rho, \xi \in \mathcal{R}(S)$,

$$\rho \vee \nu = \xi \vee \nu \Rightarrow \ker(\rho \vee \nu) = \ker(\xi \vee \nu) \Leftrightarrow \ker\rho = \ker\xi .$$

Therefore, $\rho\Psi = \xi\Psi \Rightarrow \rho K \xi$.

Let $\mathcal{BG}(S)\left[\mathcal{SG}(S)\right]$ denotes the lattice of all band [semilattice] of groups congruences on S. Clearly, $\mathcal{SG}(S) = [\nu, \omega]$.

Using Result 1 and the equivalences[1] :

$$\rho \in \mathcal{BG}(S) \Leftrightarrow \rho^T = \rho \vee \beta \qquad \text{and}$$

$$\rho \in \mathcal{SG}(S) \Leftrightarrow \rho^T = \rho \vee \eta ,$$

where $\beta[\eta]$ is the least band [semilattice] congruence on S we have the following analogue of Theorem 2.

THEOREM 5. Let S be a regular semigroup. Then

(i) The mapping

$$F_\beta : \rho \to \rho \vee \beta \qquad (\rho \in \mathcal{BG}(S))$$

is a complete homomorphism of the lattice $\mathcal{BG}(S)$ onto the lattice $[\beta, \omega]$ of all band congruences on S.

(ii) The mapping

$$F_\eta : \rho \to \rho \vee \eta \qquad (\rho \in \mathcal{PG}(S))$$

is a complete homomorphism of the lattice $\mathcal{PG}(S)$ onto the lattice $[\eta, \omega]$ of all semilattice congruences on S.

The classes of the complete congruences induced by these homomorphisms are T-classes.

For a band of groups, the same result was proved in [6] (Corollary, 8.12).

REFERENCES

1. B.P.Alimpić, D.N.Krgović, Some congruences on regular semigroups, to appear.
2. R.Feigenbaum, Regular semigroup congruences, Semigroup Forum 17(1979), 373-377.
3. J.M.Howie, An Introduction to Semigroup Theory, Academic Press, London 1976.
4. P.R.Jones, Joins and meets of congruences on a regular semigroup, Semigroup Forum, vol 30(1984), 1-16.
5. F.Pastijn and M.Petrich, Congruences on regular semigroups, Trans.Amer.Math. Soc. Vol. 295 No 2, (1986), 607-633.
6. F.Pastijn and M.Petrich, The congruence lattice of a regular semigroup, Preprint.
7. F.Pastijn and P.G.Trotter, Lattices of completely regular semigroup varieties, Pac.J.Math.Vol. 119, No 1(1985), 191-214.
8. M.Petrich, Inverse semigroups, Wiley, New York, 1984.
9. N.R.Reilly and K.E.Scheiblich, Congruences on regular semigroups, Pac.J.Math.Vol. 23, No 2(1967), 349-360.

Branka P. Alimpić
Prirodno matematički fakultet
Studentski trg 16/IV
11000 Beograd

Dragica N. Krgović
Matematički institut
Knez Mihajlova 35/I
11000 Beograd

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

SEMIGROUPS WHOSE PROPER SUBSEMIGROUPS ARE (RIGHT-) t - ARCHIMEDEAN

Stojan Bogdanović and Todor Malinović

Abstract. In [1] S. Bogdanović characterized semigroups whose left ideals are left archimedean semigroups. B. Pondeliček in [7] described semigroups whose proper one-sided ideals are t-archimedean semigroups. Semigroups with an idempotent in which every subsemigroup is a t-archimedean semigroup are studied by A.C. Spolentini and A. Varisco, [2].

In this paper we generalize their results to arbitrary semigroups. Moreover, we characterize semigroups in which every proper subsemigroup is right archimedean.

Troughout this paper let Z^+ denote the set of all positive integers.

A semigroup S is archimedean if for any $a,b \in S$ there exists $n \in Z^+$ for which $a^n \in SbS$, [6]. S is right archimedean if for every $a,b \in S$ there exixtx $n \in Z^+$ such that $a^n \in bS$, [8]. S is t-archimedean if for every $a,b \in S$ there exists $n \in Z^+$ for which $a^n \in bS \cap Sb$, [8].

Undefined notions and terminology are as in [3] and [6].

This paper is in final form and no version of it will be submitted for publication elsewhere.

From [1], we state the following

THEOREM 1. Every proper right ideal of a semigroup S is a right archimedean subsemigroup of S if and only if one of the following conditions holds:

1^o S is right archimedean;

2^o S contains exactly two right ideals R_1 and R_2 which are right simple semigroup and $S=R_1 \cup R_2$;

3^o S has a maximal right ideal M which is right archimedean and $M \subseteq aM$ for every $a \in S \setminus M$.

We also use the following results

THEOREM 2. [5, 4] Let M be a proper right ideal of a semigroup S. Then M is a unique maximal ideal if and only if one of the following conditions holds:

(i) $S \setminus M = \{a\}$, $a^2 \cup aM = M$

(ii) $S \setminus M = \{a \in S \mid aS = S\}$ if and only if $S \setminus M = P \cup K$, where $P = \{a \in S \setminus M \mid aM = M\}$ is a right simple semigroup of S and $K = \{a \in S \setminus M \mid aM = S\}$ is a two-sided ideal of a semigroup $S \setminus M$.

COROLLARY 1. [4] Let S be a partially right simple semigroup and M be unique maximal right ideal of S. Then M is a two-sided ideal if and only if $S \setminus M$ is a right simple subsemigroup of S.

DEFINITION 1. A semigroup S is R-semigroup if for any $a,b \in S$ there exists $n \in Z^+$ such that $a^n \in b \cdot \langle a,b \rangle$.

L-semigroup is defined dually.

Remark 1. It is easy to verify that a semigrup S is an R-semigroup if and only if every subsemigroup of S is right archimedean.

THEOREM 3. Every proper subsemigroup of a semigroup S is a right archimedean subsemigroup of S if and only if one of the following conditions holds:

(i) S is an R-semigroup;

(ii) S contains exactly two right ideals R_1 and R_2 which are right simple R-semigroups, $S=R_1 \cup R_2$ and $S = \langle a,b \rangle$ for every $a \in R_1$, $b \in R_2$;

(iii) S has a (maximal) two-sided ideal M which is an R-semigroup, $S \setminus M$ is a right simple R-semigroup and $S = \langle a,b \rangle$ for every $a \in M$, $b \in S \setminus M$.

Proof. Suppose that S is not right simple. If every proper subsemigroup of S is right archimedean, then every proper right ideal of S is right archimedean. Hence, by Theorem 1, we have one of the cases 1^o, 2^o or 3^o of this theorem. If 1^o holds, then every subsemigroup of S is right archimedean so S is an R-semigroup. Suppose that 2^o holds. Then S contains exactly two right ideals R_1 and R_2 which are right simple. Hence, every subsemigroup of R_1 and R_2 is right archimedean, and thus R_1 and R_2 are R-semigroups. Let $a \in R_1$ and $b \in R_2$ be arbitrary elements. Then $S = \langle a,b \rangle$. Indeed, if $\langle a,b \rangle \neq S$, then $\langle a,b \rangle$ is a right archimedean semigroup and so

$$(\exists x \in \langle a,b \rangle)(\exists n \in Z^+)(a^n = bx).$$

From this we have that $a^n \in R_2$, which is not possible. If 3^o holds, then M is a unique maximal right ideal of S, and by Theorem 2, we have that $S \setminus M = \{a\}$, $a^2 \cup aM = M$ or $S \setminus M = \{a \in S \mid aS = S\}$. If $S \setminus M = \{a\}$, $a^2 \cup aM = M$, then S is right archimedean. From this we have that S is an R-semigroup. Assume that $S \setminus M = \{a \in S \mid aS = S\}$. Then, by Theorem 2, we have

$$S \setminus M = P \cup K,$$

where $P = \{a \in S \setminus M \mid aM = M\}$ is a right simple semigroup of S and $K = \{a \in S \setminus M \mid aM = S\}$. But, in this case $K = \emptyset$. Indeed, if $K \neq \emptyset$, then there exists an element $a \in K$ such that

$$ax = a \wedge ay = x$$

for some $x,y \in M$. Since M is right archimedean and $y, xa \in M$ we have that

$$(\exists m \in Z^+)((xay)^m \in yM)$$

which implies $x^{2m} = yu$ for some $u \in M$. Thus, we have

$$a = ax = ax^{2m} = ayu = xy \in M,$$

which is not possible. Hence, $S \setminus M$ is a right simple R-semigroup and M is a unique maximal two-sided ideal (Corollary 1) which is an R-semigroup.

Let $a \in M$ and $b \in S \setminus M$ be arbitrary elements and let $\langle a,b \rangle \neq S$. Then $\langle a,b \rangle$ is right archimedean and thus

$$(\exists n \in Z^+)(\exists x \in \langle a,b \rangle)(b^n = ax).$$

From this we have that $b^n \in M$, which is not possible.

Now, let S be right simple. Then every subsemigroup of S is right archimedean and thus S is an R-semigroup (Remark 1).

The converse follows immediately.

THEOREM 4. Every proper subsemigroup of a semigroup S is a right archimedean with idempotents if and only if one of the following conditions holds:

1° S is a periodic R-semigroup;

2° S is a band and $|S| = 2$.

Proof. Let every proper subsemigroup of S is a right archimedean with idempotents. Then, by Theorem 3, we have one of the cases (i), (ii) or (iii) of this theorem. If (i) holds, then $\langle a \rangle$ is right archimedean with idempotents for any $a \in S$ and thus

$$(\exists e \in E(S))(\exists n \in Z^+)(a^n = e).$$

From this we have that element a is of finite order. Hence, S is a periodic R-semigroup. But, the cases (ii) and (iii) are possible only if S is a band and $|S| = 2$. Indeed, let $S = R_1 \cup R_2$ where R_1 and R_2 are the disjoint right

ideals of S which are right simple R-semigroups and $S = \langle a,b \rangle$ for arbitrary elements $a \in R_1$, $b \in R_2$. If e and f are the idempotents of R_1 and R_2, respectively, then $S = \langle e,f \rangle$. Furthermore, $ef \in R_1$, $fe \in R_2$ and there exists $m,n \in Z^+$ such that

$$e = (ef)^n \wedge f = (fe)^m$$

since R_1 and R_2 are the R-semigroups. From this we have

$$ef = e \wedge fe = f.$$

Hence,

$$\langle e,f \rangle = \{e,f\}$$

and thus S is a band and $|S| = 2$. Let (iii) holds and let e and f are the idempotents of M and $S \setminus M$, respectively. Then

$$ef,\ fe \in M$$

and

$$(\exists m,n \in Z^+)(e = (ef)^n \wedge e = (fe)^m),$$

since M is an R-semigroup. From this we have

$$ef = e \wedge fe = e.$$

Hence,

$$\langle e,f \rangle = \{e,f\}$$

ant thus S is a band and $|S| = 2$.

The converse follows immediately.

From [1] we state the following.

LEMMA 1. S is a right simple t-archimedean semigroup if and only if S is a group.

DEFINITION 2. A semigroup S is T-semigroup if for any $a,b \in S$ there exists $n \in Z^+$ such that $a^n \in b \cdot \langle a,b \rangle \cdot b$.

Remark 2. It is clear that a semigroup S is T-semigroup if and only if every subsemigroup of S is t-archimedean.

THEOREM 5. Every proper subsemigroup of S is t-archimedean if and only if one of the following conditions holds:

1° S is a T-semigroup;

2° S is a band and $|S|=2$

Proof. Suppose that S is not right simple and let every proper subsemigroup of S be t-archimedean. Then, by Theorem 3, we have one of the cases (i), (ii) or (iii) of this theorem. If (i) holds, then S is right archimedean (Remark 1). Let $R(S)$ denote the union of all proper right ideals of S. If $R(S)\neq S$, then $R(S)=M$ is a unique maximal right ideal of S and it is a t-archimedean semigroup. By Theorem 2, we have that $S\setminus M=\{a\in S \mid aS=S\}$ or $S\setminus M=\{a\}$, $a^2\cup aM=M$. If $S\setminus M=\{a\in S \mid aS=S\}$, then $S\setminus M$ is a subsemigroup of S and we have that

$$(\exists n\in Z^{+})(a^{n}\in bS\subseteq M)$$

for any $a\in S\setminus M$, $b\in M$, since S is right archimedean, which is not possible. If $S\setminus M=\{a\}$, $a^2\cup aM=M$, then S is t-archimedean and thus S is a T-semigroup (Remark 2). Now, assume that $R(S)=S$. In this case we can prove that S is of the type 1°. But, the cases (ii) and (iii) are possible only if S is a band and $|S|=2$. Indeed, let $S=R_1\cup R_2$, where R_1 and R_2 are disjoint right ideals of S which are right simple R-semigroups and $S=\langle a,b\rangle$ for arbitrary elements $a\in R_1$, $b\in R_2$. Then, by Lemma 1, we have that R_1 and R_2 are groups. If e and f are the identities of R_1 and R_2, respectively, then

$$S=\langle a,f\rangle. \tag{1}$$

Furthermore,

$$ef\in R_1 \wedge fe\in R_2$$

and

$$(ef)^2=(efe)f=(ef)f=ef.$$

Since R_1 is a group, it follows that

$$ef=e. \tag{2}$$

Similarly

$$fe=f \tag{3}$$

From (1), (2) and (3) we have

$$S=\{e,f\}$$

and thus S is a band and $|S|=2$. If (iii) holds, then I is

a two-sided ideal of S and $S\setminus I$ is a right simple semigroup. Furthermore, $S\setminus I$ is t-archimedean and by Lemma 1, we have that $S\setminus I$ is a group. Let x be an arbitrary element of I and let e be the identity of $S\setminus I$. Then,

$$ex,\ xe,\ x^{k}e\in I \tag{4}$$

for any $k\in Z^{+}$ and thus

$$S=\langle e,ex\rangle=\langle e,xe\rangle. \tag{5}$$

From this we have that $x=ey$ for some $y\in S$ so that

$$ex=e(ey)=ey=x \tag{6}$$

and thus

$$(xe)^{k}=(xe)(xe)\ldots(xe)=x(ex)\ldots(ex)e=x^{k}e. \tag{7}$$

By (5), (6) and (7), it follows that

$$S=\{e,\ xe,\ x^{2}e,\ldots\}$$

and thus

$$A=\{e,\ x^{2}e,\ x^{3}e,\ldots\}$$

is a subsemigroup of S. Since A is t-archimedean we have

$$e\in x^{k}eA\subseteq I$$

which is not possible. Hence,

$$S=\{e,\ x^{2}e,\ x^{3}e,\ldots\}=\{x^{2}e,\ x^{3}e,\ldots\}\cup\{e\}$$

and thus

$$M=\{x^{2}e,\ x^{3}e,\ldots\} \tag{8}$$

By (4), (7) and (8) it follows that

$$xe=x^{k}e=(xe)^{k}$$

for some $k>1$ and thus M is a group. For the identity $(xe)^{k-1}=x^{k-1}e$ of this group we have

$$S=\{(xe)^{k-1},\ e\}=\{x^{k-1}e,e\}$$

and thus S is a band and $|S|=2$.

Now, let S be right simple. Then we have two cases:
(a) S is left simple. In this case S is a T-semigroup.
(b) If S is not left simple, then using the dual of Theorem 3, we have, as in the case when S is not right simple, that S is T-semigroup or S is a band and $|S|=2$.

The converse follows immediately.

R E F E R E N C E S

[1] S. Bogdanović, Semigroups with a system of subsemigroups, Inst. of Math., Novi Sad, 1985.

[2] A. Cherubini Spolentini and A. Varisko, Sui Semigruppi i cui sottosemigruppi propri sono t-archimedei, Inst. Lombardo, 112 (1978), 91-98.

[3] A.H. Clifford and G.B. Preston, The algebraic theory of semigroups I, Amer. Math. Soc., 1961.

[4] T. Malinović, Semigrups whose subsemigroups are partially simple, Proc. of the conf. "Algebra and logic", Zagreb, 1984, 95-103.

[5] T. Malinović. Partially simple semigroups, Matematički Vesnik, 37 (1985), 196-204.

[6] M. Petrich, Introduction to semigroups, Merrill, Ohio, 1973.

[7] B . Pondeličček, Semigroups whose proper one-sided ideals are t-archimedean, Mat. Vesnik 37(3), 1985, 315-321..

[8] M.S. Putsha, Band of t-archimedean semigroup, Semigroup Forum 6(1973), 232-239.

Stojan Bogdanović
26000 - Pančevo
Moše Pijade 114
Yugoslavia

Todor Malinović
17500 - Vranje,
Lenjinova 4/16
Yugoslavia

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

VECTOR VALUED ASSOCIATIVES

N. Celakoski, B. Janeva

Abstract. In this paper the notion of vector valued associative is introduced (as a generalization of the notion of associative [1] as well as of the notion of vector valued semigroup [3]). Some examples of such associatives are given, and an attempt is made to carry over some results already obtained for other vector valued structures. It is shown also that the class of vector valued subassociatives of vector valued semigroups is, in general, a proper subclass of the class of vector valued associatives.

1. DEFINITION OF (F,δ,m)-ASSOCIATIVE

Let F be a (nonepmty) set and $\delta: f \to \delta(f)$, $\rho: f \to \rho(f)$ be two mappings from F into the set of positive integers. If A is a nonempty set and $\xi: f \to \overline{f}$ is a mapping from F into the set $\overline{F}$ of vector valued operations such that

$$\overline{f}: A^{\delta(f)} \to A^{\rho(f)},$$

then a vector valued algebra $(A;\overline{F})$ is built up. We call $(A;\overline{F})=\underline{A}$ an (F,δ,ρ)-algebra. Further on we will write F instead of $\overline{F}$ and f instead of $\overline{f}$. The integers $\delta(f)$ and $\rho(f)$ are called the length and the dimension of f respectively.

We will consider in this paper a class of vector valued algebras which satisfy the condition

$$(\forall f \in F) \quad \delta(f) > m, \tag{1.1}$$

This paper is in final form and no version of it will be submitted for publication elsewhere.

where $m=\rho(f) \geq 2$ is fixed. The elements of F will be called primary operations of $\underline{A}$; the identity operation will be denoted by 1. (Note that $1 \notin F$).

First we will define polynomial operations (on A) inductively in the following way:

(i) 1 and every $f \in F$ are polynomial operations

(ii) if $g, g_1, \ldots, g_p$ are polynomial operations such that $\delta(g)=\rho(g_1)+\ldots+\rho(g_p)$ [1], then the operation $h=g(g_1 \times \cdots \times g_p)$ is a polynomial operation.

(Here: $h(\underline{x})=g(g_1(\underline{x}_1)g_2(\underline{x}_2)\ldots g_p(\underline{x}_p))$, where $x=\underline{x}_1\ldots\underline{x}_p$ and the length $|\underline{x}_\nu|$ of the string $\underline{x}_\nu$ is $|\underline{x}_\nu|=\delta(g_\nu)$.)

Clearly, $\delta(h)=\delta(g_1)+\ldots+\delta(g_p)$ and $\rho(h)=\rho(g)$.

The set of all polynomial operations of $\underline{A}$ will be denoted by $P_F(A)=P_F$. Obviously,

$$(\forall h \in P_F)\ h \neq 1 \Longrightarrow \rho(h) = m. \tag{1.2}$$

According to (1.1), $\delta(f)-m > 0$ for every $f \in F$. The positive integer

$$i(f) = \delta(f)-m \tag{1.3}$$

will be called the index of the operation f. The index of the identity operation is 0. We denote by P' the set $P_F \setminus \{1\}$ (of non-identity polynomial operations belonging to P_F).

PROPOSITION 1.1. *The set $i(P')$ of the indexes of the non-identity polynomial operations coincides with the semigroup generated by the set $i(F)=J$ of indexes of the primary operations, i.e.*

$$i(P') = \langle i(F) \rangle = \langle J \rangle.$$

[1] $\rho(g)$ will denote the dimension, and $\delta(g)$ the length of the polynomial operation g.

Proof. Let $h \in P'$, and $h=gf$, where $g \in P'$, $f \in P_F$. Since $\delta(h)=\delta(f)$, $\rho(f)=\delta(g)$ and $\rho(h)=\rho(g)$, it follows that

$$i(h) = \delta(h)-\rho(h) = \delta(f)-\rho(f)+\rho(f)-\rho(g) = i(f)+i(g).$$

If $h=g \times f$ where

$$(g \times f)(x_1^{\delta(g)}, y_1^{\delta(g)}) = (g(x_1^{\delta(g)}), f(y_1^{\delta(f)}))$$

then $i(h) = i(g) + i(f)$.

Inductively, if $h=g(g_1 \times \ldots \times g_p)$, where $g \in P'$, $g_1, \ldots, g_p \in P_F$, then

$$i(h) = i(g) + i(g_1)+\ldots+i(g_p). \tag{1.4}$$

We can assume that $i(g) \in \langle J \rangle$ and that either $i(g_\nu)=0$ or $i(g_\nu) \in \langle J \rangle$. This implies that $i(h) \in \langle J \rangle$, i.e. $i(P') \subseteq \langle J \rangle$.

Conversely, let $k \in \langle J \rangle$ and $k \notin J$. Then there exist $i_1, \ldots, i_r \in J$, such that $k=i_1+\ldots+i_r$. Put $h=f_1(f_2 \times 1^{i_1})\ldots(f_r \times 1^{i_1+\ldots+i_{r-1}})$ where $i(f_j)=i_j$. Then $i(h) = k$, i.e. $\langle J \rangle \subseteq i(P')$. □

Now we are ready to introduce the concept of vector valued associative.

An (F,δ,m)-algebra $(A;F)$ is called an (F,δ,m)-associative iff any two polynomial operations of $\underline{A}$ with the same length are equal, i.e.

$$(g,h \in P_F \ \&\ \delta(g) = \delta(h)) \Longrightarrow g = h. \tag{1.5}$$

Using the notation $J=i(F)$ and the fact that the dimension of the operations is fixed, an (F,δ,m)-associative $(A;F)$ will be called an m-dimensional J-associative, or shortly, a (J,m)-associative, and it will be denoted by $(A;J)$.

Further on we will often write $[x_1^{\delta(g)}]$ or $[x_1^{k+m}]$ instead of $g(x_1^{\delta(g)})$, where g is a fixed polynomial operation, $k=i(g)$, and $[x]=x$ for the identity operation.

From the definition of the notion of a (J,m)-associative we obtain the following

PROPOSITION 1.2. If (A;J) is a (J,m)-associative, then for every k∈J, (A;[ ]) is an (m+k,m)-semigroup ([3]). □

(We say that this (m+k,m)-semigroup is induced by the given (J,m)-associative.)

2. EXAMPLES OF (J,m)-ASSOCIATIVES

We will consider two examples of (J,m)-associatives.

Example 1. Let (A;[ ]) be an (m+d,m)-semigroup and let $d \mid i(f)$ for every f∈F, where F is the set of all (m+sd,m)-operations obtained from [ ] by the general associative law ([3]). Define

$$(\forall f \in F) \quad f(a_1^{\delta(f)}) = [a_1^{\delta(f)}].$$

Then (A;[ ]) becomes an (F;δ,m)-associative.

Example 2. Let A={a,b,c}, a≠b≠c≠a and J be a set of positive integers such that d=GCD(J)∉J. Denote by p the least element of J. Then the set L=J\{αp | α ≥ 1} is nonempty and let q be the least element of L.

Define a set F={f_k | k∈J} of vector valued operations on A in the following way:

$$(\forall k \in J) \quad \delta(f_k) = m+k, \quad \rho(f_k) = m \text{ and}$$

$$f_k(x_1^{m+k}) = \begin{cases} (b^m) & \text{if } k=q, \ (x_1^{m+k}) = (c^{m+q}) \\ (a^m) & \text{otherwise.} \end{cases}$$

We are going to show that (A;F) is a (J,m)-associative.

Namely, let h∈P' be a polynomial operation with a positive index k∈J. Then the following implication holds:

$$h \neq f_q \text{ or } \underline{x} \neq (c^{m+q}) \Longrightarrow h(\underline{x}) = (a^m). \qquad (2.1)$$

We will show (2.1) by induction of the construction of polynomial operations.

If h∈F, then (2.1) is satisfied by the definition of F.

Assume that $h=g(g_1 \times \ldots \times g_r)$. Then g≠1 and put

$k=i(h) = i(g) + i(g_1)+\ldots+i(g_r)$. Therefore

$$k = q \Longleftrightarrow g = f_q, \quad g_1=\ldots=g_r=1. \qquad (2.2)$$

Namely it is clear that the implication ⟸ is true. Let k=q. Then $i(g) \leq q$, $i(g_\nu) \leq q$ and $i(g) \neq 0$, which implies that $i(g)=q$, $i(g_\nu)=0$.

Let $g \neq f_q$ or $g_\lambda \neq 1$ for some λ. In the first case we have $h(\underline{x})=g(\underline{y})=(a^m)$. In the second case, i.e. if $g=f_q$ and $g_\lambda \neq 1$ for some λ, we have $h(\underline{x})=g(\underline{y})$, where $\underline{y} \neq (c^{m+q})$, and therefore $g(\underline{y})=(a^m)$.

Clearly, (2.1) implies that (A;F) is a (J,m)-associative.

3. (K,m)-SUBASSOCIATIVES OF (m+d,m)-SEMIGROUPS

Let (A;J) be a (J,m)-associative and J⊆L⊆<J>. Then, for every ℓ∈L, by the given (J,m)-associative (A;J), an (ℓ+m,m)-operation is induced such that (A;L) is an (L,m)-associative. Note that (A;L) is not essentially different from (A;J). Therefore, further on, we will consider only (K,m)-associatives where K is a subsemigroup of the additive semigroup of positive integers.

In this case, if M⊆K, then a given (K,m)-associative (A;K) induces a corresponding (M,m)-associative wich is called an M-restriction of (A;K). Specially, if k∈K, then we have (m+k,m)-semigroup (A;[[ ]]) induced by the (K,m)-associative (A;K).

We note that an (m+k,m)-semigroup is in fact a (<k>,m)-associative.

A (K,m)-associative (A;[[ ]]) is a (K,m)-subassociative of an (m+d,m)-semigroup (Q;[ ]) iff $d \mid GCD(K)$, A⊆Q and

$$(\forall a_1^{k+m} \in A^{k+m}) \quad [[a_1^{k+m}]] = [a_1^{k+m}]. \qquad (3.1)$$

PROPOSITION 3.1. A (K,m)-associative (A;[[ ]]) is a (K,m)-subassociative of an (m+d,m)-semigroup iff (A;[[ ]]) is a (K,m)-subassociative of an (m+1,m)-semigroup.

Proof. If $(A;[\![\ ]\!])$ is a (K,m)-subassociative of a $(d+m,m)$-semigroup $(Q;[\ ]')$, then $(Q;[\ ]')$ is a $(d+m,m)$-subsemigroup of an $(m+1,m)$-semigroup $(P;[\ ])$ ([4]). Thus, $(A;[\![\ ]\!])$ is a (K,m)-subassociative of a an $(m+1,m)$-semigroup $(P;[\ ])$.

Conversely, if $(A;[\![\ ]\!])$ is a (K,m)-subassociative of an $(m+1,m)$-semigroup $(Q;[\ ]')$, then the operation $[\ ]$ defined by

$$(\forall x_\nu \in Q)\ [x_1^{d+m}] = [x_1^{d+m}]',$$

is the $(m+d,m)$-operation induced by $[\ ]'$ on Q, and $(A;[\![\ ]\!])$ is a (K,m)-subassociative of an $(m+d,m)$-subsemigroup $(Q;[\ ])$.

PROPOSITION 3.2. A (K,m)-associative is a (K,m)-subassociative of an $(m+1,m)$-semigroup iff $d=GCD(K)\in K$.

Proof. If $d\in K$, then the (K,m)-associative $(A;[\![\ ]\!])$ is a (K,m)-subassociative of an $(m+d,m)$-semigroup $(A;[\ ])$ induced by the (K,m)-associative $(A;[\![\ ]\!])$.

Conversely, we will show that if $d\notin K$, then the (K,m)-associative $(A;F)$ of Example 2 is not a (K,m)-subassociative of an $(m+d,m)$-semigroup.

Suppose that there exists an $(m+d,m)$-semigroup $(P;[\ ])$, such that $A\subseteq P$ and

$$(\forall x_\nu \in A)(\forall k\in K) f_k(x_1^{k+m}) = [x_1^{k+m}].$$

Let q be as in Example 2 and $q=tp+r$, where $d|r$ and $r>0$. Then

$$\begin{aligned}(b^m) &= f_q(c^{q+m}) = [c^{tp+r+m}] = [[c^{tp+m}]c^r] = \\ &= [a^m c^r] = [f_{tp}(a^{tp+m})c^r] = [[a^{tp+m}]c^r] = \\ &= f_q(a^{tp+m}c^r) = (a^m)\end{aligned}$$

which contradicts the fact that $b\neq a$.

Thus, $(A;F)$ is not a (K,m)-subassociative of an $(m+d,m)$-semigroup, and, by Proposition 3.1, $(A;F)$ is not a (K,m)-subassociative of an $(m+1,m)$-semigroup as well. □

COROLLARY 3.3. If $d\notin GCD(K)$, then the class of (K,m)-subassociatives of semigroups is a proper subclass of the class of (K,m)-associatives. □

It is desirable to have an axiom system for the class of (K,m)-subassociatives of $(m+1,m)$-semigroups. Such a system is described in [2] when $m=1$, but we do not know a convenient axiom system of (K,m)-subassociatives of $(m+1,m)$-semigroups in the case $m\geq 2$.

We can only state the following proposition, which does not give enough informations for this class of algebras.

PROPOSITION 3.4. Let $(Q;[\![\ ]\!])$ be a (K,m)-associative and let $(P;[\ ])$ be the free $(m+1,m)$-semigroup with a base Q. Denote by $\approx$ the minimal congruence on P, such that

$$[\![a_1^{m+k}]\!] = (b_1^m) \text{ in } (Q;[\![\ ]\!]) \Longrightarrow [a_1^{m+k}] \approx (b_1^m)$$

Then $(Q;[\![\ ]\!])$ is a (K,m)-subassociative of an $(m+1,m)$-semigroup iff the following statement is satisfied

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

(Above, $(x_1^m)\approx(y_1^m)$ means $x_\nu \approx y_\nu$ for every $\nu\in\{1,2,\ldots,m\}$).

We note that a satisfactory description of free vector valued semigroups is given in [5].

R E F E R E N C E S

[1] Ѓ.Чупона: За асоцијативите, *Contributions, I 1-Sect. nat Sc. and Math., Maced. Acad. Sc. and Arts, (1969), 11-20*

[2] *N.Celakoski: On semigroup associatives, Maced. Acad. Sc. and Arts, Contributions IX 2-Sect. nat. Sc. and Math., (1977), 5-19*

[3] *G.Čupona: Vector valued semigroups, Semigroup Forum, Vol. 26 (1983), 65-74*

[4] *G.Čupona, S.Markovski, B.Janeva: Post theorem for vector valued semigroups, This volume*

[5] *D.Dimovski: Free vector valued semigroups, This volume*

N.Celakoski, Mašinski fakultet, Skopje

B.Janeva, Prirodno-matematički fakultet, Skopje

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

C - (m,n) - I D E A L S E M I G R O U P S

Ć i r i ć M i r o s l a v

ABSTRACT: In this paper we consider semigroups in which every cyclic subsemigroup is an (m,n)-ideal.

INTRODUCTION: The generalization of the ideal of semigroups are given by S. Lajos, by a notion of an (m,n)-ideal of a semigroup [4]. P. Protić and S. Bogdanović considered (m,n)-ideal semigroups in which every subsemigroup is an (m,n)-ideal [5]. This class of semigroups are described by P. Protić and S. Bogdanović [5,6]. Bi-ideal semigroups, as a special case of (m,n)-ideal semigroups, are described by B. Trpenovski [7], S. Bogdanović, P. Kržovski, B. Trpenovski and P. Protić [8]. The construction of the (m,n)-ideal semigroup is given by S. Bogdanović and S. Milić [9].

Here, we consider c-(m,n)-ideal semigroups in which every cyclic subsemigroup is an (m,n)-ideal. In Theorem 1.5. c-(m,n)-ideal semigroups are described by an ideal extension. In Theorem 4.1. we have a construction of a c-(m,n)-ideal semigroup, where results of Theorem 1.1. [10] are used (see also the book of S. Bogdanović [1], Chapter VIII).

1. C-(m,n)-IDEAL SEMIGROUPS

A subsemigroup A of á semigroup S is an (m,n)-ideal of S if $A^mSA^n \subseteq A$, where $m,n \in N \cup \{0\}$ ($A^oS=SA^o=S$) [4].

This paper is in final form and no version of it will be submitted for publication elsewhere.

S is an (m,n)-ideal semigroup if every subsemigroup of S is an (m,n)-ideal of S [5]. Every (1,1)-ideal semigroup we call bi-ideal semigroup.

S is a c-(m,n)-ideal semigroup if every cyclic subsemigroup of S is an (m,n)-ideal of S. It is clear that the class of all (m,n)-ideal semigroups is a subclass of the class of all c-(m,n)-ideal semigroups.

The (m,n)-ideal of S generated by nonempty subset C of S is $[C]_{m,n}= C\cup C^2\cup\ldots\cup C^{m+n}\cup C^mSC^n$. If C={a} we obtain the principal (m,n)-ideal of S generated by element a which is $[a]_{m,n}= a\cup a^2\cup\ldots\cup a^{m+n}\cup a^mSa^n$.

A subset R of a partial semigroup Q is a partial subsemigroup of Q if for x,y∈R, xy∈Q implies xy∈R. A partial subsemigroup R of a partial semigroup Q is an (m,n)-ideal of Q if $R^mQR^n\subseteq Q$ implies $R^mQR^n\subseteq R$. Q is an (m,n)-ideal partial semigroup if every partial subsemigroup of Q is an (m,n)-ideal of Q [5]. Q is a c-(m,n)-ideal partial semigroup if every partial cyclic subsemigroup of Q is an (m,n)-ideal of Q.

Let S be a semigroup with zero O, then S is a nil-semigroup if for every a∈S there exists k∈N such that $a^k=O$ [8]. A partial semigroup Q is a partial nil-semigroup if for every a∈Q there exists k∈N such that $a^k\notin Q$ (In [6] it is called the power breaking partial semigroup).

THEOREM 1.1. The folloving conditions on a semigroup S are equivalent:

(i) S is c-(m,n)-ideal

(ii) (∀a∈S) $a^mSa^n\subseteq\langle a\rangle$

(iii) (∀a∈S) $[a]_{m,n}=\langle a\rangle$

Proof: Let a∈S and let S be a c-(m,n)-ideal semigroup. Then $a^mSa^n\subseteq\langle a\rangle^mS\langle a\rangle^n\subseteq\langle a\rangle$. Conversely, let (ii) holds and let ⟨a⟩ be a cyclic subsemigroup of S. Since $\langle a\rangle^m=\{a^p: p\geq m\}$, then every element from $\langle a\rangle^mS\langle a\rangle^n$ is of the form a^psa^q where p≥m and q≥n, whence $a^psa^q=a^{p-m}a^msa^na^{q-n}\in\langle a\rangle\langle a\rangle\langle a\rangle\subseteq\langle a\rangle$. Thus (i)⇔(ii).

(ii)⇒(iii). Then $[a]_{m,n}= a\cup a^2\cup\ldots\cup a^{m+n}\cup a^mSa^n\subseteq\langle a\rangle\cup\langle a\rangle\cup\ldots\cup\langle a\rangle=\langle a\rangle$. Conversely, $a^mSa^n\subseteq[a]_{m,n}=\langle a\rangle$ i.e. (ii)⇔(iii).□

THEOREM 1.2. Let S be a c-(m,n)-ideal semigroup. Then:

(i) S is periodic

(ii) the set E of all idempotents of S is a rectangular band and it is an ideal of S

(iii) S\E is a c-(m,n)-ideal partial nil-semigroup

(iv) (∀a∈S) $|\langle a\rangle|\leq 2m+2n+1$

(v) S is a disjoint union of the maximal unipotent c-(m,n)-ideal semigroups $S_e=\{x\in S: (\exists p\in N)\ x^p=e\}$, e∈E and e is a zero in S_e

(vi) (∀a,b∈S) $e_ae_b\in\langle a^mb^n\rangle$, where e_a and e_b are the idempotents from ⟨a⟩ and ⟨b⟩.

Proof:

(i) Let a∈S. Let ⟨a⟩ be an infinite semigroup. Then $B=\langle a^2\rangle=\{a^{2k}:k\in N\}$ is a subsemigroup of S and $a^{2m}aa^{2n}\in B^mSB^n\subseteq B$ which is impossible. Hence, for every a∈S, ⟨a⟩ is a finite semigroup and so E≠∅.

(ii) For e∈E we have that $eSe\subseteq\langle e\rangle=\{e\}$, whence for every x∈S is exe=e and by Proposition 3.2. [3] E is a rectangular band. Also, for every e∈S and every x∈S from exe=e we have that ex=exex and xe=xexe whence ex and xe are elements from E and E is an ideal of S.

(iii) From (i), for every a∈S\E the cyclic subsemigroup ⟨a⟩ contains an idempotent and S\E is a partial nil-semigroup. Let A be a cyclic partial subsemigroup of S\E generated by element a∈S\E. Then $a^mSa^n\subseteq S\setminus E$ implies that $a^mSa^n\subseteq A$ whence A is an (m,n)-ideal of S\E and S\E is a partial c-(m,n)-ideal semigroup.

(iv) Let a∈S and p∈N be the smallest natural number such that $a^p\in E$ and let $a^p=e$. Then $a^{p+1}=aa^p$ and $a^{p+1}=a^pa$ implies that $a^{p+1}=ea=ae\in E$ since E is an ideal of S. Every finite cyclic semigroup is unipotent, whence $a^{p+1}=e$, e is a zero in ⟨a⟩ and $\langle a\rangle=\{a,a^2,\ldots,a^p=e\}$. Let p>2m+2n+1. Then for the semigroup B from (i) we have the same contradiction as like in (i). Hence 2m+2n+1≥p, where $p=|\langle a\rangle|$.

(v) Let $x,y\in S_e$. Then, there exists $p,q\in N$ such that $x^p=y^q=e$ and e is a zero for x and y. By Theorem 1.1. we have that $(xy)^m e(xy)^n\in\langle xy\rangle$ i.e. $e\in\langle xy\rangle$. Hence, there exists $r\in N$ such that $e=(xy)^r$.

(vi) Let $a,b\in S$ and $e_a\in\langle a\rangle$, $e_b\in\langle b\rangle$. Let $g\in\langle a^m b^n\rangle$ i.e. $(a^m b^n)^k=g$. Then $ge_a=a^m b^n(a^m b^n)^{k-1}e_a\in a^m S e_a\subseteq\langle a\rangle$, whence $ge_a=e_a$. Also, $e_b g=e_b(a^m b^n)^{k-1}a^m b^n\in e_b S b^n\subseteq\langle b\rangle$, whence $e_b g=e_b$. From $ge_a=e_a$ and $e_b g=e_b$ we have that $g=ge_a e_b g=e_a e_b$ i.e. $e_a e_b\in\in\langle a^m b^n\rangle$.□

THEOREM 1.3. Let Q be a periodic partial c-(m,n)-ideal semigroup, E be a rectangular band and $Q\cap E=\emptyset$. Let $f: S=Q\cup E\to E$ such that $f(e)=e$ for every $e\in E$ and $f_{/Q}$ is a partial homomorphism. We define an operation on S by

$$xy=\begin{cases}xy & \text{as in Q, if } x,y\in Q \text{ and } xy \text{ is definied in Q}\\ f(x)f(y) & \text{otherwise}\end{cases}$$

Then S is a c-(m,n)-ideal semigroup.

Proof: Let $a,s\in S$. Then $a^m s a^n\in Q$ implies $a^m s a^n=a^k\in\in\langle a\rangle$. Let $a^m s a^n\notin Q$. Then $a^m s a^n=f(a^m)f(s)f(a^n)=f(a)^m f(s)f(a)^n==f(a)f(s)f(a)$. If $p\in N$ is the smallest number such that $a^p\notin Q$, then $a^p=aa^{p-1}=f(a)f(a^{p-1})=f(a)f(a)^{p-1}=f(a)f(a)=f(a)$. Hence, $a^m s a^n=f(a)\in\langle a\rangle$.□

THEOREM 1.4. S is a c-(m,n)-ideal semigroup with zero if and only if S is a c-(m,n)-ideal nil-semigroup.

Proof: Let S be a c-(m,n)-ideal semigroup with zero 0 and let $a\in S$. Then $a^m 0 a^n\in\langle a\rangle$ i.e. $0\in\langle a\rangle$. Hence, S is a nil-semigroup. If e is an idempotent from S then $0\in\langle e\rangle=\{e\}$, whence e=0 and S is unipotent. Conversely follovs immediately.□

Let M and T be the disjoint semigroups and T contains a zero 0. The semigroup S is called ideal extension of a semigroup M by T if M is an ideal in S and the Rees quotient semigroup $S_{/M}$ is isomorphic to T [2].

THEOREM 1.5. S is a c-(m,n)-ideal semigroup if and only if S is an ideal extension of the rectangular band E by a c-(m,n)-ideal nil-semigroup.

Proof: Let S be a c-(m,n)-ideal semigroup. By Theorem 1.2.(iii) we have that $S\setminus E$ is a c-(m,n)-ideal partial nil-semigroup and we can get $S_{/E}$ from $S\setminus E$ by the extension by 0 as like in Theorem 1.3.. From this Theorem $S_{/E}$ is a c-(m,n)-ideal semigroup.

Conversely, let S is an ideal extension of the rectangular band by a c-(m,n)-ideal nil-semigroup. For $a\in S\setminus E$ we have that $(a\rho)^m S_{/E}(a\rho)^n\subseteq\langle\langle a\rho\rangle\rangle=\langle\{a\}\rangle$, where $a\rho$ is the class of the element a of modE. Hence for all $b\in S$ we have that $(a\rho)^m(b\rho)(a\rho)^n\subseteq\langle a\rangle$, whence $a^m b a^n\in\langle a\rangle$. Also, for $e\in E$ we have that $e^m S e^n=eSe=e(eSe)e=eEe=e$.

Hence, for every $a\in S$ we have that $a^m S a^n\in\langle a\rangle$ and by Theorem 1.1. it implies that S is a c-(m,n)-ideal semigroup.□

2. (m,n)-IDEAL SEMIGROUPS

THEOREM 2.1. The folloving conditions on a semigroup S are equivalent:

(i) S is (m,n)-ideal

(ii) $C^m S C^n\subseteq\langle C\rangle$ for every nonempty $C\subset S$

(iii) $[C]_{m,n}=\langle C\rangle$ for every nonempty $C\subset S$

Proof: Let (i) holds. Then for every nonempty subset C of S we have that $\langle C\rangle^m S\langle C\rangle^n\subseteq\langle C\rangle$ i.e. $C^m S C^n\subseteq\langle C\rangle^m S\langle C\rangle^n\subseteq\subseteq\langle C\rangle$. Conversely, if (ii) holds, let B be a subsemigroup of S and C is the set of generators of B. Then $x\in B^m$ is of the form $x=a_1\ldots a_m$ where $a_i\in B$ and $y\in B^n$ is of the form $y=b_1\ldots b_n$ where $b_j\in B$. Since $a_i,b_j\in B$ and C generates B, we have that $a_i\in C^{k_i}(k_i\geq 1)$, $b_j\in C^{r_j}(r_j\geq 1)$. Then $xsy\in B^m S B^n$ is of the form $xsy=a_1\ldots a_m s b_1\ldots b_n\in C^{k_1}\ldots C^{k_m}SC^{r_1}\ldots C^{r_n}=C^{k_1+\ldots+k_m}SC^{r_1+\ldots+r_n}==C^{k_1+\ldots+k_m-m}C^m S C^n C^{r_1+\ldots+r_n-n}\in\langle C\rangle\langle C\rangle\langle C\rangle\subseteq\langle C\rangle=B$. Hence, we have that (i)$\Leftrightarrow$(ii).

Let (ii) holds. Then $[C]_{m,n}=C\cup C^2\cup\ldots\cup C^{m+n}\cup\cup C^m S C^n\subseteq\langle C\rangle\cup\ldots\cup\langle C\rangle=\langle C\rangle$. Conversely, let (iii) holds. Then $C^m S C^n\subseteq[C]_{m,n}=\langle C\rangle$, whence (ii)$\Leftrightarrow$(iii).□

THEOREM 2.2. If S is an (m,n)-ideal semigroup, then S is an ideal extension of the rectangular band E by a (m,n)-ideal nil-semigroup.

Proof: $S_{/E}$ is a semigroup with zero. By Theorem 3.1. [5] $S \setminus E$ is a partial (m,n)-ideal semigroup and we can get $S_{/E}$ from $S \setminus E$ by an extension by the zero as like in Theorem 3.2. [5]. From this Theorem $S_{/E}$ is an (m,n)-ideal semigroup and by Theorem 1.4. it is a nil-semigroup.□

3. BI-IDEAL SEMIGROUPS

COROLLARY 3.1. The folloving conditions on a semigroup S are equivalent:

(i) S is bi-ideal

(ii) $CSC \subseteq \langle C \rangle$ for every nonempty $C \subset S$

(iii) $B[C] = \langle C \rangle$ for every nonempty $C \subset S$

(iv) $(\forall a,b \in S)\ aSb \subseteq \langle a,b \rangle$

(v) $(\forall a,b \in S)\ \{a,b\}S\{a,b\} \subseteq \langle a,b \rangle$

(vi) $(\forall a,b \in S)\ B[\{a,b\}] = \langle a,b \rangle$

Proof: From Theorem 5. [8] we have that (i)⇔(ii)⇔⇔(iii). Also, it is clear that (iii)⇒(vi).

(vi)⇒(v) since $\{a,b\}S\{a,b\} \subseteq B[\{a,b\}] = \langle a,b \rangle$

(v)⇒(iv) since $aSb \subseteq \{a,b\}S\{a,b\} \subseteq \langle a,b \rangle$

(iv)⇒(ii) since for every $asb \in CSC$ we have that $asb \in aSb \subseteq \langle a,b \rangle \subseteq \langle C \rangle$.□

The folloving Theorem 3.3. and Lemma are got from Theorem 1.5. and Theorem 1.2.(vi) for the c-bi-ideal semigroup.

THEOREM 3.3. S is a c-bi-ideal semigroup if and only if S is an ideal extension of the rectangular band E by a c-bi-ideal nil-semigroup.

LEMMA: Let S is a c-bi-ideal semigroup. Then for every $a,b \in S$ $e_a e_b \in \langle ab \rangle$, where e_a and e_b are idempotents from $\langle a \rangle$ and $\langle b \rangle$.

COROLLARY 3.4. S is a bi-ideal semigroup if and only if S is an ideal extension of the rectangular band E by a bi-ideal nil-semigroup.

Proof: Let S be a bi-ideal semigroup. From Theorem 2.2. we have that $S_{/E}$ is a bi-ideal semigroup and it is a nil-semigroup.

Conversely, let S be an ideal extension of the rectangular band E by a bi-ideal nil-semigroup $S_{/E}$. Then $S_{/E}$ is a c-bi-ideal nil-semigroup and by Theorem 3.3. S is a c-bi-ideal semigroup and the condition of Lemma holds.

Let $a,b,s \in S$. If $asb \in E$, by Lemma we have that $asb = e_a e_s e_b = e_a e_b \in \langle a,b \rangle$. If $asb \in S \setminus E$ i.e. $asb = 0$ in $S_{/E}$, then by Corollary 3.1. we have that $asb \in \langle a,b \rangle$ in $S_{/E}$ since $S_{/E}$ is a bi-ideal semigroup, whence $asb \in \langle a,b \rangle$ in S. Hence, the condition $aSb \subseteq \langle a,b \rangle$ holds for every $a,b \in S$ and by Corollary 3.1. S is a bi-ideal semigroup.□

4. THE CONSTRUCTION OF A C-(m,n)-IDEAL SEMIGROUP

CONSTRUCTION: Let $E = I \times J$ be a rectangular band and let Q be a partial semigroup such that $E \cap Q = \emptyset$.

Let $\Phi: p \to \Phi_p$ be a mapping from Q into the semigroup $\mathcal{T}(I)$ of all mappings from I into itself and, also, let $\Psi: p \to \Psi_p$ be a mapping from Q into $\mathcal{T}(J)$.

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

(i) $pq \in Q \Rightarrow \Phi_{pq} = \Phi_q \Phi_p$, $\Psi_{pq} = \Psi_p \Psi_q$

(ii) $pq \notin Q \Rightarrow \Phi_q \Phi_p = \text{const.}$, $\Psi_p \Psi_q = \text{const.}$

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

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

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

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

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

(5) $pq \notin Q \Rightarrow pq = (i\Phi_q\Phi_p, j\Psi_p\Psi_q)$

Then S with this multiplication is a semigroup [10, 5,1-VIII]. A semigroup which is constructed in this way will be denoted by $\Sigma(I,J,Q,\Phi,\Psi)$.

THEOREM 4.1. S is a c-(m,n)-ideal semigroup if and only if S is isomorphic to a semigroup $\Sigma(I,J,Q,\Phi,\Psi)$ where Q is a partial c-(m,n)-ideal semigroup $(m,n \geq 1)$.

Proof: Let S is a c-(m,n)-ideal semigroup. Then by Theorem 1.5. S is an ideal extension of a rectangular band E by a c-(m,n)-ideal nil-semigroup $T = S_{/E}$. Let $Q = T \setminus 0 = S \setminus E$. Then Q is a c-(m,n)-ideal partial semigroup.

From Theorem 4.20.[2]we have that S is a subsemigroup of an ideal extension $\bar{S}$ of a translational hull $\Omega(E)$ of E by T. Since translational hull $\Omega(E)$ is a semigroup with identity, then by Theorem 4.19.[2] we have that the multiplication on $\bar{S}$ is determined by a partial homomorphism $f:Q\to\Omega(E)$ with:

$$ab=\begin{cases} ab & \text{if } ab\in Q \\ f(a)f(b) & \text{if } ab\notin Q \end{cases}$$

$$ua=uf(a),\quad au=f(a)u,\quad uv=uv$$

for all $a,b\in Q$ and all $u,v\in\Omega(E)$.

The translational hull $\Omega(E)$ of a rectangular band $E=IxJ$ is isomorphic to a Cartesian product $\mathcal{T}(I)x\mathcal{T}(J)$ where the multiplication is given with:

$$(\Phi_1,\Psi_1)(\Phi_2,\Psi_2)=(\Phi_2\Phi_1,\Psi_1\Psi_2)$$

for all $(\Phi_1,\Psi_1),(\Phi_2,\Psi_2)\in\Omega(E)$[3].

Also, E is an ideal of $\Omega(E)$ and elements from E are of the form (Φ^i,Ψ^j) where Φ^i and Ψ^j are constant mappings i.e. for every $k\in I$ and every $\ell\in J$

$$k\Phi^i=i \quad\text{and}\quad \ell\Psi^j=j\ .$$

Then, we can write $(i,j)=(\Phi^i,\Psi^j)$. Then

$$(i,j)(\Phi,\Psi)=(\Phi^i,\Psi^j)(\Phi,\Psi)=(\Phi\Phi^i,\Psi^j\Psi)=(i,j\Psi)\in E$$
$$(\Phi,\Psi)(i,j)=(\Phi,\Psi)(\Phi^i,\Psi^j)=(\Phi^i\Phi,\Psi\Psi^j)=(i\Psi,j)\in E$$

For $a\in Q$ let $f(a)=(\Phi_a,\Psi_a)$. Since f is a partial homomorphism, for $a,b\in Q$, $ab\in Q$ we have that

$(\Phi_{ab},\Psi_{ab})=f(ab)=f(a)f(b)=(\Phi_a,\Psi_a)(\Phi_b,\Psi_b)=(\Phi_b\Phi_a,\Psi_a\Psi_b)$ whence $\Psi_{ab}=\Phi_b\Phi_a$ and $\Psi_{ab}=\Psi_a\Psi_b$.

Since S is a subsemigroup of $\bar{S}$, we have that $ab=f(a)f(b)\in E$ i.e. $(\Phi_b\Phi_a,\Psi_a\Psi_b)\in E$ for $a,b\in Q$, $ab\notin Q$, whence $\Phi_b\Phi_a=$const. and $\Psi_a\Psi_b=$const.

Hence conditions (i) and (ii) hold.

From the definition of a multiplication on $\bar{S}$ we have that conditions (1) and (4) hold and

$$a(i,j)=f(a)(i,j)=(\Phi_a,\Psi_a)(i,j)=(i\Phi_a,j)$$
$$(i,j)a=(i,j)f(a)=(i,j)(\Phi_a,\Psi_a)=(i,j\Psi_a)$$

For $a,b\in Q$, $ab\notin Q$

$$ab=f(a)f(b)=(\Phi_b\Phi_a,\Psi_a\Psi_b)=(i\Psi_b\Phi_a,j\Psi_a\Psi_b)$$

since $\Phi_b\Phi_a=$const and $\Psi_a\Psi_b=$const. Hence, conditions (2), (3) and (5) hold.

Conversely, let $S=\Sigma(I,J,Q,\Phi,\Psi)$ where Q is a partial c-(m,n)-ideal semigroup. It is clear that $Q\cup\{0\}$ is a c-(m,n)-ideal nil-semigroup and S is an ideal extension of a rectangular band E by $Q\cup\{0\}$. Hence, by Theorem 1.5. we have that S is a c-(m,n)-ideal semigroup.□

THEOREM 4.2. S is a c-(m,0)-ideal (c-(0,n)-ideal) semigroup if and only if S is an ideal extension of a left zero (right zero) semigroup E by a c-(m,0)-ideal (c-(0,n)-ideal) nil-semigroup. ($m\geq 1 (n\geq 1)$)

Proof: Let S is a c-(m,0)-ideal semigroup. Then for all $a\in S$, $\langle a\rangle$ must be a finite semigroup, since $a^{2m}a\in\langle a^2\rangle^m S\subseteq\subseteq\langle a^2\rangle$. Then S is periodic and the set E of all idempotents from S is nonempty set. For all $e\in E$ and $s\in S$ we have that $es=e^m s\in\langle e\rangle^m S\subseteq\langle e\rangle=\{e\}$, i.e. $es=e$ and, also, $(se)(se)=sese=s(es)e=see=se$. Then $se,es\in E$ i.e. E is an ideal of S. Now, it is clear that S_E is a c-(m,0)-ideal nil-semigroup.

Conversely, if S is an ideal extension of a left zero semigroup E by a c-(m,0)-ideal nil-semigroup, then for $a\in S\setminus E$ we have that $(a\rho)^m S_E\subseteq\langle(a\rho)\rangle=\langle a\rangle$, where $a\rho$ is the class of the element a of modE. Hence, for all $b\in S$ we have that $(a\rho)^m(b\rho)\subseteq\langle a\rangle$ i.e. $a^m b\in\langle a\rangle$. Also, for $e\in E$ we have that $e^m S=eS=e(eS)=eE=e$. Hence S is a c-(m,0)-ideal semigroup.□

COROLLARY 4.3. S is a (m,0)-ideal ((0,n)-ideal) semigroup if and only if S is an ideal extension of a left zero (right zero) semigroup E by a (m,0)-ideal ((0,n)-ideal) nil-semigroup. ($m\geq 1 (n\geq 1)$)

COROLLARY 4.4. S is a c-(m,0)-ideal (c-(0,n)-ideal) semigroup if and only if S is isomorphic to a semigroup $\Sigma(I,J,Q,\Phi,\Psi)$ where $|I|=1$ and Q is a partial c-(m,0)-ideal semigroup ($|J|=1$ and Q is a partial c-(0,n)-ideal semigroup).($m\geq 1 (n\geq 1)$)

COROLLARY 4.5. S is a (m,0)-ideal ((0,n)-ideal) semigroup if and only if S is isomorphic to a semigroup $\Sigma(I,J,Q,\Phi,\Psi)$ where $|I|=1$ and Q is a partial (m,0)-ideal semigroup ($|J|=1$ and Q is a partial (0,n)-ideal semigroup). ($m\geq 1 (n\geq 1)$)

COROLLARY 4.6. S is a bi-ideal semigroup if and only if S is isomorphic to a semigroup $\Sigma(I,J,Q,\Phi,\Psi)$ where Q is a partial bi-ideal semigroup.

Proof: By Theorem 1.[9] and Corollary 3.4.└

REFERENCES

[1] S. Bogdanović: Semigroups with a system of subsemigroups, University of Novi Sad - Institute of Mathematics 1985.

[2] Clifford A.H. and G.B. Preston: The algebraic theory of semigroups, Amer. math. soc. 1961

[3] Howie J. An introduction to semigroup theory, Acad press 1976

[4] Lajos S. Generalized ideals in semigroups, Acta sci. Math. 22(1961) 217-222

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

[8] S. Bogdanović, P. Kržovski, P. Protić, B. Trpenovski: Bi and quasi ideal semigroup with n-property, Third Algebraic conference Beograd 1982, 27-34

[9] Bogdanović S. and S. Milić: (m,n)-ideal semigroups, Proc of the Third Algebraic conference, Beograd 1982, 35-39

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

Filozofski fakultet
grupa za Matematiku
Ćirila i Metodija 2
18000 Niš

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

POST THEOREM FOR VECTOR VALUED SEMIGROUPS

Ǵ. Čupona, S. Markovski, B. Janeva

Abstract. The main result of this paper is the following

THEOREM. Let m,k,p and q be integers such that $m,k,q \geq 1$, $p \geq 0$. If $(Q;[\![\ ]\!])$ is an $(m+p+q,m+p)$-semigroup, then there is an $(m+1,m)$-semigroup $(P;[\ ])$ such that $Q \subseteq P$ and

$$[\![a_1^{m+p+q}]\!] = (b_1^{m+p}) \Longleftrightarrow [a_1^{m+p+q}] = [b_1^{m+p}], \qquad (*)$$

for any $a_\nu, b_\lambda \in Q$. (If $p=0$, then we write $[b_1^m]$ instead of (b_1^m).)

0. We give here necessary preliminary definitions and results.

Let n and m be positive integers such that $n-m=k \geq 1$. A mapping

$$[\ ]: (x_1,\ldots,x_n) \longmapsto [x_1 \ldots x_n]$$

from Q^n to Q^m [1)] is called an associative (n,m)-operation iff the following identity is satisfied for every $j \in \{1,2,\ldots,k\}$:

$$[[x_1^n]x_{n+1}^{n+k}] = [x_1^j[x_{j+1}^{j+n}]x_{j+n+1}^{n+k}].$$

In this case we say that $(Q;[\ ])$ is an (n,m)-semigroup, or a vector valued semigroup. (We remark that the notion of vector

[1)] Q^r is the r-th cartezian power of Q; x_α^β is an abbreviation for the „string" sequence $x_\alpha x_{\alpha+1} \ldots x_\beta$ if $\alpha \leq \beta$, and it is „empty" if $\alpha > \beta$. Thus, (x_α^β) stands for $(x_\alpha, x_{\alpha+1}, \ldots, x_\beta)$.

This paper is in final form and no version of it will be submitted for publication elsewhere.

valued semigroups is defined in [5]).

If $[\ ]$ is an (n,m)-operation, nonnecessarily associative, then we can define an (m+sk,m)-operation $[\ ]^s$, for every $s \geq 1$, in the following way: $[x_1^n]^1 = [x_1^n]$ and

$$[x_1^{sk+m}]^s = [x_1^k[x_{k+1}^{sk+m}]^{s-1}] \text{ if } s \geq 2$$

The following „associative law" holds:

0.1. If $(Q;[\ ])$ is an (m+k,m)-semigroup, then for every $r,s \geq 1$, $j \in \{1,2,\ldots,sk\}$ the equality:

$$[x_1^j y_1^{rk+m} x_{j+1}^{sk}]^{r+s} = [x_1^j[y_1^{rk+m}]^r x_{j+1}^{sk}]^s$$

is an identity on $(Q;[\ ])$.

As a corollary we have:

0.2. If $(Q;[\ ])$ is an (m+k,m)-semigroup then $(Q;[\ ]^s)$ is an (m+sk,m)-semigroup for any $s \geq 1$. (In the future, we will omit the index s in $[\ ]^s$. Thus, an (m+1,m)-semigroup $(Q;[\ ])$ induces an (m+k,m)-semigroup $(Q;[\ ])$ for any $k \geq 1$. We note that this simplification in the notation is already used in the formulation of Theorem.)

If $(P;[\ ])$ is an (m+1,m)-semigroup and if $Q \subseteq P$ such that:

$$(a_1^{m+k}) \in Q^{m+k} \Longrightarrow [a_1^{m+k}] \in Q^m,$$

then we say that Q is an (m+k,m)-subsemigroup of $(P;[\ ])$. In this case, the restriction of $[\ ]^k$ on Q induces an (m+k,m)-semigroup $(Q;[\ ])$, called (m+k,m)-subsemigroup of $(P;[\ ])$.

Thus, the conclusion of Theorem for p=0 can be stated as follows:

THEOREM 1. Every (m+k,m)-semigroup is an (m+k,m)-subsemigroup of an (m+1,m)-semigroup.

We note that the following generalization is a corollary of Theorem 1:

THEOREM 1´. Every (m+sk,m)-semigroup is an (m+sk,m)-subsemigroup of an (m+k,m)-semigroup.

Also, in the case $p > 0$, the following generalization is a corollary of Theorem:

THEOREM 2. If m,p,q and k are positive integers such that k is a divisor of the both p and q, then for every (m+p+q,m+p)-semigroup $(Q;[\![\ ]\!])$ there is an (m+k,m)-semigroup $(P;[\ ])$ such that $Q \subseteq P$ and (*) holds for any $a_\nu, b_\lambda \in Q$.

We have named the subject of this work Post Theorem, because there is an analogy with corresponding Post's Theorem for polyadic groups ([4]). The question whether Post Theorem is true for vector valued groups is a natural one, but we do not know the answer till now.

Further on we assume that $m \geq 2$, since our Theorem reduces to the well known Post Theorems concerning embeddings of polyadic semigroups in (binary) semigroups (see, for example [2]) in the case p=0, m=1, and to the fact that every vector valued semigroup is a vector valued subsemigroup of a (binary) semigroup ([1]) in the case m=1, $p > 0$.

We also note that in the proof of our results we use some ideas from the paper [3], where a convenient description of free vector valued semigroups is given.

1. Let $(Q;[\![\ ]\!])$ be an (m+p+q,m+p)-semigroup and let $(\overline{Q};\{[\ ]_i^s \mid s \geq 1, i \in \{1,2,\ldots,m\}\})$ be the absolutely free universal algebra with a base Q, where $[\ ]_i^s$ is an m+s-ary operator symbol for any $s \geq 1$ and any $i \in \{1,2,\ldots,m\}$. We will give below a description of this algebra.

If X is a non empty set, then X^* is the set of all finite sequences on X (including the empty sequence). (In other words, X^* is the free monoid (freely) generated by X.) If $x = x_1 x_2 \ldots x_r$, where $x_\nu \in X$, then r is said to be the dimension of x, and is denoted by d(x). The empty sequence (denoted by 1) has, by definition, dimension zero. Also, we will write x_1^r instead of $x_1 x_2 \ldots x_r$.

We put $Q_o = Q$, $N_m = \{1,2,\ldots,m\}$ and

$$C_s = \{u \in Q_s^* \mid d(u) \geq m+1\}$$

$$Q_{s+1} = Q_s \cup C_s \times N_m,$$

and

$$\overline{Q} = \bigcup_{s \geq 0} Q_s.$$

Thus we have:

1.1. $u \in \overline{Q}$ iff $u \in Q$ or $u=(v,i)$, where $v \in \overline{Q}^*$, $d(v) \geq m+1$, $i \in N_m$.

Now, the algebra $(\overline{Q};\{[\ ]_i^s \mid s \geq 1,\ i \in N_m\})$ is defined in the following way:

If $s \geq 1$, $u_1,u_2,\ldots,u_{s+m} \in \overline{Q}$, and $i \in N_m$, then:

$$[u_1^{s+m}]_i^s = (u_1^{s+m},i).$$

By putting:

$$[u_1^{s+m}]^s = (v_1^m) \Longleftrightarrow [u_1^{s+m}]_i^s = v_i,$$

we obtain the absolutely free vector valued algebra $(\overline{Q};[\ ]^s, s \geq 1)$ with a base Q, where $[\ ]^s$ is an $(m+s,m)$-operation on $\overline{Q}$.

Remark: We will use below the following notations:

(i) a,b,c,d (with or without indexes) will always denote elements of Q.

(ii) x,y,z,u,v,w,t (with or without indexes) will always denote elements of $\overline{Q}^*$.

(iii) $(x,i) \in \overline{Q}$ will always mean that $x \in \overline{Q}^*$ is such that $d(x) \geq m+1$.

(iv) Sometimes, for technical reasons, an element $u_i \in \overline{Q}$ will be denoted by (u_1^m,i), where $u_\nu \in \overline{Q}$, $i \in N_m$. (Note that $(u_1^m,i) \in \overline{Q}$ by the construction of $\overline{Q}$.)

We assume that the meaning of „an appearence of u in v", and „w is obtained from v by substitution of an appearence of u in v by t", are clear. Also, the validness of the two properties below are evident.

1.2. If $u \in \overline{Q}$ and if v is obtained when an appearence of $u' \in \overline{Q}$ in u is substituted by $v' \in \overline{Q}$, then $v \in \overline{Q}$.

1.3. If $(xyz,i) \in \overline{Q}$, and $(y,\nu) \in \overline{Q}$, where $d(xz) \geq 1$, then $u = (x(y,1)(y,2)\ldots(y,m)z,i) \in \overline{Q}$ as well[1].

We define two relations $\vdash_1$ and $\vdash_2$ in $\overline{Q}$ as follows.

If $u,v \in \overline{Q}$, then

$\vdash_1$: $u \vdash_1 v$ iff v is obtained from u when an appearence of (b_1^{m+p},i) is substituted by (a_1^{m+p+sq},i), where $[\![a_1^{m+p+sq}]\!] = (b_1^{m+p})$ in $(Q;[\ ])$. (If $p=0$, then $(b_1^m,i)=b_i$.)

$\vdash_2$: $u \vdash_2 v$ iff v is obtained from u when an appearence of $(xyz,j) \in \overline{Q}$ is substituted by $(x(y,\nu)_{\nu=1}^m z,j)$, where $d(y) \geq m+1$.

Then, we define a relation ~ by:

~: $u \sim v$ iff $u \vdash_1 v$ or $v \vdash_1 u$ or $u \vdash_2 v$ or $v \vdash_2 u$, i.e. ~ is the symmetric extension of the union of $\vdash_1$ and $\vdash_2$.

Finally, let $\approx$ be the reflexive and transitive extension of ~, i.e.

$\approx$: $u \approx v$ iff there exist $w_o,w_1,\ldots,w_r \in \overline{Q}$, such that $u=w_o$, $v=w_r$, $r \geq 0$, and $w_{j-1} \sim w_j$ for each $j \in \{1,2,\ldots,r\}$.

Thus:

1.4. $\approx$ is an equivalence relation on $\overline{Q}$. (Namely, it is the smallest equivalence relation containing $\vdash_1$ and $\vdash_2$.)

The following lemma is true:

LEMMA 1. $(b_1^{m+p},i) \approx (c_1^{m+p},i) \Longleftrightarrow (b_1^{m+p},i) = (c_1^{m+p},i)$.

Namely, Lemma 1 is a consequence of Lemma 2, given below. To state Lemma 2, we will denote by Q' the set

[1] Sometimes we use the abbreviated notation $(x(y,\nu)_{\nu=1}^m z,i)$ for $(x(y,1)\ldots(y,m)z,i)$.

$$Q' = \{(a_1^{m+p},i) \mid a_\nu \in Q, \quad i \in \mathbb{N}_m\}.$$

(If p=0, then $Q'=Q$.)

LEMMA 2. There exists a map $\xi:\overline{Q} \to \overline{Q}$ with the properties:

(i) $\xi(u) = u$, for every $u \in Q'$;

(ii) $u \sim v$ and $(\xi(u) \in Q'$ or $\xi(v) \in Q') \Longrightarrow \xi(u) = \xi(v)$.

Let us assume that Lemma 2 is true, and $(b_1^{m+p},i) \simeq (c_1^{m+p},i)$. Then, there exist $w_0,w_1,\ldots,w_r \in \overline{Q}$ such that $w_0=(b_1^{m+p},i)$, $w_r=(c_1^{m+p},i)$ and $w_{j-1} \sim w_j$ for each $j \in \{1,2,\ldots,r\}$. Since $w_0,w_r \in Q'$, $\xi(w_0)=w_0$, $\xi(w_r)=w_r$, and also $\xi(w_0)=\xi(w_1)=\ldots=\xi(w_r)$, i.e. $(b_1^{m+p},i) = w_0 = w_r = (c_1^{m+p},i)$.

The proof of Lemma 2, that is the construction of the map ξ, will be given in the next part of this paper. Here we will show that Theorem is a consequence of Lemma 1.

First we state two propositions.

1.5. $\simeq$ is a congruence on the algebra $(\overline{Q};[\ ]^s,\ s \geq 1)$.

Proof: It is clear that if $u,v \in \overline{Q}$, $x,y \in \overline{Q}^*$ are such that $u \underset{\alpha}{\vdash} v$, $d(xy)=m+s-1$, $s \geq 1$, then $(xuy,i) \underset{\alpha}{\vdash} (xvy,i)$ for every $i \in \mathbb{N}_m$, and this implies that $\simeq$ is a congruence.

Denote the factor algebra $(\overline{Q}/\simeq;[\ ]^s,\ s \geq 1)$ by $(P;[\ ]^s,\ s \geq 1)$, and the operation $[\ ]^1$ by $[\ ]$. If $x,y,z \in \overline{Q}^*$ are such that $d(y) \geq m+1$, $d(xz) \geq 1$, then for every $i \in \mathbb{N}_m$ we have

$$(xyz,i) \underset{2}{\vdash} (x(y,\nu)_{\nu=1}^{m}z,i),$$

i.e. $(xyz,i) \simeq (x(y,\nu)_{\nu=1}^{m}z,i)$, and this implies that:

1.6. $(P;[\ ])$ is an $(m+1,m)$-semigroup.

Now we are ready to show that Theorem is a consequence of Lemma 1.

First we consider the case p=0. Thus, we have an $(m+q,m)$-semigroup $(Q;[\![\ ]\!])$. Then, $Q'=Q$, and by Lemma 1 we have: $a \simeq b \Longrightarrow a = b$. Therefore we can assume that $Q \subseteq P$, and if $[\![a_1^{m+sq}]\!] = (b_1^m)$, then $(a_1^{m+sq},i) \simeq b_i$ for each $i \in \mathbb{N}_m$, and this implies that $[a_1^{m+sq}] = (b_1^m)$ in $(P;[\ ])$.

Conversely, let $[a_1^{m+sq}] = (b_1^m)$ in $(P;[\ ])$, i.e. $(a_1^{m+sq},i) \simeq b_i$ for each $i \in \mathbb{N}_m$, and let $[\![a_1^{m+sq}]\!] = (c_1^m)$ in $(Q;[\![\ ]\!])$. Then we have $c_i \simeq (a_1^{m+sq},i)$ and thus $b_i \simeq c_i$. By Lemma 1, this implies $b_i = c_i$. This completes the proof of Theorem 1, i.e. of Theorem for p=0.

It remains the case $p > 0$.

Let $(Q;[\![\ ]\!])$ be an $(m+p+q,m+p)$-semigroup, and let $\overline{Q}$ and $(P;[\ ])$ be defined as before. We have that $a \simeq u \Longrightarrow a = u$, for neither of the relations $a \underset{1}{\vdash} u$, $u \underset{1}{\vdash} a$, $a \underset{2}{\vdash} u$, $u \underset{2}{\vdash} a$ holds. Thus we can assume that $Q \subseteq P$.

If $[\![a_1^{m+p+sq}]\!] = (b_1^{m+p})$ in $(Q;[\![\ ]\!])$, then $(a_1^{m+p+sq},i) \simeq (b_1^{m+p},i)$ for each $i \in \mathbb{N}_m$, and thus we have $[a_1^{m+p+sq}] = [b_1^{m+p}]$ in $(P;[\ ])$. Assume that we also have $[a_1^{m+p+sq}] = [c_1^{m+p}]$ in $(P;[\ ])$. Then $(b_1^{m+p},i) \simeq (c_1^{m+p},i)$, and this, by Lemma 1, implies that $(b_1^{m+p},i) = (c_1^{m+p},i)$, i.e. $b_\nu = c_\nu$ for any $\nu \in \{1,2,\ldots,m+p\}$. This completes the proof of Theorem for $p > 0$.

2. Here we will construct a mapping $\xi:\overline{Q} \to \overline{Q}$ such that the conditions of Lemma 2 will be satisfied.

Define the length $|x|$ of an element $x \in \overline{Q}^*$ by

$$|1| = 0, \quad |a| = 1, \quad |(u,i)| = |u|, \quad |tv| = |t| + |v|,$$

where $(u,i) \in \overline{Q}$.

The mapping $\xi:\overline{Q} \to \overline{Q}$ will be defined by induction on the length of elements of $\overline{Q}$ as follows:

(0) $\qquad \xi(a) = a.$

Let $u=(x,i) \in \overline{Q}$, where $x=x_1x_2\cdots x_s$, $x_1,\ldots,x_s \in \overline{Q}$. Assume that for every $v \in \overline{Q}$, such that $|v|<|u|$, $\xi(v) \in \overline{Q}$ is well defined, and that the following statements hold:

$$|\xi(v)| \leq |v|, \ \xi(\xi(v)) = \xi(v), \ \xi(v) \neq v \Longleftrightarrow |\xi(v)| < |v| \qquad (2.1)$$

Thus $\xi(x_\nu)$ is a well defined element of $\overline{Q}$ for every $\nu\in\mathbb{N}_s$, and if we put

$$y = \xi(x_1)\cdots\xi(x_s)$$

then by (2.1) $y \neq x$ iff $|y|<|x|$. Assume that $y \neq x$. Then we define $\xi(u)$ by:

(i) $\xi(u) = \xi(y,i)$.

Assume, now, that $y = x$, and that x has the following form:

$$x = x'(y_1,1)(y_2,2)\cdots(y_m,m)x''$$

where x' has the least possible length. Now, $\xi(u)$ is defined by

(ii) $\xi(u) = \xi(x'y_1x'',i)$.

If $x = a_1^{m+p+sq}$, $s \geq 1$ and if $[\![a_1^{m+p+sq}]\!]=(b_1^{m+p})$, then $\xi(u)$ is defined by:

(iii) $\xi(u) = (b_1^{m+p},i)$

(Note that in the case $p=0$ (b_1^m,i) denotes b_i.)

If $\xi(u)$ is not defined by either of the cases (0)-(iii), then we put

(iv) $\xi(u) = u$.

Thus $\xi:\overline{Q} \to \overline{Q}$ is a well defined mapping.

We can extend ξ to a mapping $\xi^*:\overline{Q}^* \to \overline{Q}^*$ by the usual way. Namely,

$$\xi^*(1) = 1,\ u\in\overline{Q} \Longrightarrow \xi^*(u) = \xi(u),\ \xi^*(xy) = \xi^*(x)\xi^*(y)$$

Further on we will write ξ instead of ξ^*.

We say that x is <u>reducible</u> if $\xi(x) \neq x$ or $x=x'(y_1,1)\cdots\cdots(y_m,m)x''$, where $d(y_\nu) \geq m+1$ for $\nu\in\mathbb{N}_m$. Otherwise x is said to be <u>reduced</u>.

The following nine propositions are clear by the definition of ξ.

<u>2.1</u>. $\xi(\xi(u)) = \xi(u)$.

<u>2.2</u>. $\xi(u) \neq u \Longleftrightarrow |\xi(u)| < |u|$.

<u>2.3</u>. $\xi(xyz) = \xi(x\xi(y)z)$.

<u>2.4</u>. $(xyz,i)\in\overline{Q} \Longrightarrow \xi(xyz,i) = \xi(x\xi(y)z,i)$.

<u>2.5</u>. <u>If</u> $p>0$ <u>then</u>:

a) $\xi(u)\in Q \Longleftrightarrow u\in Q$;

b) $\xi(a_1^{m+r},i) = (a_1^{m+r},i)$, $r\in\mathbb{N}_p$.

<u>2.6</u>. <u>If</u> $(x,i)\in\overline{Q}$ <u>and</u> $\xi(x,i) = (y,j)\notin Q$, <u>then</u> $i = j$.

<u>2.7</u>. <u>If</u> $(x,i)\in\overline{Q}$ <u>is such that</u> $\xi(x,i)\notin Q$, <u>then</u> $\xi(x,j)\notin Q$ <u>for every</u> $j\in\mathbb{N}_m$.

<u>2.8</u>. <u>Let</u> $v\in\overline{Q}$ <u>be obtained from</u> $u\in\overline{Q}$ <u>in such a way that one appearence of</u> $u'\in\overline{Q}$ <u>is substituted by</u> $v'\in\overline{Q}$. <u>If</u> $\xi(u') = \xi(v')$ <u>then</u> $\xi(u) = \xi(v)$.

<u>2.9</u>. <u>If</u> $x=a_1^\beta(y,\lambda)z$, $\beta \geq 0$, $\lambda \geq 2$, $\xi(y,\lambda) = (\overline{y},\lambda)\in Q$, $(x,i)\in\overline{Q}$, <u>then</u> $\xi(x,i)\notin Q'$.

<u>2.10</u>. <u>Let</u> $xz \neq 1$, $(y_\nu,\nu)\in\overline{Q}$ <u>and suppose that</u> $\xi(y_\nu,\nu) = (y_\nu,\nu)$ <u>or</u> $\xi(y_\nu,\nu)\notin Q'$. <u>Then</u>:

$$\xi(x(y_1,1)\cdots(y_m,m)z,i) = \xi(xy_1z,i) \qquad (2.2)$$

<u>Proof</u>: Let $\xi(y_\nu,\nu) = (\overline{y}_\nu,\nu)$. By induction on the lengths of the elements of $\overline{Q}^*$ it can be easily seen that (2.2) is true if anyone of the following four conditions is satisfied:

a) $\xi(xy_1\cdots y_mz) \neq xy_1\cdots y_mz$;

b) x is reducible;

c) $\overline{y}_\lambda \neq y_\lambda$ for some $\lambda \geq 2$;

d) y is not reduced.

In the case when none of a), b), c), d) is true, then (2.2) follows by the definition of ξ.

2.11. Let $[a_1^{m+p+sq}] = (b_1^{m+p})$ in $(Q;[\ ])$, and suppose that $v\in\bar{Q}$ is obtained from $u\in\bar{Q}$ when an appearence of a_1^{m+p+sq} in u is replaced by b_1^{m+p}. Then

$$\xi(u)\in Q' \text{ or } \xi(v)\in Q' \Longrightarrow \xi(u) = \xi(v).$$

Proof: There exists an $\alpha \geq 0$ and $u_0,u_1,\ldots,u_\alpha$, $v_0,v_1,\ldots,v_\alpha\in\bar{Q}$ such that

$$u = u_0,\ v = v_0$$

$$u_\lambda = (x_\lambda u_{\lambda+1} z_\lambda, i_\lambda),\quad v_\lambda = (x_\lambda v_{\lambda+1} z_\lambda, i_\lambda),\ 0 \leq \lambda < \alpha \qquad (2.3)$$

$$u_\alpha = (x_\alpha a_1^{m+p+sq} z_\alpha, i_\alpha),\quad v_\alpha = (x_\alpha b_1^{m+p} z_\alpha, i_\alpha).$$

It is clear that if one of the following conditions

a) $\xi(x_0\cdots x_\alpha z_\alpha\cdots z_0) \neq x_0\cdots x_\alpha z_\alpha\cdots z_0$,

b) x_λ is reducible for some λ,

is satisfied, then we can obtain a sequence of elements of $\bar{Q}$: $\bar{u}=\bar{u}_0$, $\bar{u}_1,\ldots,\bar{u}_\alpha$, $\bar{v}=\bar{v}_0,\bar{v}_1,\ldots,\bar{v}_\alpha$ such that (2.3) is satisfied, and moreover

$$\xi(u) = \xi(\bar{u}),\ \xi(v) = \xi(\bar{v}),\ |\bar{u}|<|u|,\quad |\bar{v}| < |v|,$$

which implies $\xi(u)=\xi(v)$ by induction.

Thus we can assume that:

a') $\xi(x_\lambda) = x_\lambda$, $\xi(z_\lambda) = z_\lambda$ for any λ, and

b') x_λ is reduced for any λ.

If there exists a λ such that $\xi(u_\lambda) = \xi(v_\lambda)$, then by 2.8 we have $\xi(u) = \xi(v)$.

Consider the case $\alpha = 0$, i.e.

$$u = (xa_1^{m+p+sq}z,i),\quad v = (xb_1^{m+p}z,i)$$

and $[a_1^{m+p+sq}] = (b_1^{m+p})$ in $(Q;[\ ])$.

If z is reducible then we can again obtain two elements

$$\bar{u} = (xa_1^{m+p+sq}z',i),\quad \bar{v} = (xb_1^{m+p}z',i)$$

such that

$$\xi(u) = \xi(\bar{u}),\ \xi(v) = \xi(\bar{v}),\quad |\bar{u}| < |u|,\ |\bar{v}| < |v|$$

and the proof follows by induction. So, we can assume that z is reduced.

Now, $\xi(u)\in Q'$ or $\xi(v)\in Q'$, iff $x=c_1^\beta$, $z=d_1^\gamma$ where $\beta+\gamma = rq$, $r \geq 0$. Then we have:

$$\begin{aligned}\xi(u) &= ([c_1^\beta a_1^{m+p+sq} d_1^\gamma], i) = \\ &= ([c_1^\beta [a_1^{m+p+sq}] d_1^\gamma], i) = \\ &= ([c_1^\beta b_1^{m+p} d_1^\gamma], i) = \\ &= \xi(v).\end{aligned}$$

There remains the case $\alpha > 0$. By the same argument as in the case $\alpha = 0$ we can assume that z_α is reduced. Also as in the case $\alpha = 0$ we can conclude that

$$\xi(u_\alpha) \neq u_\alpha \text{ iff } \xi(u_\alpha) = \xi(v_\alpha)\in Q',$$

and by 2.8 we will have $\xi(u) = \xi(v)$.

Thus, we can assume that $\xi(u_\alpha) = u_\alpha$, and then we will also have $\xi(v_\alpha) = v_\alpha$.

The fact that $\xi(u_0)\in Q'$ or $\xi(v_0)\in Q'$ and $\alpha > 0$ implies that $\xi(u_0) \neq u_0$, $\xi(v_0) \neq v_0$. Let β be the largest number such that $\xi(u_\beta) \neq u_\beta$ or $\xi(v_\beta) \neq v_\beta$. Then we have $\beta < \alpha$ and

$$\xi(u_{\beta+1}) = u_{\beta+1},\quad \xi(v_{\beta+1}) = v_{\beta+1}.$$

Since it is assumed that x_β is reduced, from the equalities

$$u_\beta = (x_\beta u_{\beta+1} z_\beta, i_\beta),\quad v_\beta = (x_\beta v_{\beta+1} z_\beta, i_\beta)$$

it follows that $\xi(u_\beta) \neq u_\beta$ or $\xi(v_\beta) \neq v_\beta$, iff one of the following three statements hold:

1) $x_\beta = x'(t_1,1)\cdots(t_{\nu-1},\nu-1)$, $i_{\beta+1} = \nu > 1$, $z_\beta = (t_{\nu+1},\nu+1)\cdots(t_m,m)z'$;

2) $i_{\beta+1} = 1$, $z_\beta = (t_2,2)\cdots(t_m,m)z'$;

3) $z_\beta = z'(t_1,1)\cdots(t_m,m)z''$ and $x_\beta u_{\beta+1}z'$, $x_\beta v_{\beta+1}z'$ are reduced.

In the case 1) we have

$$\xi(u_\beta) = \xi(x't_1z',i_\beta) = \xi(v_\beta)$$

which implies $\xi(u_o) = \xi(v_o)$ by 2.8.

In the case 2) we have

$$\xi(u_\beta) = \xi(\bar{u}_\beta),\ \xi(v_\beta) = \xi(\bar{v}_\beta),$$
$$|\bar{u}_\beta| < |u_\beta|,\ |\bar{v}_\beta| = |v_\beta|,$$

where

$$\bar{u}_\beta = (x_\beta x_{\beta+1}u_{\beta+2}z_{\beta+1}z',i_\beta),\quad \bar{v}_\beta = (x_\beta x_{\beta+1}v_{\beta+2}z_{\beta+1}z',i_\beta)$$

and the conclusion follows by induction.

In the case 3) we have the same situation as in 2) where

$$\bar{u}_\beta = (x_\beta u_{\beta+1}z't_1z'',i_\beta),\quad \bar{v}_\beta = (x_\beta u_{\beta+1}z't_1z'',i_\beta).$$

This completes the proof of 2.11.

As a corollary from 2.8 we obtain the following proposition:

2.12. If $u,v\in\bar{Q}$ are such that $u \vdash_1 v$, then $\xi(u) = \xi(v)$.

To complete the proof of Lemma 2 we need the following proposition:

2.13. Let $u,v\in\bar{Q}$ and $u \vdash_2 v$. If $\xi(u)\in Q'$ or $\xi(v)\in Q'$, then $\xi(u) = \xi(v)$.

Proof: From $u \vdash_2 v$ it follows that there exist an $\alpha \geq 0$, $u_\lambda, v_\lambda \in \bar{Q}$ such that

$u = u_o,\quad v = v_o$

$u_\lambda = (x_\lambda u_{\lambda+1}z_\lambda,i_\lambda),\quad v_\lambda = (x_\lambda v_{\lambda+1}z_\lambda,i_\lambda),\quad 0 \leq \lambda < \alpha$

$u_\alpha = (x_\alpha yz_\alpha,i_\alpha),\quad v_\alpha = (x_\alpha(y,1)\cdots(y,m)z_\alpha,i_\alpha).$

By the same arguments as in the proof of 2.11 we can assume that:

a) $\xi(y) = y$, $\xi(x_\lambda) = x_\lambda$, $\xi(z_\lambda) = z_\lambda$, for every λ;

b) x_λ is reduced for every λ.

If $\xi(y,\nu)\notin Q'$ or $\xi(y,\nu) = (y,\nu)$ then by 2.10 we have $\xi(u_\alpha) = \xi(v_\alpha)$, and, by 2.8, $\xi(u) = \xi(v)$.

Thus we can assume that $\xi(y,\nu) = (b_1^{m+p},\nu)\in Q'$ and $\xi(y,\nu) \neq (y,\nu)$

Let y be reducible and let $y = y'(y_1,1)\cdots(y_m,m)y''$, where y' is reduced. Then, $x_\alpha y'$ is reduced, for if it were reducible, then we would have

$$x_\alpha = x'(t_1,1)\cdots(t_{\gamma-1},\gamma-1),\quad y' = (t_\gamma,\gamma)\cdots(t_m,m)y''',\ \gamma \geq 2,$$

but this is impossible by 2.9.

Thus we have:

$$\xi(u_\alpha) = \xi(\bar{u}_\alpha),\quad \xi(v_\alpha) = \xi(\bar{v}_\alpha)$$

where

$$\bar{u}_\alpha = (x_\alpha y'y_1y''z_\alpha,i_\alpha),\quad \bar{v}_\alpha = (x_\alpha(y'y_1y'',1)\cdots(y'y_1y'',m)z_\alpha,i$$

and this implies there exist $\bar{u},\bar{v}\in\bar{Q}$ such that

$$\xi(u) = \xi(\bar{u}),\quad \xi(v) = \xi(\bar{v}),\quad |\bar{u}| < |u|,\ |\bar{v}| < |v|,\quad \bar{u} \vdash_2 \bar{v}.$$

Thus, the conclusion follows by induction.

Therefore we can assume that y is reduced. Then $\xi(y,\nu)\in Q'$, $\xi(y,\nu) \neq (y,\nu)$ is possible only if $y = a_1^{m+p+sq}$, $s \geq 1$. If $[a_1^{m+p+sq}] = (b_1^{m+p})$ in $(Q;[\ ])$, and if we put

$$\bar{v}_\alpha = (x_\alpha b_1^{m+p}z_\alpha,i_\alpha)$$
$$\bar{v}_\lambda = (x_\lambda \bar{v}_{\lambda+1}z_\lambda,i_\lambda)$$

we obtain that $\xi(v) = \xi(\bar{v}_o)$, and by 2.11 we have $\xi(u) = \xi(\bar{v}_o)$.

This completes the proof of 2.13.

Finally conclude that (i) of Lemma 2 is a corollary of 2.5 b), and (ii) is a corollary of 2.12 and 2.13.

3. We make a few more remarks.

The (m+1,m)-semigroup (P;[ ]), obtained in 1, has a universal property of this kind:

If (P′;[ ]′) is any (m+1,m)-semigroup, such that $Q \subseteq P'$ and

$$[a_1^{m+p+q}] = (b_1^{m+p}) \text{ in } (Q;[\ ]) \iff$$

$$\iff [a_1^{m+p+q}]' = [b_1^{m+p}]' \text{ in } (P';[\ ]')$$

for all $a_\nu, b_\nu \in Q$, then there exists a unique homomorphism $\xi:(P;[\ ]) \to (P';[\ ]')$, such that $\xi(a)=a$ for all $a \in Q$.

It should be noted that when Theorem 1′ and Theorem 2 are considered, the (m+k,m)-semigroup used there has not this universal property. Nevertheless, by slightly modified construction of $\overline{Q}$, one can get an (m+k,m)-semigroup with wanted universal property. Namely, we first construct the absolutely free vector valued algebra $\overline{Q}'$ of type $\{[\ ]^s \mid s \geq 1\}$ freely generated by Q, where $[\ ]^s$ is a symbol for an (m+sk,m)-operation for all $s \geq 1$. Further, we define the relations ρ_1, ρ_2, $\simeq$ in the same manner as in 1. In such a way the obtained (m+k,m)-semigroup (P′;[ ]′) is the wanted universal (m+k,m)-semigroup for the given (m+p+q, m+p)-semigroup (Q;[ ]). We can realize a proof of this fact almost without any changes, but we actually do not need such a proof, since the universal property of (P′,[ ]′) is clear if we have had proved Lemma 1 for k = 1.

REFERENCES

[1] Ǵ.Čupona: Vector valued semigroups, Semigroup Forum, Vol. 26 (1983), 65-74

[2] Ǵ.Čupona, N.Celakoski: Polyadic subsemigroups of semigroups, Alg. Confer. Skopje, 1980, 131-151

[3] D.Dimovski: Free vector valued semigroups, This volume

[4] E.L.Post: Polyadic groups, Trans. of the Amer. Math. Soc. (1940), 208-350

[5] Б.Трпеновски, Ǵ.Чупона: [m,n]-групоиди, Билтен ДМФ СРМ Скопје, 21 (1970), 19-29

Ǵorǵi Čupona
Smile Markovski
Biljana Janeva

Prirodno-matematički fakultet
Gazi Baba b.b. (p.f. 162)
91000 Skopje
Yugoslavia

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

ON D-REGULAR NEAR-RINGS

Vučić Dašić

Abstract. In this paper we define a class of the D-regular near-rings, where D is a defect of distributivity. We consider some properties of the D-regular near-rings which generalize corresponding properties of the regular near-rings.

A left zero-symmetric near-ring R is a set with two binary operations + and . such that:

1° (R,+) is a group (not necessarily abelian)

2° (R,.) is a semigroup

3° The left distributive law holds, i.e.

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

Let R be a near-ring and let (S,.) be a multiplicative subsemigroup of (R,.) whose elements generate (R,+). Denote by D=D(S) the normal subgroup of the group (R,+) generated by the set

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

It was proved in [3] that D is an ideal of R. If S is a proper subset of R, then we say that R is a near-ring with the defect of distributivity D. If we wish to stress the set S of generators, then we write (R,S). Thus, in the near-ring (R,S) with the defect D, every element $r \in R$ can be represented as a finite sum $\sum_i (\pm) s_i$ $(s_i \in S)$ and for all $x,y \in R$, $s \in S$ there exists $d \in D$ such that

$$(x+y)s=xs+ys+d$$

This paper is in final form and no version of it will be submitted for publication elsewhere.

Supported by SIZ for Scientific Research of SRCG.

Specially, if D={o}then R is a distributively generated (d.g) near-ring.

if h:R→R'is a homomorphism of the near-rings (R,S) and (R',S') with the defects D and D'respectively, then we require that (S)h⊆S'. A right ideal A of R is a normal subgroup of (R,+) such that (x+a)y-xy∈A for all x,y∈R, a∈A. A right ideal A of R is an ideal of R if ra∈A for all a∈A, r∈R. An R-subgroup B of R is a subgroup of (R,+) such that br∈B for all b∈B, r∈R. An ideal P of R will be called completely prime if ab∈P implies a∈P or b∈P.

DEFINITION 1. Let R be a near-ring with a defect of distributivity D. We say that R is a D-regular near-ring,if for all x∈R there exists y∈R such that xyx-x∈D.

Examples. 1) Every regular near-ring is D-regular,but not conversely.

2) The near-ring whose additive group is $(Z_6,+)$ and multiplication is defined by the following table (|7|,(34)p.409) is a D-regular near-ring, where D={0,3}, but it is not regular.

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	5	4	3	2	1
2	0	1	2	3	4	5
3	0	0	0	0	0	0
4	0	5	4	3	2	1
5	0	1	2	3	4	5

3. The near-ring $E_\Delta(Z_4)$ of Δ-endomorphismes of the group $(Z_4,+)$ for Δ={0,2}(|4|,Table 1,p.71) with D= $\{f_o,f_3,f_{12},f_{13}\}$is D-regular. This near-ring is not regular.

PROPOSITION 1.a) Every homomorphic image of a D-regular near-ring is again D-regular.

b) A direct sum of D-regular near-rings is a D-regular near-ring too.

Proof.a) The assertion follows from the fact that for a homomorphism h of near-rings R and R'with the defect D and D'respectively, holds (D)h⊆D:

b) The result follows by the definition of D-regular near-rings and by the Theorem 2.3b) of|3|

THEOREM 1. R is a D-regular near-ring, if and only if R/D is a regular near-ring.

Proof.Let R be a D-regular near-ring, then there is a natural near-ring homomorphism π:R→R/D. Since R/D is a d.g. near-ring (|3|, Corollary of Theorem 2.6) it follows by Proposition 1 that R/D is regular.

Conversely, if $\bar{R}$=R/D is regular, then for all $\bar{x}\in\bar{R}$ there exists $\bar{y}\in\bar{R}$ such that $\bar{x}\bar{y}\bar{x}=\bar{x}$. Thus, for all x∈R there exists y∈R such that xyx-x∈D.

DEFINITION 2. We say that an element x of the near-ring R with a defect D is a notrivial D-idempotent, if x^2-x∈D,where x∉D.

Clearly, an element x∈R is a D-idempotent, if and only if x+D is an idempotent in R/D.

COROLLARY 1. Let R be a D-regular near-ring, Then for all x∈R and y∈R such that xyx-x∈D, the elements xy and yx are D-idempotents.

Proof. Since $\bar{R}$=R/D is a regular near-ring, the elements xy+D and yx+D are idempotents in $\bar{R}$, i.e.$(xy)^2$-xy∈D and $(yx)^2$-yx∈D.

DEFINITION 3. A near-ring R with a defect of distributivity D is said to be D-simple if R has not other nontrivial ideals besides D.

Clearly, if R is D-simple, than R/D is a simple near-ring.

DEFINITION 4. Let R be a near-ring R with a defect D. We say that the element x∈R is D-nilpotent if there is a natural number n such that $x^n\in D$ and $x^{n-1}\notin D$. The near-ring R has only trivial D-nilpotent elements if $x^n\in D$ implies x∈D.

It is evident that every nilpotent element x is D-nilpotent in R,if and only if x+D is nilpotent in R/D. A non empty subset A of R is a D-nil subset, if every element in A is D-nilpotent. A D-nil R-subgroup B is nontrivial if B≠D.

By the following corollary we extend the part of the Theorem 2.1. in |5| to a class of D-regular near-rings.

COROLLARY 2. Let R be a D-simple near-ring satisfying the d.c.c. on R-subgroups and with only trivial D-nilpotent elements. Then R is D-regular near-ring.

Proof. A simple near-ring R/D has only trivial nilpotent elements and satisfies the d.c.c. on R-subgroups. By Theorem 2.1.(6) in |5| R/D is a regular near-ring. By using the Theorem 1 it follows that R is D-regular.

The following theorem extends the results of |1|, (Theorem 2) and |6|, (Theorem 4.2) to a class of D-regular near-rings.

THEOREM 2. Let (R,S) be a near-ring with identity and with a defect D. Then R is D-regular, if and only if every principal R-subgroup of R coincides with a principal R-subgroup generated by an D-idempotent.

Proof. Suppose that R is a D-regular near-ring, i.e. for all $x\in R$ there exists $y\in R$ such that $xyx-x\in D$. By Corollary 1, the elements xy and yx are D-idempotent. Clearly, $(xy)R\subseteq xR$. On the other hand, if we write every $r\in R$ as a finite sum $r=\Sigma(\pm s_i)(s_i\in S)$, then we have $xR=(-d+xyx)\ R=xyxR+d'(d,d'\in D)$. Thus, $xR\subseteq(xyx)R\subseteq(xy)R$. Consequently $xR=(xy)R$, where xy is a D-idempotent element in R.

Conversely, let for $x\in R$ $xR=zR$, where $z-z^2\in D$. We need only to show that R is a D-regular near-ring. Since R is with identity, there exist $u,v\in R$ such that $x=zv$ and $z=xu$. Hence, for $v=\Sigma(\pm s_i)(s_i\in S)$ we have

$$x=zv=(d+z^2)v=(d+z^2)\Sigma(\pm s_i),\ (d\in D)$$

$$x=\Sigma\pm(d+z^2)s_i$$

$$x=\Sigma\pm(ds_i+z^2s_i+d_i),\ (d,d_i\in D)$$

$$x=d'+z^2\Sigma(\pm s_i),\ (d',ds_i\in D)$$

$$x-d'+z^2v$$

$$x=d'+zx$$

$$x=d'+xux$$

Thus $x-xux\in D$ and cosequentiy R is a D-regular near-ring.

LEMMA 1. Let R be a near-ring with a defect of distributivity D. A D-idempotent element x is D-nilpotent, if and only if x is a trivial D-nilpotent element.

Proof. Let $x^2-x\in D$, i.e. $x^2=d+x$ for some $d\in D$. Now assume that x is a D-nilpotent element in R. Thus, there is an integer n such that $x^n\in D$. Then, by induction on n, $x^2-x\in D$ implies $x^n-x\in D$. Namely $x^{n+1}=x^{n-1}.x^2=x^{n-1}(d+x)=x^{n-1}.d+x^n$. Assume that the assertion is true for n, i.e. $x^n-x\in D$. Hence, $x^{n+1}=x^{n-1}.d+d_1+x$, where $d,d_1\in D$ and thus $x^{n+1}-x\in D$. Therefore, if x is D-idempotent, i.e. $x^2-x\in D$, then $x^n\in D$ implies $x\in D$.

The following proposition generalizes the Corollary 1 in |1|.

PROPOSITION 2. If R is a D-regular near-ring with identity, then R contains no nontrivial D-nil R-subgroups.

Proof. Asume that B is a nontrivial D-nil R-subgroup. Therefore B contains D-nilpotent elements that are not in D. If $b\in B$ is such an element, then by Theorem 2 there exists a nontrivial D-idempotent c ($c\notin D$) such that $cR=bR$. Since R has an identity so $c=c.1\in bR$, i.e. $c\in B$. Thus, the element c is D-nilpotent. By Lemma 1 it follows that c is a trivial D-nilpotent element, i.e. $c\in D$, a contradiction.

The following result is a modification of IFP property (|7|, p.288).

LEMMA 2. Let R be a near-ring with a defect D. If R has no nontrivial D-nilpotent elements, then $ab\in D$ implies $ba\in D$ and $arb\in D$ for all $r\in R$.

Proof. If $ab\in D$, then $(ba)^n=ba.ba...ba\in D$. But, since R has no nontrivial D-nilpotent elements, it follows $ba\in D$. Also, $(arb)^n=arb.arb...arb$. Since $ba\in D$ and D is an ideal of R, we have $(arb)^n\in D$, i.e. $arb\in D$.

A part of the following thoerem is a generalization of a statement proved by H. Bell in |2|.

THEOREM 3. Let R be a near-ring with a defect $D \neq R$ and having no nontrivial D-nilpotent elements. Then R contains a family of completely prime ideals whose intersection is D. Moreover, if R is a D-regular near-ring, then R/D is a regular d.g. near-ring which is isomorphic to a subdirect sum of division rings

Proof. Since $D \neq R$ there exist multiplicative subsemigroups which do not contain the elements from D. By application of Zorn's Lemma there is a maximal subsemigroup M with respect to excluding the elements of D. Define

$$A_D(M)=\{x \in R / ax \in D \text{ for at least one } a \in M\}$$

We first prove that $A_D(M)$ is an ideal of R. If $u,v \in A_D(M)$, then $au \in D$ and $bv \in D$ for some $a,b \in M$. By Lemma 2 we obtain $abu \in D$ and $abv \in D$, i.e. $ab(u-v) \in D$. Hence $u-v \in A_D(M)$. Also, $a(x+u-x)= =ax+au-ax \in D$ and so $x+u-x \in A_D(M)$ for all $u \in A_D(M)$, $x \in R$. Further for all $u \in A_D(M)$ and $x,y \in R$ we have a $((x+u)y-xy)=(ax+au)y-axy \in D$, because D is an ideal of R. Thus $((x+u)y-xy \in A_D(M)$ and $A_D(M)$ is a right ideal of R. By using Lemma 2 it is easy to show that $A_D(M)$ is a left ideal of R. Consequently, $A_D(M)$ is an ideal of R.

M is the set-theoretic complemet of $A_D(M)$. It suffices to show that $R \setminus M \subseteq A_D(M)$ holds. Namely, if $x \notin M$ then the multiplicative subsemigroup generated by M and x must contain the elements from D. Hence, some finite product containing the elements x and $m \in M$ as at least one factor, belongs to D. By using Lemma 2 we have $(mx)^n \in D$ for some integer n and thus $mx \in D$, i.e. $x \in A_D(M)$.

Now we prove that $\bigcap_M A_D(M)=D$. Every element x in R $(x \notin D)$ does not belong to at least one of the ideals $A_D(M)$. Thus $\bigcap_M A_D(M)=D$. Since $D \subseteq A_D(M)$ for any M, it follows $\bigcap_M A_D(M)=D$

If R is a D-regular near-ring, then by Theorem 1 R/D is regular. By using the Corollary of the Theorem 2.6 in |3| it follows that R/D is a d.g. near-ring. Also, R/D has no nontrivial D-nilpotent elements. From Theorem 1 of |8| we get

that R/D is isomorphic to a subdirect sum of division rings.

DEFINITION 5. A near-ring R with a defect D is a D-subdirect sum of near-rings R_i, if and only if there exist the ideals A_i $(i \in I)$ of R with $\bigcap_{i \in I} =D$ and $R_i \cong R/A_i$ as near-rings.

THEOREM 4. A near-ring R with a defect D is a D-subdirect sum of near-rings R_i, if and only if a d.g. near-ring R/D is a subdirect sum of d.g. near-rings R_i.

Proof. Let R be a D-direct sum of near-rings R_i. Thus there exists a family of ideals A_i of R such that $R_i = R/A_i$ and $\bigcap_i A_i=D$. From this it follows $\frac{\frac{R}{D}}{\frac{A_i}{D}} \cong \frac{R}{A_i} \cong R_i$ and $\bigcap_i \frac{A_i}{D}= D$ becaus $\bigcap_i A_i = D$. Thus $\frac{R}{D}$ is a subdirect sum of near-rings R_i. By using the Corollary of the Theorem 2.6 in |3| we have that R/D and R_i are d.g. near-rings, because $D \subseteq A_i$ for all $i \in I$.

Conversely, if $\frac{R}{D}$ is a subdirect sum of near-rings R_i, then there exist ideals $\frac{A_i}{D}$ of $\frac{R}{D}$ with $\bigcap_i \frac{A_i}{D} = D$ and $R_i \cong \frac{\frac{R}{D}}{\frac{A_i}{D}}$. Since $\frac{\frac{R}{D}}{\frac{A_i}{D}} \cong \frac{R}{A_i}$ we have $R_i \cong \frac{R}{A_i}$. Also $\bigcap_i A_i = D$, because $\bigcap_i \frac{A_i}{D} = D$. Thus R is a D-direct sum of near-rings R_i.

By using the Definition 5, we can extend the Theorem 1 in |8| to a class of D-regular near-rings expressing this result in the form of a D-subdirect sum representation.

THEOREM 5 Let R be a D-regular near-ring with a defect D. Then R is isomorphic to a D-subdirect sum of division rings, if and only if R has no nontrivial D-nilpotent elements.

Proof. Let R be isomorphic to a subdirect sum of division rings R_i, then there is a family of ideals A_i $(i \in I)$ such that $R_i \cong R/A_i$ and $\bigcap_i A_i=D$. Thus $x^n \in D$ implies $x^n \in A_i$ for all $i \in I$. Since R/A_i has no notrivial nilpotent elements, then from $(x+A_i)^n=x^n+A_i \in A_i$ it follows $x+A_i \in A_i$. Hence $x \in A_i$ for all $i \in I$, i.e $x \in D$. Therefore R has no nontrivial D-nilpotent elements.

Conversely, if R has no nontrivial D-nilpotent elements, then R/D is a d.g. near-ring and R/D has no nontrivial nilpotent elements. By Theorem 1 R/D is a regular near-ring. Using Theorem 1 in [8], it follows that R/D is isomorphic to a subdirect sum of division rings R_i. Consequently by Theorem 4, R/D is isomorphic to a D-subdirect sum of division rings R_i.

COROLLARY 3. If R is a D-regular near-ring without nontrivial D-nilpotent elements, then additive commutator of R is contained in D.

Proof. By the Theorem 5 R is isomorphice to a D-subdirect sum of divison rings R_i. Thus, there is a family of ideals A_i such that $\bigcap_i A_i = D$ and $R_i \cong R/A_i$. Hence, the additive group of R/A_i is abelian. Consequently for any A_i the additive commutator of R is contained in A_i i.e it is contained in D.

REFERENCES

1. J. Beidlemen. A note on regular near-rings, Journal of the Indian Math. Soc. 33 (1969),207-210.
2. H.Bell. Near-rings in which each element is a power of itself, Bull.Austral.Math.Soc.vol 2 (1970),363-368.
3. V.Dašić. A defect of distributivity of the near-rings, Math. Balkanica 8:8 (1978), 63-75
4. V.Dašić.D-endomorphis near-rings, Publ.de l'Institut Mathematique 28 (42) 1980,61-75.
5. H.Heatherly, Near-rings without nilpotent elements, Publ.Math.Debrecen, 20(1973) No 3-4, 201-205
6. S.Ligh On regular near-rings, Math. Japonicae 15 (1970), 7-13
7. G.Pilz. Near-rings, North-Holland 1983.
8. G.Szeto. On regular near-rings with no non-zero niplotent elements, Math. Japonicae 19(1974) No 2,65-70.

Institut za matematiku i fiziku
Univerziteta u Titogradu
81000 Titograd,Cetinjski put bb
Jugoslavija

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

FREE VECTOR VALUED SEMIGROUPS

Dončo Dimovski

Abstract. The aim of this paper is to give a combinatorial description of free vector valued semigroups.

0. Vector valued semigroups are defined in [1], where the question about a suitable description of free vector valued semigroups is stated. In this paper we answer this question, i.e. we think the answer is satisfactory. I thank Professor Čupona for the helpfull conversations during the course of this work.

1. Here we recall the necessary definitions and known results. From now on, let n,m be integers, such that $m \geq 2$ and $n - m = k \geq 1$.

Let Q be a nonempty set and $[\,]: Q^n \to Q^m$ a map. (Here, Q^i is the i^{th} product of Q.) Then we say that $(Q;[\,])$ is an (n,m)-groupoid. If $[\,]((a_1,\ldots,a_n))=(b_1,\ldots,b_m)$ then we set $[a_1^n] = (b_1^m)$, where c_i^j stands for $c_i c_{i+1}\cdots c_j$, if $i \leq j$, and for the "empty sequence" if $i > j$.

We say that an (n,m)-groupoid $(Q;[\,])$ is an (n,m)-semigroup if for each $1 \leq j \leq k$, the identity

$$(1.1) \qquad \left[[x_1^n]x_{n+1}^{n+k}\right] = \left[x_1^j[x_{j+1}^{j+n}]x_{j+n+1}^{n+k}\right]$$

holds in $(Q;[\,])$.

For given (n,m)-groupoid $(Q;[\,])$ and integer $s \geq 1$, an $(sk+m,m)$-groupoid $(Q;[\,]^s)$ is defined by:

$$[\,]^1 = [\,]$$

$$(1.2) \qquad \left[x_1^{(s+1)k+m}\right]^{s+1} \overset{\text{def}}{=} \left[[x_1^n]x_{n+1}^{(s+1)k+m}\right]^s .$$

By taking Q with all the $[\ ]^s$, $s \geq 1$, we get an m-dimensional vector valued algebra $(Q; \{[\ ]^s \mid s \geq 1\})$. The proof of the following fact is by induction.

Proposition 1. An (n,m)-groupoid $(Q; [\ ])$ is an (n,m)-semigroup if and only if for each $r,s \geq 1$, and each $0 \leq j \leq sk$, the identity

$$(1.3) \qquad [x_1^j [y_1^{rk+m}]^r x_{j+1}^{sk}]^s = [x_1^j y_1^{rk+m} x_{j+1}^{sk}]^{s+r}$$

holds in the vector valued algebra $(Q; \{[\ ]^s \mid s \geq 1\})$. ∎

To each (n,m)-groupoid $(Q; [\ ])$ we can associate two universal algebras $(Q; [\ ]_1, \ldots, [\ ]_m)$ and $(Q; \{[\ ]_i^s \mid s \geq 1,\ 1 \leq i \leq m\})$, defined by

$$(1.4) \qquad \begin{aligned} [\ ]_i &= [\ ]_i^1 \\ [x_1^{sk+m}]^s &= (y_1^m) \iff [x_1^{sk+m}]_i^s = y_i \ . \end{aligned}$$

These universal algebras are called component algebras for $(Q; [\ ])$. The definition of (n,m)-semigroups and Proposition 1. imply:

Proposition 2. (A) An (n,m)-groupoid $(Q; [\ ])$ is an (n,m)-semigroup if and only if for each $1 \leq i \leq m$ and each $1 \leq j \leq k$, the identity

$$(1.1') \qquad [[x_1^n]_1 \ldots [x_1^n]_m x_{n+1}^{n+k}]_i = [x_1^j [x_{j+1}^{j+n}]_1 \ldots [x_{j+1}^{j+n}]_m x_{j+n+1}^{n+k}]_i$$

holds in the algebra $(Q; [\ ]_1, \ldots, [\ ]_m)$.

(B) An (n,m)-groupoid $(Q; [\ ])$ is an (n,m)-semigroup if and only if for each $1 \leq i \leq m$, $r,s \geq 1$, $0 \leq j \leq k$, the identity

$$(1.3') \qquad [x_1^j [y_1^{rk+m}]_1^r \ldots [y_1^{rk+m}]_m^r x_{j+1}^{sk}]_i^s = [x_1^j y_1^{rk+m} x_{j+1}^{sk}]_i^{s+r}$$

holds in the algebra $(Q; \{[\ ]_i^s \mid s \geq 1,\ 1 \leq i \leq m\})$. ∎

2. The fact that the (n,m)-groupoids can be characterised by the associated component algebras, allows us to translate all the notions from the universal algebras to the class of (n,m)-groupoids. It is clear that each of these notions can be defined directly for the (n,m)-groupoids. The same is true for the (n,m)-semigroups. Here we do not give explicit formulations of the corresponding definitions.

Proposition 2. implies the following:

Proposition 3. An arbitrary nonempty set B is a basis of a free (n,m)-semigroup, and moreover, B can be thought as a subset of the (n,m)-semigroup. ∎

The Proposition 3. is stated in [2], but a suitable description for free (n,m)-semigroups was not given. The aim of this paper is to give a combinatorial description of free (n,m)-semigroups.

In the following, for a nonempty set X, the set of all finite sequences with elements from X will be denoted by X^*.

Let B be a nonempty set. We define a sequence of sets $B_0, B_1, \ldots, B_p, B_{p+1}, \ldots$ by induction as follows:

$B_0 = B$;

Let B_p be defined, and let C_p be the subset of B_p^* which consists of all elements u_1^{sk+m}, $u_\alpha \in B_p$, $s \geq 1$. Define B_{p+1} to be $B_p \cup C_p \times \mathbb{N}_m$, where $\mathbb{N}_m = \{1,2,\ldots,m\}$.

Let $\overline{B} = \bigcup_{p \geq 0} B_p$.

Then $u \in \overline{B}$ if and only if $u \in B$ or $u = (u_1^{sk+m}, i)$ for some $u_\alpha \in \overline{B}$, $s \geq 1$, $i \in \mathbb{N}_m$.

Remark. By giving different "names" to the elements in B, we may assume that for each p, $C_p \times \mathbb{N}_m \cap B = \emptyset$, and B_p^* does not contain elements of the form u_1^r, $r \geq 2$, $u_\alpha \in B_p$.

Define a length for elements of $\overline{B}$, i.e. a map $|\ |: \overline{B} \longrightarrow \mathbb{N}$, ($\mathbb{N}$- the set of positive integers) as follows:

If $u \in B$ then $|u| = 1$;

If $u = (u_1^{sk+m}, i)$ then $|u| = |u_1| + |u_2| + \ldots + |u_{sk+m}|$.

By induction on the length we are going to define a map $\varphi: \overline{B} \longrightarrow \overline{B}$. For $b \in B$, let $\varphi(b) = b$. Let $u \in \overline{B}$ and suppose that for each $v \in \overline{B}$ with $|v| < |u|$, $\varphi(v) \in \overline{B}$, and

$$(2.1) \qquad \text{If } \varphi(v) \neq v \text{ then } |\varphi(v)| < |v|;$$

$$(2.2) \qquad \varphi(\varphi(v)) = \varphi(v) \ .$$

Let $u = (u_1^{sk+m}, i)$. Then, for each α, $\varphi(u_\alpha) = v_\alpha \in \overline{B}$ is defined, $|\varphi(u_\alpha)| \leq |u_\alpha|$ and $\varphi(\varphi(u_\alpha)) = \varphi(u_\alpha)$. Let $v = (v_1^{sk+m}, i)$.

(i) If for some α, $u_\alpha \neq v_\alpha$, then $|v_\alpha| < |u_\alpha|$, and so, $|v| < |u|$. In this case let $\varphi(u) = \varphi(v)$.

Because $|v| < |u|$ it follows that $\varphi(v)$ is defined, and moreover, (2.1) and (2.2) imply that $|\varphi(u)| = |\varphi(v)| \leq |v| < |u|$, $\varphi(u) \neq u$, and $\varphi(\varphi(u)) = \varphi(\varphi(v)) = \varphi(v) = \varphi(u)$.

(ii) Let $u_\alpha = v_\alpha$ for each α. Then $u = v$. Suppose that there is $j \in \{0,1,2,\ldots,sk\}$ and $r \geq 1$, such that $u_{j+\nu} = (w_1^{rk+m}, \nu)$, for each $\nu \in \mathbb{N}_m$, and let t be the smallest such j. In this case, let

$$\varphi(u) = \varphi(u_1^t\, w_1^{rk+m}\, u_{t+m+1}^{sk+m}, i) .$$

Because $|(u_1^t\, w_1^{rk+m}\, u_{t+m+1}^{sk+m}, i)| < |u|$, it follows that $\varphi(u)$ is well defined, and moreover, (2.1) and (2.2) imply that $\varphi(u) \neq u$, $|\varphi(u)| < |u|$ and $\varphi(\varphi(u)) = \varphi(u)$.

(iii) If $\varphi(u)$ can not be defined by (i) or (ii), let $\varphi(u) = u$. In this case, $\varphi(\varphi(u)) = \varphi(u) = u$ and $|\varphi(u)| = |u|$.

The above discusion and (i), (ii) and (iii) complete the inductive step, and so we have defined a map $\varphi : \overline{B} \longrightarrow \overline{B}$. Moreover, we have proved the following:

Lemma 4. (a) For $b \in B$, $\varphi(b) = b$.
(b) For each $u \in \overline{B}$, $|\varphi(u)| \leq |u|$.
(c) For $u \in \overline{B}$, if $\varphi(u) \neq u$, then $|\varphi(u)| < |u|$.
(d) For each $u \in \overline{B}$, $\varphi(\varphi(u)) = \varphi(u)$. ∎

Next, we have the following lemmas.

Lemma 5. Let $u = (u_1^{sk+m}, i) \in \overline{B}$ and let $v_\alpha = \varphi(u_\alpha)$ for $1 \leq \alpha \leq sk+m$. Then:
(a) $\varphi(u) = \varphi(v_1^{sk+m}, i)$; and
(b) $\varphi(u) = \varphi(u_1^{\alpha-1}\, v_\alpha\, u_{\alpha+1}^{sk+m}, i)$ for each $1 \leq \alpha \leq sk+m$.

Proof. (a) If $u_\alpha = v_\alpha$ for each α, then (a) is obvious. If there is α, such that $u_\alpha \neq v_\alpha$, then (a) follows from (i).

(b) If $u_\alpha = v_\alpha$, then (b) is obvious. If $u_\alpha \neq v_\alpha$ then (b) follows from (a), Lemma 4.(d) and (i). ∎

Lemma 6. Let $u = (u_1^{sk+m}, i)$, $j \in \{0,1,\ldots,sk\}$, and $u_{j+\alpha} = (v_1^{rk+m}, \alpha)$ for some $r \geq 1$ and each $\alpha \in \mathbb{N}_m$. Then

$$\varphi(u) = \varphi(u_1^j\, v_1^{rk+m}\, u_{j+m+1}^{sk+m}, i) .$$

Proof. By induction on the length.

(A) Let $\varphi(u_t) = w_t \neq u_t$ for some $1 \leq t \leq j$ or $j+m+1 \leq t \leq sk+m$, or $\varphi(v_q) = z_q \neq v_q$ for some $1 \leq q \leq rk+m$. Then $\varphi(u)$ is defined by (i) and $\varphi(u) = \varphi(w)$ where $w = (w_1^{sk+m}, i)$, $w_\beta = \varphi(u_\beta)$ for each $1 \leq \beta \leq sk+m$. Because $|w| < |u|$, by induction, and using Lemma 5. (a),

$$\begin{aligned}
\varphi(u) = \varphi(w) &= \varphi(w_1^j (z_1^{rk+m}, 1)\ldots(z_1^{rk+m}, m) w_{j+m+1}^{sk+m}, i) = \\
&= \varphi(w_1^j\, z_1^{rk+m}\, w_{j+m+1}^{sk+m}, i) = \\
&= \varphi(\varphi(u_1)\ldots\varphi(u_j)\varphi(v_1)\ldots\varphi(v_{rk+m})\varphi(u_{j+m+1})\ldots\varphi(u_{sk+m}), i) \\
&= \varphi(u_1^j\, v_1^{rk+m}\, u_{j+m+1}^{sk+m}, i) .
\end{aligned}$$

Above, $\varphi(u_\gamma)$ was denoted by w_γ, and $\varphi(v_\gamma)$ by z_γ.

(B) Let $\varphi(u_\alpha) = u_\alpha$ and $\varphi(v_\beta) = v_\beta$ for each $1 \leq \alpha \leq j$, $j+m+1 \leq \alpha \leq sk+m$ and $1 \leq \beta \leq rk+m$, and let $\varphi(v_1^{rk+m}, \alpha) \neq (v_1^{rk+m}, \alpha)$ for some $1 \leq \alpha \leq m$. Then $\varphi(v_1^{rk+m}, \alpha)$ must be defined by (ii), since $\varphi(v_\beta) = v_\beta$ for each β. So, there is $0 \leq t \leq rk$ such that $v_{t+\nu} = (w_1^{pk+m}, \nu)$ for each $\nu \in \mathbb{N}_m$. By induction, since $|(v_1^{rk+m}, \nu)| < |u|$, we have that $\varphi(v_1^{rk+m}, \gamma) = \varphi(v_1^t\, w_1^{pk+m}\, v_{t+m+1}^{rk+m}, \gamma)$ for each γ. Then, by induction, and using Lemma 5.,

$$\begin{aligned}
\varphi(u) &= \varphi(u_1^j \varphi(v_1^{rk+m}, 1)\ldots\varphi(v_1^{rk+m}, m) u_{j+m+1}^{sk+m}, i) = \\
&= \varphi(u_1^j (v_1^t\, w_1^{pk+m}\, v_{t+m+1}^{rk+m}, 1)\ldots(v_1^t\, w_1^{pk+m}\, v_{t+m+1}^{rk+m}, m) u_{j+m+1}^{sk+m}, i) \\
&= \varphi(u_1^j\, v_1^t\, w_1^{pk+m}\, v_{t+m+1}^{rk+m}\, u_{j+m+1}^{sk+m}, i) = \\
&= \varphi(u_1^j\, v_1^t (w_1^{pk+m}, 1)\ldots(w_1^{pk+m}, m) v_{t+m+1}^{rk+m}\, u_{j+m+1}^{sk+m}, i) = \\
&= \varphi(u_1^j\, v_1^{rk+m}\, u_{j+m+1}^{sk+m}, i).
\end{aligned}$$

Above, we have applied Lemma 6. on w and z where $w = (u_1^j (v_1^t\, w_1^{pk+m}\, v_{t+m+1}^{rk+m}, 1)\ldots(v_1^t\, w_1^{pk+m}\, v_{t+m+1}^{rk+m}, m) u_{j+m+1}^{sk+m}, i)$ and $z = (u_1^j\, v_1^t (w_1^{pk+m}, 1)\ldots(w_1^{pk+m}, m)\, v_{t+m+1}^{rk+m}\, u_{j+m+1}^{sk+m}, i)$; It was possible, since $|w| < |u|$ and $|z| < |u|$.

(C) Let $\varphi(u_\alpha) = u_\alpha$ for each $1 \le \alpha \le sk+m$. Because of the assumption in the Lemma, it is possible to apply (ii). If the given j is the smallest such number, then by (ii) $\varphi(u) = \varphi(u_1^j\, v_1^{rk+m}\, u_{j+m+1}^{sk+m}, i)$.
If not, let t be the smallest such number. Then for each $\gamma \in \mathbb{N}_m$, $u_{t+\gamma} = (z_1^{pk+m}, \gamma)$, and because $t < j$ and $u_{j+\alpha} \neq u_{t+m}$ for each $1 \le \alpha \le m-1$, it follows that $t+m \le j$. Then by induction and (ii),

$$\begin{aligned}\varphi(u) &= \varphi(u_1^t\, z_1^{pk+m}\, u_{t+m+1}^j (v_1^{rk+m},1)\ldots(v_1^{rk+m},m) u_{j+m+1}^{sk+m}, i) = \\ &= \varphi(u_1^t\, z_1^{pk+m}\, u_{t+m+1}^j\, v_1^{rk+m}\, u_{j+m+1}^{sk+m}, i) = \\ &= \varphi(u_1^t (z_1^{pk+m},1)\ldots(z_1^{pk+m},m) u_{t+m+1}^j\, v_1^{rk+m}\, u_{j+m+1}^{sk+m}, i) = \\ &= \varphi(u_1^j\, v_1^{rk+m}\, u_{j+m+1}^{sk+m}, i)\ .\end{aligned}$$

Above, we have applied Lemma 6. on $w = (u_1^t z_1^{pk+m} u_{t+m+1}^{sk+m}, i)$ and $w' = (u_1^j v_1^{rk+m} u_{j+m+1}^{sk+m}, i)$; It was possible since $|w| < |u|$ and $|w'| < |u|$. ∎

Now, let $Q = \varphi(\overline{B})$. By Lemma 4.(d),

$$Q = \{u \mid u \in \overline{B},\ \varphi(u) = u\}.$$

Define a map $[\ ]: Q^n \longrightarrow Q^m$, by

(2.3) $\quad [u_1^n] = (v_1^m) \iff v_i = \varphi(u_1^n, i)$ for each $i \in \mathbb{N}_m$.

Because $u_j \in Q$, it follows that $(u_1^n, i) \in \overline{B}$, and so: $\varphi(u_1^n, i) \in Q$ for each $i \in \mathbb{N}_m$. Hence $[\ ]$ is well defined.

Theorem 7. $(Q; [\ ])$ is a free (n,m)-semigroup with a basis B.

Proof. (A) Let $[x_1^j [x_{j+1}^{j+n}]\, x_{j+n+1}^{n+k}] = (a_1^m)$, and $[x_{j+1}^{j+n}] = (b_1^m)$. Then $b_\alpha = \varphi(x_{j+1}^{j+n}, \alpha)$ and $a_i = \varphi(x_1^j\, b_1^m\, x_{j+n+1}^{n+k}, i)$ for each $\alpha, i \in \mathbb{N}_m$. Lemmas 5. and 6. imply that

$$\begin{aligned}a_i &= \varphi(x_1^j (x_{j+1}^{j+n},1)\ldots(x_{j+1}^{j+n},m) x_{j+n+1}^{n+k}, i) = \\ &= \varphi(x_1^{n+k}, i) \quad \text{for each } i \in \mathbb{N}_m\ .\end{aligned}$$

On the other side, let $[[x_1^n] x_{n+1}^{n+k}] = (c_1^m)$ and $[x_1^n] = (d_1^m)$. Similarly as above, Lemmas 5. and 6. imply that for each $i \in \mathbb{N}_m$, $c_i = \varphi(x_1^{n+k}, i)$, i.e. $a_i = c_i$. Hence, for each $1 \le j \le k$, $[[x_1^n] x_{n+1}^{n+k}] = [x_1^j [x_{j+1}^{j+n}]\, x_{j+n+1}^{n+k}]$, i.e. $(Q; [\ ])$ is an (n,m)-semigroup.

(B) Because $\varphi(b) = b$ for each $b \in B$, it follows that $B \subseteq Q$. Let $u = (u_1^{sk+m}, i) \in Q$, and suppose that for each $1 \le \alpha \le sk+m$, $u_\alpha \in \langle B \rangle$, where $\langle B \rangle$ is the (n,m)-subsemigroup of $(Q; [\ ])$ generated by B. Since $u_\alpha \in \langle B \rangle$, it follows that $[u_1^{sk+m}] = (a_1^m) \in \langle B \rangle^m$, i.e. $a_i \in \langle B \rangle$ for each $i \in \mathbb{N}_m$. But $a_i = \varphi(u_1^{sk+m}, i) = \varphi(u) = u$, since $u \in Q$, i.e. $u \in \langle B \rangle$. Hence, $\langle B \rangle = Q$, i.e. $(Q; [\ ])$ is generated by B. Here we have used (1.2) and Proposition 1.

(C) Let $(G; [\![\ ]\!])$ be an (n,m)-semigroup and let $f: B \longrightarrow G$ be a map. Define a map $g: Q \longrightarrow G$, by induction, as follows: for $b \in B$ let $g(b) = f(b)$; and

$$g(u_1^{sk+m}, i) = x_i \iff (x_1^m) = [\![g(u_1)\ldots g(u_{sk+m})]\!].$$

This map is well defined, since $(u_1^{sk+m}, i) = (v_1^{rk+m}, j)$ for elements from Q implies that $i = j$, $s = r$, and $u_\alpha = v_\alpha$ for each $1 \le \alpha \le sk+m$. Let $h: \overline{B} \longrightarrow G$ be the map $g \circ \varphi$, i.e. $h(u) = g(\varphi(u))$. It is clear that $h|_Q = g$. Now we are going to show by induction, that $h(u_1^{sk+m}, i) = [\![g(u_1)\ldots g(u_{sk+m})]\!]_i$ for each $(u_1^{sk+m}, i) \in \overline{B}$ with $u_\alpha \in Q$. Since $u_\alpha \in Q$, it follows that $\varphi(u_1^{sk+m}, i)$ is not defined by (i).

If $\varphi(u_1^{sk+m}, i) = (u_1^{sk+m}, i)$, then

$$h(u_1^{sk+m}, i) = g(u_1^{sk+m}, i) = [\![g(u_1)\ldots g(u_{sk+m})]\!]_i\ .$$

If $\varphi(u_1^{sk+m}, i) \neq (u_1^{sk+m}, i)$, then $\varphi(u_1^{sk+m}, i)$ is defined by (ii). Let $p = rk+m$ and $u_{j+\gamma} = (v_1^p, \gamma)$ for each $\gamma \in \mathbb{N}_m$. Then

$$\begin{aligned}g(\varphi(u_1^{sk+m}, i)) &= g(\varphi(u_1^j\, v_1^p\, u_{j+m+1}^{sk+m}, i) = \\ &= [\![g(u_1)..g(u_j)g(v_1)..g(v_p)g(u_{j+m+1})..g(u_{sk+m})]\!]_i = \\ &= [\![g(u_1).g(u_j)[\![g(v_1).g(v_p)]\!]g(u_{j+m+1}).g(u_{sk+m})]\!]_i = \\ &= [\![g(u_1)\ldots g(u_j)[\![g(v_1)\ldots g(v_p)]\!]_1 \cdots \\ &\quad ..[\![g(v_1)\ldots g(v_p)]\!]_m g(u_{j+m+1})\ldots g(u_{sk+m})]\!]_i = \\ &= [\![g(u_1)\ldots g(u_j)g(v_1^p,1)\ldots g(v_1^p,m)g(u_{j+m+1})\ldots \\ &\quad \ldots g(u_{sk+m})]\!]_i = \\ &= [\![g(u_1).g(u_j)g(u_{j+1}).g(u_{j+m})g(u_{j+m+1}).g(u_{sk+m})]\!]_i \\ &= h(u_1^{sk+m}, i).\end{aligned}$$

The above implies that g is an (n,m)-homomorphism, since $g([u_1^{k+m}]_i) = g(\varphi(u_1^{k+m},i)) = h(u_1^{k+m},i) = [\![g(u_1)\ldots g(u_{k+m})]\!]_i$, i.e. $g^m([u_1^{k+m}]) = [\![g(u_1)\ldots g(u_{k+m})]\!]$. ∎

Remark 8. From the construction of Q, it follows that $\overline{B}$ is a free algebra with signature $\{[\,]_i^s \mid s \geq 1,\ i \in \mathbb{N}_m\}$ generated by B, where $[\,]_i^s$ denotes an $sk+m$ operation. If $u \in \overline{B}$, then we can say that $\varphi(u)$ is an "irreducible representative" of u. The definition of φ implies that $\varphi(u)$ is obtained from u by a finitely many transformations of type

$$(\ldots(v_1^{rk+m},1)\ldots(v_1^{rk+m},m)\ldots,i) \rightsquigarrow (\ldots v_1^{rk+m}\ldots,i)\ ,$$

and Lemmas 4.,5., and 6. imply that $\varphi(u)$ does not depend on the order of those transformations.

References

[1] G. Čupona, Vector valued semigroups, Semigroup Forum, Vol. 26 (1983) 65-74 .

D. Dimovski
Inst. za Matematika
Prirodno-Matematički Fakultet
P.F. 162
91000 Skopje

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

ON (3,2) - GROUPS

Dončo Dimovski

Abstract. The goal of this paper is to put together some known facts about (3,2)-groups. Some equivalent definition for (3,2)-groups are given. It is mentioned that finite (3,2)-groups do not exist. An elementary proof that finite (3,2)-groups with less than 12 elements do not exist is given. At the end, it is shown that (3,2)-groups do exist, by giving a combinatorial description of a free (3,2)-group without generators. Such a group is countable-infinite.

0. Introduction. Vector valued groups are defined in [1]. Here we focus on vector valued (3,2)-groups. A (3,2)-group is a set G together with a map $[\,]: G^3 \to G^2$ satisfying the following conditions:

(1) $[[xyz]t] = [x[yzt]]$, (associativity); and

(2) For given $a,b,c \in G$, there exist $x,y,z,t \in G$ such that $[axy] = (b,c) = [zta]$ (solvability of equations).

Because of (1) $[[\ldots[[xyz]t]\ldots]u]$ is denoted by $[xyzt\ldots u]$.

In [1], Theorem 4.3 it is stated that a free (3,2)-group is nontrivial, i.e. has more than one element. Although the statement is true, the proof has some gaps. In professor Čupona's seminar at Skopje, we tried to fill up these gaps. In this paper, a combinatorial description of free (3,2)-groups without generators is given, showing that they are nontrivial. Besides this, we give some basic facts, equivalent definitions, and nonexistence conditions for (3,2)-groups.

1. Basic facts. Let $(G,[\ ])$ be a (3,2)-group.

Proposition 1. $(G^2,\cdot)$ where $(x,y)\cdot(z,t) = [xyzt]$, is a group with identity element a pair (e,e). Moreover:

1) $(x,e)\cdot(e,y) = [xeey] = (x,y)$;

2) $[xyz] = [xab] \Leftrightarrow (y,z) = (a,b) \Leftrightarrow [yzx] = [abx]$;

3) For each $x \in G$, there exist unique $y,z \in G$, such that $[xyz] = [yzx] = [zxy] = (e,e)$, and if $x = y$ or $y = z$ or $z = x$, then $x = y = z$; and

4) For each $x \in G$, $[xee] = [eex]$.

The proof of this Proposition is given in [2]. ∎

We denote the pair $[xee]$ by $(\alpha(x),\beta(x))$. This defines maps $\alpha,\beta: G \longrightarrow G$. In this notation, for each $x,y,z \in G$ $[xyz] = [xy\alpha(z)\beta(z)] = [x\alpha(y)\beta(y)z] = [\alpha(x)\beta(x)yz]$. Moreover $[e\alpha(e)\beta(e)] = (e,e) = (\alpha(e),\beta(e))\cdot(\alpha(e),\beta(e))$.

Proposition 2. Let $f: G^2 \longrightarrow G^2$ be the involution $f(x,y) = (y,x)$. Then $(G,[\ ]')$, where $[xyz]' = f([zyx])$, is a (3,2)-group. In the group $(G^2,\circ)$ associated to $(G,[\ ]')$, the pair (e,e) is still the identity element, and $f((x,y)\circ(z,t)) = f(z,t)\cdot f(x,y)$. Moreover, $\alpha' = \beta$ and $\beta' = \alpha$ i.e. $(\alpha'(x),\beta'(x)) = [xee]' = (\beta(x),\alpha(x))$.

Proof. (i) Associativity: $[[xyz]'t]' = [f([zyx])t]' =$
$= f([tf(f([zyx]))]) = f([t[zyx]]) = f([[tzy]x]) =$
$= [xf([tzy])]' = [x[yzt]']'$.

(ii) The solvability of the equations for $[\ ]'$ follows from the solvability of the equations for $[\ ]$ and the fact that f is a bijection.

(iii) The operation $\circ$ on G^2 is defined by $(x,y)\circ(z,t) = [xyzt]' = f(f(z,t)\cdot f(x,y))$. Hence,
$(x,y)\circ(e,e) = f(f(e,e)\cdot f(x,y)) = f((e,e)\cdot f(x,y)) = ff(x,y) =$
$= (x,y)$, and
$[xee]' = f([eex]) = f(\alpha(x),\beta(x)) = (\beta(x),\alpha(x))$. ∎

Proposition 3. If for some $x \in G$ (i) $\alpha(x) = x$, or (ii) $\beta(x) = x$, or (iii) $\alpha(G) \cap \beta(G) \neq \emptyset$, then $|G| = 1$.

Proof. Because of Proposition 2. it is enough to consider only (i) and (iii).

(i) Let $\alpha(x) = x$. Then $[xee] = (\alpha(x),\beta(x)) =$

$= [x\beta(x)ee]$ implies that $[\beta(x)ee] = (e,e)$. Now, for each $z \in G$, $(z,\beta(x)) = [z\beta(x)ee] = [zee] = [eez] = [\beta(x)eez] =$
$= (\beta(x),z)$, implies that $z = \beta(x)$, i.e. $|G| = 1$.

(iii) Let $\alpha(x) = \beta(y)$. Then from $[xee] = (\alpha(x),\beta(x))$ and $[yee] = (\alpha(y),\beta(y)) = (\alpha(y),\alpha(x))$ we have that $(\alpha(y),x) = [\alpha(y)xee] = [\alpha(y)\alpha(x)\beta(x)] = [yee\beta(x)] = (y,\beta(x))$, i.e. $y = \alpha(y)$. Now, (i) implies that $|G| = 1$. ∎

Proposition 4. (1) If $e \in \alpha(\alpha(G))$, then $|G| = 1$.
(2) If for some $x \in G$, $x = \alpha(\alpha(x))$, then $e \in \beta(G)$.
(3) If for some $x \in G$, $x = \beta(\beta(x))$, then $e \in \alpha(G)$.
(4) If $e \in \beta(\beta(G))$, then $|G| = 1$.
(5) If for some $x,y \in G$, $x = \alpha(\alpha(x))$ and $y = \beta(\beta(y))$, then $|G| = 1$.

Proof. (4) follows from (1) and Proposition 2. (3) follows from (2) and Proposition 2. (5) follows from (2), (3) and Proposition 3.(iii).

(1) Let $e = \alpha(\alpha(x))$, i.e. $[\alpha(x)ee] = (e,\beta(\alpha(x))$. Then, $[\beta(\alpha(x))ee] = (e,\alpha(x)) = (\alpha(\beta(\alpha(x))),\beta(\beta(\alpha(x))))$, i.e. $\alpha(G) \cap \beta(G) \neq \emptyset$. Now apply Proposition 3.(iii).

(2) Let $x = \alpha(\alpha(x))$. Then $[xee] = (\alpha(x),\beta(x)) =$
$= [\alpha(x)ee\beta(x)] = [\alpha(\alpha(x))\beta(\alpha(x))\beta(x)] = [x\beta(\alpha(x))\beta(x)]$ implies that $\beta(\alpha(x)) = \beta(x) = e$, i.e. $e \in \beta(G)$. ∎

2. Equivalent definitions of (3,2)-groups. The next Proposition gives an equivalent definition for (3,2)-groups, analogous to the definition of (ordinary) groups via a binary, unary and nullary operations.

Proposition 5. The existence of a (3,2)-group structure on a set G is equivalent to the existence of: maps $[\ ]: G^3 \longrightarrow G^2$ and $g: G \longrightarrow G$, and an element $e \in G$ satisfying the following conditions: (i) The map $[\ ]$ is associative, i.e. $[[xyz]t] = [x[yzt]]$; (ii) $[x[yee]] = (x,y)$; (iii) $g^3 = id_G$; and (iv) $[xg(x)g^2(x)] = (e,e)$. We say that g is the $[\ ]$-inverse map.

Proof. Let $(G,[\ ])$ be a (3,2)-group. Then $[\ ]$ and $e \in G$ (Proposition 1.) satisfy (i) and (ii). For $x \in G$, let $g(x) = y$, where $[xyz] = (e,e)$. Then Proposition 1. implies that (iii) and (iv) are satisfied.

Conversely, let $[\ ]$, g, and $e \in G$ be given, satisfying (i) to (iv). The condition (i) is the associativity for $[\ ]$. Let $a,b,c \in G$. Then $(b,c) = [bcee] = [bcg(a)g^2(a)a] = [eebc] = [ag(a)g^2(a)bc]$ implies that $[axy] = (b,c) = [uva]$ for $(x,y) = [g(a)g^2(a)bc]$ and $(u,v) = [bcg(a)g^2(a)]$. ∎

Proposition 6. The existence of a (3,2)-group structure on a set G is equivalent to the existence of a group structure on G^2 and elements $e,e',\alpha,\beta \in G$ satisfying the following conditions: (1) (e',e) is the identity element in the group G^2; (2) $(x,e)(e',y) = (x,y)$; and (3) $(\alpha,\beta)(x,e) = (e',x)(\alpha,\beta)$.

Proof. Let $(G,[\ ])$ be a (3,2)-group. Then $(G^2,\cdot)$ is a group (Proposition 1.) and $e = e'$, $\alpha = \alpha(e)$, $\beta = \beta(e)$ satisfy (1), (2) and (3).

Conversely, let G^2 be a group and $e,e',\alpha,\beta \in G$ satisfy (1), (2) and (3). Define a map $[\ ]: G^3 \to G^2$ by: $[xyz] = (x,e)(\alpha,\beta)(y,z)$.

Then,
(i) $[xyz] = (x,e)(\alpha,\beta)(y,e)(e',z) =$
$= (x,e)(e',y)(\alpha,\beta)(e',z) = (x,y)(\alpha,\beta)(e',z)$.

(ii) $[[xyz]t] = [xyz](\alpha,\beta)(e',t) =$
$= (x,y)(\alpha,\beta)(e',z)(\alpha,\beta)(e',t) =$
$= (x,e)(e',y)(\alpha,\beta)(\alpha,\beta)(z,e)(e',t) =$
$= (x,e)(\alpha,\beta)(y,e)(\alpha,\beta)(z,t) =$
$= (x,e)(\alpha,\beta)[yzt] = [x[yzt]]$.

(iii) For given $a,b,c \in G$, $[axy] = (b,c) = [uva]$ where $(x,y) = (\alpha,\beta)^{-1}(a,e)^{-1}(b,c)$ and $(u,v) = (b,c)(e',a)^{-1}(\alpha,\beta)^{-1}$. ∎

Proposition 7. The existence of a (3,2)-group structure on a set G is equivalent to the existence of a group structure on a set H and $X \subseteq H$, such that $|X| = |G|$ and each element from H is a unique product of two elements from X.

Proof. Let $(G,[\ ])$ be a (3,2)-group. Define $X = \{(\alpha(x),\beta(x)) \mid x \in G\}$.
Then Proposition 1. implies that each element from the group $(G^2,\cdot)$ is a unique product of two elements from X, and $|X| = |G|$.

Conversely, let H be a group and $X \subseteq H$ satisfies the condition from the Proposition. Then the map $f: X^2 \to H$ defined by $f(x,y) = xy$, is a bijection. Define $[\ ]$ on X by $[xyz] = f^{-1}(xyz)$. Then $[xyz] = f^{-1}(f(x,y)z) = f^{-1}(xf(y,z))$, and so: $[[xyz]t] = f^{-1}(f([xyz])t) = f^{-1}(xyzt) = [x[yzt]]$. Moreover, for given $a,b,c \in X$, $f^{-1}(a^{-1}bc)$, $f^{-1}(bca^{-1}) \in X^2$, and so $[af^{-1}(a^{-1}bc)] = (b,c) = [f^{-1}(bca^{-1})a]$. Hence, $(X,[\ ])$ is a (3,2)-group. Since there is a bijection from X to G, it follows that there is a (3,2)-group structure on G. ∎

Proposition 8. The existence of a (3,2)-group structure on a set G is equivalent to the existence of inclusions $\varphi, \psi: G \to \mathrm{Perm}(G^2)$ satisfying the following conditions:
(1) $\varphi(x)(a,y) = \psi(y)(x,a)$ for each $x,y,a \in G$; and
(2) $\varphi(x) \circ \psi(y) = \psi(y) \circ \varphi(x)$ for each $x,y \in G$, where $\circ$ is the composition of permutations.

Proof. Let $(G,[\ ])$ be a (3,2)-group. Define φ and ψ by $\varphi(x)(a,b) = [xab]$ and $\psi(x)(a,b) = [abx]$. The (3,2)-group structure on G implies that φ and ψ are inclusions from G to $\mathrm{Perm}(G^2)$ and satisfy the conditions (1) and (2).

Conversely, let φ and ψ are given and satisfy (1) and (2). Define $[\ ]: G^3 \to G^2$ by $[xyz] = \varphi(x)(y,z)$. Then (1) implies that $[xyz] = \psi(z)(x,y)$, and (2) implies that $[\ ]$ is associative. For given $a,b,c \in G$, $[axy] = (b,c) = [uva]$, where $(x,y) = (\varphi(a))^{-1}(b,c)$ and $(u,v) = (\psi(a))^{-1}(b,c)$. ∎

3. (Non) Existence conditions for (3,2)-groups. In [2] it is shown that the existence of a (3,2)-group structure on a finite set G, implies that 6 is a divisor of $|G|$ or $|G| = 1$. (Here $|G|$ is the number of elements in G.) The next Proposition gives an elementary proof that on a set with 6 elements there does not exist a (3,2)-group structure. Professor John Thompson provided me with a proof that finite (3,2)-groups do not exist. He proved that if G is a finite group and $X \subseteq G$ such that $XX = \{xy \mid x,y \in X\} = G$ and $|X|^2 = |G|$, then $|G| = 1$. Then we apply Proposition 7. His proof uses group algebras over the field of complex numbers, Wedderburn's theorem, and representations and characters of finite groups.

Proposition 9. A set with 6 elements does not admit a (3,2)-group structure.

Proof. Let $|G| = 6$, and let (e,e) be the identity element in the group $(G^2,\cdot)$. Propositions 3. and 4. imply that $|\{e,\alpha(e),\alpha(\alpha(e)),\beta(e),\beta(\beta(e))\}| = 5$. Proposition 4. implies that $\alpha(\alpha(\alpha(e))) \neq e \neq \beta(\beta(\beta(e)))$, $\alpha(\alpha(\alpha(e)))\neq\alpha(\alpha(e))$, and $\beta(\beta(\beta(e))) \neq \beta(\beta(e))$. Since $\alpha(\alpha(\alpha(e))) \neq \beta(\beta(\beta(e)))$ and $|G| = 6$, it follows that $\alpha(\alpha(\alpha(e))) = \alpha(e)$ or $\beta(\beta(\beta(e)))=\beta(e)$. By Proposition 2. we can assume that $\alpha(\alpha(\alpha(e))) = \alpha(e)$. Then Proposition 4. implies that $\beta(\beta(\beta(e))) \neq \beta(e)$, and so: $G = \{e,\alpha(e),\alpha(\alpha(e)),\beta(e),\beta(\beta(e)),\beta(\beta(\beta(e)))\}$. Now, $\alpha(\alpha(\alpha(e))) = \alpha(e)$ implies that $\beta(\alpha(e)) = \beta(\alpha(\alpha(e))) = e$. If $\beta(\beta(\beta(\beta(e)))) = \beta(\beta(e))$, then Proposition 3. implies that $|G| = 1$. Hence, $\beta(\beta(\beta(\beta(e)))) = \beta(e)$. Then $[eee] = (\alpha(e),\beta(e))$ and $[eee] \neq [ee\beta(\beta(\beta(e)))]$ imply that $\alpha(\beta(\beta(\beta(e))))=\alpha(\alpha(e))$. Now, $[ee\beta(\beta(\beta(e)))]=[\alpha(\alpha(e))\alpha(\beta(e))\alpha(\beta(\beta(e)))\beta(\beta(\beta(e)))]$ implies that $[\alpha(\alpha(e))\alpha(\beta(e))\alpha(\beta(\beta(e)))] = (e,e)$. This, together with $[e\alpha(e)\beta(e)] = (e,e)$ and $\alpha(\alpha(e))\neq e,\alpha(e),\beta(e)$ implies that $\alpha(\beta(e)) \neq e,\alpha(e),\beta(e)$, and since $\alpha(\beta(e))\neq\beta(\beta(e))$, $\alpha(\beta(e)) \neq \beta(\beta(\beta(e)))$, it follows that $\alpha(\beta(e)) = \alpha(\alpha(e))$, and by Proposition 1., $\alpha(\beta(\beta(e))) = \alpha(\alpha(e))$. Now,

$(e,e) = [\alpha(\alpha(e))\alpha(\alpha(e))\alpha(\alpha(e))] =[\alpha(e)e\alpha(e)e\alpha(e)e] =$
$= [e\alpha(e)e\alpha(e)e\alpha(e)]$ implies that $(\beta(e),\beta(e))=(e,\alpha(e))$. ∎

4. Free (3,2)-groups without generators. In this section we give a combinatorial description of a free (3,2)-group without generators, i.e. generated by the empty set $\emptyset$. This group is an initial object in the category of (3,2)-groups, and is countable-infinite.

Let $A_0 = \{e\}$. If A_k, $k \geq 0$ is defined, let

$$A_{k+1} = \{(x_1^n,i) | x_j \in A_k,\ n \geq 3,\ i = 1,2\} \cup A_k \setminus \{(eex,i) | i = 1,2,\ x \in A_k,\ x \neq e\}.$$

Above, x_1^n stands for $x_1x_2\ldots x_{n-1}x_n$.

Let $A = \bigcup_{k=0}^{\infty} A_k$, and let $S(A)$ be the free semigroup generated by A. We say that $x_1^n = a \in S(A)$, $x_j \in A$ has dimension n and write $\dim(a) = n$. Define a length $|a|$ of $a = x_1^n \in S(A)$, $x_j \in A$, by induction, as follows:

$|c| = 1$; $|a| = |x_1^n| = |x_1| + |x_2| + \ldots + |x_n|$; and

$|(x_1^n,i)| = |x_1^n|$. Roughly put, a length of $x \in S(A)$ is the number of appearances of e in x.

Let $S_k = \{x | x \in S(A),\ |x| \leq k\}$.

Define a map $\varphi: S(A) \to S(A)$ by induction on the length, as follows:

(1) $\varphi(e) = e$;

(2) Suppose that φ is defined on S_{k-1}. Let

$M_k = \{x | x \in S(A),\ |x| = k,\ \dim(x) = 1\}$;
$N_k = \{eeu \mid |u| = k-2,\ \dim(u) = 1,\ \varphi(u) = u \neq e\}$;
$R_k = \{u_1^n \mid u_j \in A,\ n \geq 2,\ |u_1^n| = k,\ \varphi(u_j) = u_j\} \setminus N_k$; and
$T_k = S_k \setminus (S_{k-1} \cup M_k \cup N_k \cup R_k)$.

Then $N_k \cap R_k = M_k \cap (N_k \cup R_k) = T_k \cap (N_k \cup R_k \cup M_k) = \emptyset$ and $S_k = S_{k-1} \cup M_k \cup N_k \cup R_k \cup T_k$.

The extension of φ on $S_{k-1} \cup N_k$ is given by

(A) $\varphi(eeu) = uee$.

Next, the extension of φ on $S_{k-1} \cup N_k \cup R_k$ is defined as follows: Let $u_1^n \in R_k$. Define $\varphi(u_1^n)$ to be:

(B.1) $\varphi(\varphi(u_1^{n-1})u_n)$ if $|\varphi(u_1^{n-1})| < |u_1^{n-1}|$;

(B.2) $\varphi(u_1\varphi(u_2^n))$ if $|\varphi(u_2^n)| < |u_2^n|$;

(B.3) v_1^t $(= \varphi(v_1^t))$ if $n = 2$, $u_i = (v_1^t,i)$, $i=1,2$, $t \geq 3$;

(B.4) $\varphi(uv)$ if $n = 4$, $u_1^4 = uvee$, or $u_1^4 = ueev$, or $u_1^4 = eeuv$;

(B.5) ee if $u_1 = (v_1^t,2)$, $u_n = (v_1^t,1)$, $\varphi(v_1^t u_2^{n-1}) = ee$ and $t \geq 3$;

(B.6) u_1^n otherwise.

The next extension of φ on $S_{k-1} \cup N_k \cup R_k \cup T_k$ is given by

(C) $\varphi(u_1u_2\ldots u_n) = \varphi(\varphi(u_1)\varphi(u_2)\ldots\varphi(u_n))$.

At the end, the extension of φ on S_k is given by

(D) $\varphi((u_1^n,i)) = (\varphi(u_1^n),i)$, $n \geq 3$, $i = 1,2$. (Here we use the notation $(u_1u_2,i) = u_i$, $i = 1,2$. It is necessary, because $\dim(\varphi(u_1^n)) \geq 2$ for $n \geq 2$.)

The essential parts in the definition of φ are (A), (B.3), (B.4) and (B.5). The part (A) implies the fact $|xeu| = |eex|$ (Proposition 1. 4)), the part (B.3) implies the associativity, the part (B.4) implies that (e,e) is the identity element in the associated group (Proposition 1.) and the

part (B.5) implies that each x has unique y,z such that [xyz] = (e,e) (Proposition 1. 3)). The other parts are given only because of the technical difficulties in the proof of the following:

Lemma 10. The map φ is well defined and satisfies the following conditions:

1. $\varphi(e) = e$;
2. $\dim(\varphi(x)) = 1$ if and only if $\dim(x) = 1$;
3. $\dim(\varphi(u_1u_2))=2$ if and only if $\varphi(u_1u_2) = \varphi(u_1)\varphi(u_2)$;
4. $\varphi(ecu) = \varphi(u)ee$;
5. $\varphi(uee) = \varphi(u)ee$;
6. $|\varphi(u_1^n)| \leq |u_1^n|$;
7. If $u_1^n \neq ecu$ and $\varphi(u_j) = u_j$, then $|\varphi(u_1^n)| = |u_1^n|$ if and only if $\varphi(u_1^n) = u_1^n$;
8. $\varphi(u_1^n) = \varphi(u_1^{r-1}\varphi(u_r^s)u_{s+1}^n)$ for each $1 \leq r \leq s \leq n$;
9. $\varphi((u_1^n,i)) = (\varphi(u_1^n),i)$ for $n \geq 3$, $i = 1,2$; and
10. $\varphi(u_1^n) = (e,e)$ if and only if $\varphi(u_2^nu_1) = (e,e)$. ∎

The proof of this Lemma, although straightforward by induction on the length, is very long, so we do not give it here. It will appear in a paper about free (n+1,n)-groups.

Let $G = \varphi(A)$. Define maps $g_1,g_2:G \longrightarrow G$ by induction on the length as follows:

(a) $g_i(e) = (ece,i)$, $i = 1,2$;

(b) $g_i((u_1^n,1)) = \varphi((u_1^n,2)g_1(u_n)g_2(u_n)\ldots g_1(u_1)g_2(u_1),i)$; and

(c) $g_i((u_1^n,2)) = \varphi(g_1(u_n)g_2(u_n)\ldots g_1(u_1)g_2(u_1)(u_1^n,1),i)$.

Lemma 11. For each $x \in G$, $\varphi(xg_1(x)g_2(x)) = ee$.

Proof. The following equations, using induction on the length and Lemma 10. imply Lemma 11.

$\varphi(e(eee,1)(ece,2)) = \varphi(eeee) = ee$;

$\varphi((u_1^n,1)g_1((u_1^n,1))g_2((u_1^n,1))) = \varphi(u_1^ng_1(u_n)g_2(u_n)\ldots g_1(u_1)g_2(u_1))$

$= ee = \varphi(g_1(u_n)g_2(u_n)\ldots g_1(u_1)g_2(u_1)u_1^n) =$

$= \varphi(g_1((u_1^n,2))g_2((u_1^n,2))(u_1^n,2)) =$

$= \varphi((u_1^n,2)g_1((u_1^n,2))g_2((u_1^n,2)))$. ∎

Define a map $[\,]:G^3 \longrightarrow G^2$ by

$[uvw] = (\varphi(uvw,1),\varphi(uvw,2))$.

Theorem 12. $(G,[\,])$ is a free (3,2)-group generated by the empty set ϕ.

Proof. (i) $[[uvw]z] = [\varphi(uvw,1)\varphi(uvw,2)\,z] =$

$= (\varphi(uvwz,1),\varphi(uvwz,2)) = [u\varphi(vwz,1)\varphi(vwz,2)] = [u[vwz]]$.

(ii) Let $a,b,c \in G$. Then $[ax_1x_2] = (b,c) = [y_1y_2a]$, where $(x_1,x_2) = [g_1(a)g_2(a)bc]$ and $(y_1,y_2) = [bcg_1(a)g_2(a)]$.

(iii) Let $(G',[\,]')$ be a (3,2)-group, (e',e') the identity element in the associated group, and $g':G' \longrightarrow G'$ the $[\,]'$-inverse map. Define $f:G \longrightarrow G'$ by induction on the length as follows: $f(e) = e'$; $f((u_1^n,i)) = a_i$, $i = 1,2$, $n \geq 3$ and $(a_1,a_2) = [f(u_1)f(u_2)\ldots f(u_n)]'$. The map f is well defined, and the proof that f is a (3,2)-homomorphism, i.e. $(f,f)([xyz]) = [f(x)f(y)f(z)]'$, is by induction on the length and using Lemma 10. Moreover, f is a unique (3,2)-homomorphism from $(G,[\,])$ to $(G',[\,]')$.

Remark 13. Since $(G,[\,])$ is a (3,2)-group and $[xg_1(x)g_2(x)] = (e,e)$, it follows that $g = g_1$ is the $[\,]$-inverse map.

Remark 14. The set G is infinite (countable). For example, $u_n = (u_{n-1}ee,1)$, $u_1 = e$, $n > 1$, is a sequence of distinct elements in G.

References

[1] G. Čupona, Vector valued semigroups, Semigroup Forum, Vol. 26 (1983) 65-74.

[2] D. Dimovski, Some existence conditions for vector valued groups, God. Zbor. na Mat. Fak., 33-34, (1982-1983), Skopje, 99-103.

D. Dimovski
Inst. za Matematika
Prirodno-Matematički Fakultet, P.F. 162
91000 Skopje

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

MODAL DUALITY THEORY

Kosta Došen

Abstract. This talk is about some results concerning the duality between modal algebras and frames. The presentation of these results is preceded by an introductory part, in which an assessment is made of modal logic in the light of contemporary research. There the generality of this research is stressed, and it is to illustrate this generality that attention is focused on modal duality theory, one of the most abstract areas of modal logic.

Introduction

Modal logic is the general theory of unary propositional operators. This is not a definition one is likely to find in textbooks. Neither is it a definition applicable to modal logic from the beginning of its history in the twentieth century. A change of subject occurred in modal logic in the sixties, with the advent of formidable model-theoretic tools. Before, modal logicians studied particular systems, which were meant to formalize the notions of necessity and possibility, and they produced a real jungle of such systems. After the sixties, modal logicians were increasingly less concerned with particular systems, and concentrated their attention on methods with which they could deal with whole classes of systems. These classes cover the more traditional systems of modal logic, but they include also many things whose connexion with necessity and possibility, in spite of some family resemblances, is at best remote. Nowadays, particular systems in works of modal logic often occur only as examples, to make

---

This paper is in final form and no version of it will be submitted for publication elsewhere.

this or that technical point, and for no other purpose.

Another change of direction of research occurred in the seventies. Now the point was not so much the development of tools to deal with this or that particular system, or even with whole classes of systems: the model-theoretic tools themselves became an object of study. Of course, the abstract study of models can have repercussions on their development for eventual application. However, as it happens often in mathematics, this application is not the main inspiration: the abstract study of models is motivated by independent mathematical interest.

It is because of this concern with whole classes of systems, and with the abstract study of models, that we claim that modal logic is the general theory of unary propositional operators.

What are the unary propositional operators modal logic deals with? We said these are not anymore only the traditional operators "it is necessary that", and its dual, "it is possible that". The search for a single system formalizing these operators has probably come to an end. There is no such single system. The two operators above can have a variety of meanings, depending on the context they are used in. What modal logic can give us are tools to deal with practically any of these particular meanings.

Because of this vagueness in the meaning of "it is necessary that", the study of this operator was replaced by the study of unary operators whose meaning is similar, but more precise - and also more interesting for mathematics. It seems safe to say that "it is necessary that" is not anymore the central unary operator of modal logic. If there is such a central operator, then that would be "it is provable that".

Again, this is not a claim one is likely to find in textbooks, but a number of facts could substantiate this claim.

First, the best known modal logics are S4, S5, and some logics in their vicinity. Already on an intuitive level, the connexion between these logics and provability is quite strong (see [Lemmon 1959]). On a more technical level, there is a famous translation of Heyting's logic into S4, or into logics in the vicinity of S4 (cf. [Došen 1986]), and this translation justifies reading S4-like necessity operators as "it is provable that". This translation connects modal logic with topology, and, in particular, with Tarski's Cn operator, which is of a topological inspiration (see references in [Czelakowski & Malinowski 1985]). Why this translation works could be realized from the Gentzen-style syntactical analysis of S4 and S5 in [Došen 1985] and [Došen 1986a] (cf. [Scott 1971]). Note that this analysis finds a connection with provability for S5, and S5-like logics, as well.

The central role of provability in modal logic could also be substantiated by the very great success of the modal analysis of Gödel's arithmetical provability predicate (see [Boolos 1979]), which also involves logics in the vicinity of S4.

But, there are many more unary operators besides "it is provable that" modal logic is able to deal with. Some of the most famous are: "it will always be the case that", "it is known that" and "it is obligatory that". These unary operators are studied in branches of modal logic which are called respectively: tense logic, epistemic logic and deontic logic. Recently, a new branch of modal logic, called dynamic logic, has developed around the study of operators drawn from computer science, like the operator "after every computation according to the programme P it is true that".

The binary propositional connectives studied by modal logic, like the connective of strict implication, are definable in terms of nonmodal connectives and unary modal operators. Nowadays, these binary connectives are very seldom taken as primitive, as modal logic has increasingly become conscious of its vocation to study unary operators.

Modal logic deals mainly with propositional systems. This is to be expected of a theory concerned with unary propositional operators. To consider these operators together with quantifiers often complicates matters, and prevents results to be stated sharply. In a certain sense, quantifiers too are unary propositional operators, but, of course, the apparatus of binding of variables makes them fall out of the field of propositional logic (see, however, [Kuhn 1980] for an attempt to treat quantifiers as modal operators).

Is modal logic able to deal with arbitrary unary propositional operators? Without trying to answer this question with precision, it seems safe to say that the success of modal logic in dealing with particular operators, and the considerable sophistication of its tools, makes it very probable that practically any unary operator for which some axioms are offered could be dealt with. That means, modal logic could try to give models, and answer technical questions concerning completeness, decidability, and the like, with a reasonable chance of success.

This contrasts with the situation we find in the study of nonclassical propositional logics. There is as yet no logical theory able to claim the title of "general theory of binary propositional connectives". Such a theory should cover not only two-valued, or many-valued, or intuitionistic, or relevant connectives, but any connectives we might wish to consider.

The generality of modal logic, though great, is not such that it could not be greater. One limitation comes from a nearly exclusive concern with the interpretation of modal operators found in Kripke semantics:

$$x \models \Box A \Leftrightarrow \forall y(xRy \Rightarrow y \models A),$$
$$x \models \Diamond A \Leftrightarrow \exists y(xRy \ \& \ y \models A).$$

Although there were sporadic attempts to modify this interpretation, like, for example, the following, using an n+1-ary relation R [Jennings, Johnston & Schotch 1980]:

$$x \models \Box A \Leftrightarrow \forall y_1 \ldots \forall y_n (xRy_1 \ldots y_n \Rightarrow (y_1 \models A \text{ or} \ldots \text{or } y_n \models A)),$$

and though there is a well-known more general interpretation called neighbourhood semantics (sometimes also called Scott--Montague semantics), the enormous majority of papers in the central areas of modal logic deals with Kripke semantics. The reasons for that are probably the connexions with relativized quantifiers, the possibility to deal effectively with the main logics around S4 and S5, and the already considerable generality of Kripke semantics itself. Another reason is probably that the great body of papers in the general study of model--theoretic tools deals with Kripke semantics: to change now the object of study would be like changing the rules of chess, and having to revise the bulk of existing chess theory.

Another limitation of contemporary modal logic is the fact that it studies unary operators added to a Boolean basis; i.e., the nonmodal context in which these operators are introduced is classical. This is quite understandable: this logical context is not only the simplest, but presumably the most important. However, a really general theory of unary operators should pay attention to unary operators in nonclassical logics too. A start in the investigation of intuitionistic modal

logic (see [Božić & Došen 1984] and [Došen 1985a]), and relevant modal logic (see [Božić 1983]), seems to have been made. An output of these investigations is the analysis of negation as a modal operator, an analysis suggested by the greater fluidity of negation in nonclassical logics (see [Božić 1983], [Došen 1986b] and [Došen 1986c]). What has not even been started is the analysis of modal logic in some kind of minimal logic. However, the discovery of this minimal logic is probably tied to the creation of a general theory of binary propositional connectives.

Modal model theory may be divided into: completeness theory, which studies completeness problems involving modal systems and various types of models; correspondence theory, which studies the definability of conditions on models by modal formulae, and the other way round; and duality theory, which studies the interconnexions between types of models in a general algebraic setting. In the second part of this talk we shall present some rudiments of modal duality theory, in order to illustrate the abstract level of studies in modern modal logic. The results which we shall discuss are from [Došen 1986d], which develops ideas of [Goldblatt 1976] and [Thomason 1975].

An extensive survey of modal logic, including duality theory, and its interconnexions with other areas of research, can be found in the second volume of the Handbook of Philosophical Logic [Gabbay & Guenthner 1984], and in particular in the first chapter [Bull & Segerberg 1984], and in the fourth chapter [van Benthem 1984]. A useful guide to the modern literature is also [Bull 1982], [Bull 1983] and [Bull 1985]. Basic notions of category theory, which we need in the second part, can be found in the introductory parts of [Pareigis 1970].

Modal algebras and frames

A frame F is a nonempty set C, the carrier of F, together with some associated relations or functions defined over C. We can imagine that a modal model is made out of a frame in two steps: first we spread over the frame a modal algebra, and then we define a valuation on this algebra.

A modal algebra A is a Boolean algebra with an additional unary operation L. If we consider modal logic in a nonclassical setting, the underlying algebra need not be Boolean: it can be a Heyting algebra, or something else. A valuation is a homomorphism v from a propositional language with a modal operator $\Box$ into A so that for formulae φ:

$$v(\Box\varphi) = Lv(\varphi).$$

In modal duality theory valuations don't play an essential role: once we have spread a modal algebra over a frame, valuations are obtained automatically. It is this business of spreading which becomes the main subject.

To spread a modal algebra over a frame means to define it in terms of the frame. The power set $\mathcal{P}C$ of C is of course a Boolean algebra, but we can also consider subalgebras of this power set algebra. The problem is to define in this set Boolean algebras $\mathcal{A}F$ a unary operation L in terms of the relations or functions of the frame F. There are two ways of doing this, which give rise to two distinct types of frames.

First, we have relational frames, where we are given a binary relation $R \subseteq C^2$. In terms of R we can define a successor function $S: C \to \mathcal{P}C$ by $S(x) = \{y: xRy\}$ (the members of S(x) are the successors of x). Conversely, in terms of S we can define R by $xRy \Leftrightarrow y \in S(x)$. So, relational frames and

successor frames amount to the same thing. With such frames F, in the power set algebra, or its subalgebra, $\mathcal{A}F$, for $B \subseteq C$ in $\mathcal{A}F$, we define L by:

$$LB = \{x: S(x) \subseteq B\}.$$

Second, we have neighbourhood frames, where we are given a neighbourhood function $N: C \to \mathcal{P}(\mathcal{A}F)$, the set $\mathcal{A}F$ being a subset of $\mathcal{P}C$. (the set N(x) is the set of neighbourhoods of x). In terms of N we define L by:

$$LB = \{x: B \in N(x)\}.$$

Now, it is clear that, conversely, N can be defined in terms of L by:

$$N(x) = \{B: x \in LB\}.$$

So, a neighbourhood frame is essentially a set modal algebra spread over a carrier. The function N may be taken as defined in terms of L.

Is the same thing true for relational frames, viz. is R always definable in terms of L? The answer is: no. If $\mathcal{A}F$ is the whole power set $\mathcal{P}C$, then, indeed, we have:

$$(1)\quad S(x) = \cap\{B: x \in LB\},$$

or equivalently:

$$xRy \iff \forall B(x \in LB \Rightarrow y \in B).$$

However, if $\mathcal{A}F$ is not the whole power set $\mathcal{P}C$, but a proper subalgebra of $\mathcal{P}C$, then we may have:

$$S(x) \subsetneq \cap\{B: x \in LB\}.$$

The problem is S(x) need not be an element of $\mathcal{A}F$: if it were, we would have (1). So, we distinguish a subtype of relational frames where (1) holds: we call these frames reducible frames.

The question from which modal duality theory starts is:

for an arbitrary modal algebra A, can we find an isomorphic algebra $\mathcal{A}F$ spread over some frame F? The answer is: yes, there is always such a neighbourhood frame. If the algebra A is normal, i.e. if $L1 = 1$ and $L(b_1 \cap b_2) = Lb_1 \cap Lb_2$, there is always an isomorphic $\mathcal{A}F$ where F is a relational frame.

These answers are usually couched as results in category theory: one establishes duality (categorial equivalence with contravariant functors) between categories of modal algebras and categories of frames. These results of category theory yield much more than an answer to our original question. They induce us to try to translate algebraic theorems (of which we know much more) into theorems about frames. For example, we might try to answer the following: for what constructions on frames are closed classes of frames which correspond to modal algebras which make a variety? What on frames corresponds to homomorphic images, subalgebras, direct products?

Let us sketch how our duality results look like. On the algebraic side let us take the category MA of modal algebras defined by:

objects: modal algebras,
morphisms: homomorphisms,

and the category NMA of normal modal algebras which differs from MA by requiring that its objects be normal modal algebras.

On the frame side we have first the category DF of descriptive neighbourhood frames defined by:

objects: descriptive neighbourhood frames,
morphisms: frame morphisms.

We shall define descriptive neighbourhood frames together with a functor $\mathcal{F}$ which will associate with every modal algebra A a frame $\mathcal{F}A$ spread over A, and with every homomorphism h

between modal algebras a frame morphism $\mathcal{F}h$. If A is a modal algebra, $\mathcal{F}A$ will have a carrier C^A made of all ultrafilters of A, and if for an element b of A we have $q(b) = \{X \in C^A: b \in X\}$, then $N^A(X) = \{q(b): \mathrm{L}\, b \in X\}$. The mapping q is an isomorphism from A to $\mathcal{A}(\mathcal{F}A)$, as in Stone's Representation Theorem. Now, dually, we define a mapping $p: C \to \mathcal{P}(\mathcal{P}C)$ by $p(x) = \{B: x \in B\}$, where B is in $\mathcal{A}F$. A frame is descriptive iff p is one-one and onto.

The frame morphisms of DF are defined as follows. If $f: C_1 \to C_2$ and $(\mathcal{A}f)(B_2) = \{x_1: f(x_1) \in B_2\}$, then f is a frame morphism iff for every B_2 in $\mathcal{A}F_2$:

(i) $(\mathcal{A}f)(B_2) \in \mathcal{A}F_1$,

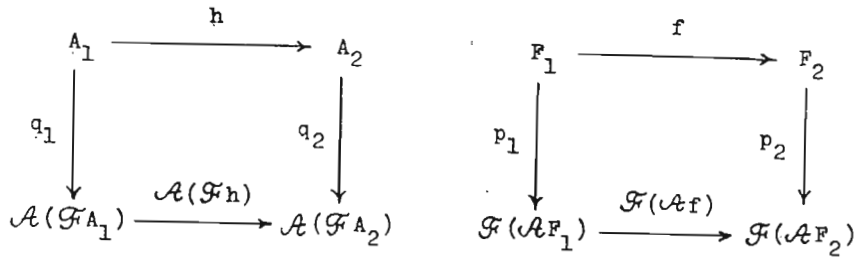
(ii) $(\mathcal{A}f)(B_2) \in N_1(x_1) \Leftrightarrow B_2 \in N_2(f(x_1))$.

A frame morphism is a frame isomorphism iff f is one-one and onto, and f^{-1} is also a frame morphism (which is not automatically satisfied). The mapping p defined above is a frame isomorphism from a descriptive F to $\mathcal{F}(\mathcal{A}F)$. Now, if $h: A_1 \to A_2$ is a homomorphism, we define the frame morphism $\mathcal{F}h: C^{A_2} \to C^{A_1}$ by $(\mathcal{F}h)(X_2) = \{b_1: h(b_1) \in X_2\}$. So, we have completely defined the functor $\mathcal{F}$ from categories of modal algebras into categories of frames. In the same way, $\mathcal{A}$ is a functor from categories of frames into categories of modal algebras. The functors $\mathcal{A}$ and $\mathcal{F}$ are contravariant.

It is possible to establish the following theorem:

THEOREM 1. The categories MA and DF are dual by the functors $\mathcal{A}$ and $\mathcal{F}$.

This theorem means that the following diagrams commute:



A neighbourhood frame F is a filter frame iff for every $x \in C$ we have that N(x) is a filter (not necessarily proper) of $\mathcal{A}F$. The category DFF is defined by the following:

objects: descriptive filter frames,

morphisms: frame morphisms.

We can prove the following:

THEOREM 2. The categories NMA and DFF are dual by the functors $\mathcal{A}$ and $\mathcal{F}$.

Reducible relational frames are intertranslatable not with filter frames, but with a slightly more restrictive type of neighbourhood frames, which we call hyperfilter frames; for every B in $\mathcal{A}F$ these frames satisfy:

$$\bigcap N(x) \subseteq B \Rightarrow B \in N(x).$$

(Note that this does not entail that for every x the set N(x) is a complete filter, i.e. it does not entail that $\bigcap N(x) \in N(x)$, since $\bigcap N(x)$ need not belong to $\mathcal{A}F$.) A hyperfilter frame is always a filter frame, but for infinite frames we don't necessarily have the converse. A reducible frame becomes a hyperfilter frame with the following definition of N:

$$N(x) = \{B: S(x) \subseteq B\},$$

where B is in $\mathcal{A}F$. Conversely, a hyperfilter frame becomes a reducible frame with the following definition of S:

$$S(x) = \bigcap N(x).$$

Frame morphisms on descriptive hyperfilter frames can equivalently be defined by replacing (ii) by:

$$(ii')\ S_2(f(x_1)) = \{f(x_2): x_2 \in S_1(x_1)\}.$$

Although not every filter frame is a hyperfilter frame, every descriptive filter frame is a hyperfilter frame. So, descriptive filter frames are intertranslatable with descriptive reducible frames. Our Theorem 2 then amounts to a result of [Goldblatt 1976] which establishes duality between NMA and the category of descriptive reducible frames with frame morphisms.

Let us now consider the frames F of a more usual kind, where $\mathcal{A}F$ is the whole power set algebra. We shall call such frames full. What categories of modal algebras are dual with categories of full frames? An answer is provided by the following.

Let CAA be the category:

objects: complete atomic modal algebras,
morphisms: complete homomorphisms,

and let FNF be the category:

objects: full neighbourhood frames,
morphisms: frame morphisms.

The functor $\mathcal{G}$ from CAA to FNF is defined by the following. If A is an object of CAA, then for the frame $\mathcal{G}A$ we have:

$$C^A = \{a: a \text{ is an atom of } A\},$$

$$N^A(a) = \{Z \subseteq C^A: a \leqslant L \cup Z\}.$$

If $h: A_1 \to A_2$ is a complete homomorphism, then the frame morphism $\mathcal{G}h: C^{A_2} \to C^{A_1}$ is defined by $(\mathcal{G}h)(a_2) = a_1 \Leftrightarrow a_2 \leqslant h(a_1)$. Then we can prove the following:

THEOREM 3. The categories CAA and FNF are dual by the functors $\mathcal{A}$ and $\mathcal{G}$.

If NCAA differs from CAA by requiring moreover that its objects be normal modal algebras, and FFNF differs from FNF by requiring moreover that its objects be filter frames, we can prove:

THEOREM 4. The categories NCAA and FFNF are dual by the functors $\mathcal{A}$ and $\mathcal{G}$.

Full relational frames, which are always reducible, are intertranslatable with full hyperfilter frames, as above. Full relational frames are the usual Kripke frames for modal logic.

Let now CCAA be the category which differs from CAA by requiring moreover that its objects be modal algebras which satisfy:

$$L \cap \{b_i: i \in I\} = \bigcap \{L\, b_i: i \in I\}.$$

These modal algebras are normal. Next, let HFNF be the category which differs from FNF by requiring moreover that its objects be hyperfilter frames (in these frames for every x we now have that N(x) is a complete filter). The following theorem, with which we conclude this lecture, can be derived from [Thomason 1975]:

THEOREM 5. The categories CCAA and HFNF are dual by the functors $\mathcal{A}$ and $\mathcal{G}$.

REFERENCES

J. van Benthem 1984, Correspondence theory, in [Gabbay & Guenthner 1984], pp.167-247.

G. Boolos 1979, The Unprovability of Consistency, Cambridge University Press, Cambridge.

M. Božić 1983, A Contribution to the Semantics of Relevant Logics (in Serbo-Croatian), doctoral dissertation, University of Belgrade, Belgrade.

M. Božić & K. Došen 1984, Models for normal intuitionistic modal logics, Studia Logica 43, pp.217-245.

R.A. Bull 1982, Review of papers by Fine, Goldblatt, Lachlan, Thomason and van Benthem, The Journal of Symbolic Logic 47, pp.440-445.

R.A. Bull 1983, Review of papers by Blok, Fine, Gerson, Šehtman, Thomason and van Benthem, The Journal of Symbolic Logic 48, pp.488-495.

R.A. Bull 1985, Review of papers by Esakia, Fine and Meskhi, The Journal of Symbolic Logic 50, pp.231-234.

R.A. Bull & K. Segerberg 1984, Basic modal logic, in [Gabbay & Guenthner 1984], pp.1-88.

J. Czelakowski & G. Malinowski 1985, Key notions of Tarski's methodology of deductive systems, Studia Logica 44, pp.321-351.

K. Došen 1985, Sequent-systems for modal logic, The Journal of Symbolic Logic 50, pp.149-168.

K. Došen 1985a, Models for stronger normal intuitionistic modal logics, Studia Logica 44, pp.39-70.

K. Došen 1986, Modal translations and intuitionistic double negation, Logique et analyse (to appear).

K. Došen 1986a, Higher-level sequent-systems for intuitionistic modal logic, Publications de l'Institut Mathématique (Belgrade) N.S. 39(53), pp. 3-12.

K. Došen 1986b, Negation as a modal operator, Reports on Mathematical Logic (to appear).

K. Došen 1986c, Negation and impossibility, in J. Perzanowski (ed.), Essays on Logic and Philosophy, Jagiellonian University, Cracow (to appear).

K.Došen 1986d, Duality between modal algebras and neighbourhood frames (to appear)

D.M. Gabbay & F. Guenthner 1984, Handbook of Philosophical Logic, vol.II: Extensions of Classical Logic, Reidel, Dordrecht.

R.I.Goldblatt 1976, Metamathematics of modal logic, Reports on Mathematical Logic 6, pp.41-78; 7, pp.21-52.

R.E. Jennings, D.K. Johnston & P.K. Schotch 1980, Universal first-order definability in modal logic, Zeitschrift für mathematische Logik und Grundlagen der Mathematik 26, pp.327-330.

S.T. Kuhn 1980, Quantifiers as modal operators, Studia Logica 39, pp.145-158.

E.J. Lemmon 1959, Is there only one correct system of modal logic? , Proceedings of the Aristotelian Society Suppl. 33, pp.23-40.

B. Pareigis 1970, Categories and Functors, Academic Press, New York.

D.S. Scott 1971, On engendering an illusion of understanding, The Journal of Philosophy 68, pp.787-807.

S.K. Thomason 1975, Categories of frames for modal logic, The Journal of Symbolic Logic 40, pp.439-442.

Matematički Institut
Knez Mihailova 35
11000 Beograd
Yugoslavia

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

ON HOMOTOPIES OF n-ARY GROUPOIDS WITH DIVISION

Ivo Đurović

Abstract. The properties of homotopic mappings of binary groupoids are described in [2]. In this paper some properties of n-ary groupoids with division in regard to homotopies especially in the case when the homotopic image of that groupoid is a n-ary quasigroup are investigated.

Let us first summarize the notations and terminology which we use in this paper.

According to [1] the sequence $a_h, a_{h+1}, \dots, a_m$ is denoted with $(a_i)_{i=h}^{m}$ or briefly with a_h^m. Analogously $(a_i b_i)_{i=h}^{m}$ and $(ab)_h^m$ are designations for the sequence $a_h b_h, a_{h+1} b_{h+1}, \dots, a_m b_m$. The sequence $a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_n$, so-called i-cut of a_1^n is denoted with a_1^{i-1}, a_{i+1}^{n} or $a_1^n \overset{i}{|}$.

Analogously, $(ab)_1^n \overset{i}{|}$ denotes the i-cut of $(ab)_1^n$. The sequences $a_1, \dots, a_{i-1}, c, a_{i+1}, \dots, a_n$ and $a_1 b_1, \dots, a_{i-1} b_{i-1}, c, a_{i+1} b_{i+1}, \dots, a_n b_n$ are denoted with $a_1^n \overset{i}{|} c$ and $(ab)_1^n \overset{i}{|} c$ respectively.

The n-ary groupoid $\langle G, \omega \rangle$ is n-ary groupoid with i-division if and only if for every $\langle a_1^{n+1} \overset{i}{|} \rangle \in G^n$ there exists at least one $x \in G$ such that $\omega \langle a_1^n \overset{i}{|} x \rangle = a_{n+1}$.

The n-ary groupoid $\langle G, \omega \rangle$ is n-ary groupoid with division (briefly Dn-groupoid) if and only if it is n-ary groupoid with i-division for every $i \in J_n = \{1, 2, \dots, n\}$.

The i-class of solutions of Dn-groupoid $\langle G, \omega \rangle$ for $\langle a_1^{n+1} \overset{i}{|} \rangle \in G^n$, $i = 1, 2, \dots, n$, is the set $\overset{i}{[\omega]} \langle a_1^{n+1} \overset{i}{|} \rangle = \{x \in G : \omega \langle a_1^n \overset{i}{|} x \rangle = a_{n+1}\}$.

For every $i \in J_n$ the i-translation of n-ary groupoid $\langle G, \omega \rangle$

This paper is in final form and no version of it will be submitted for publication elsewhere.

by $\langle a_1^n \overset{i}{|} \rangle \in G^{n-1}$ and operation ω is the mapping

$\overset{i}{\boxed{\omega}}\langle a_1^n \overset{i}{|}\rangle : G \to G$, $\overset{i}{\boxed{\omega}}\langle a_1^n \overset{i}{|}\rangle x = \omega\langle a_1^n \overset{i}{|} x\rangle$.

Obviously, every translation of Dn-groupoid is a surjection.

The homotopy of n-ary groupoid $\langle G,\omega\rangle$ into n-ary groupoid $\langle \bar G,\bar\omega\rangle$ is an ordered (n+1)-tuple $\langle \varphi_1^{n+1}\rangle$ of mappings from G into $\bar G$ such that $(\forall \langle x_1^n\rangle \in G^n)\ \varphi_{n+1}\omega\langle x_1^n\rangle = \bar\omega\langle(\varphi x)_1^n\rangle$.

It is well known that a homotopic image of a Dn-groupoid is a Dn-groupoid.

LEMMA 1. Let $\langle G,\omega\rangle$ be Dn-groupoid, let $\varphi_1,\dots,\varphi_{n+1}$ be mappings from the set G onto a set $\bar G$ and let $\bar\omega\langle(\varphi x)_1^n\rangle = \varphi_{n+1}\omega\langle x_1^n\rangle$ for any elements $x_1,\dots,x_n$ of the set G.

$\langle \bar G,\bar\omega\rangle$ is Dn-groupoid if and only if

$$(\forall \langle x_1^n\rangle,\langle y_1^n\rangle \in G^n)\ (\varphi_1 x_1=\varphi_1 y_1 \wedge \dots \wedge \varphi_i x_i=\varphi_i y_i \wedge \dots \wedge \varphi_n x_n=\varphi_n y_n) \Rightarrow \varphi_{n+1}\omega\langle x_1^n\rangle=\varphi_{n+1}\omega\langle y_1^n\rangle. \quad (1)$$

Proof. If $\langle \bar G,\bar\omega\rangle$ is Dn-groupoid, it is easy to verify that (1) holds.

Conversely, if $\langle x_1^n\rangle, \langle y_1^n\rangle \in G$ such that $\varphi_i x_i = \varphi_i y_i$ for every $i \in J_n$ and if (1) holds, then $\varphi_{n+1}\omega\langle x_1^n\rangle = \varphi_{n+1}\omega\langle y_1^n\rangle$ and consequently $\bar\omega\langle(\varphi x)_1^n\rangle = \bar\omega\langle(\varphi y)_1^n\rangle$, which means that $\langle \bar G,\bar\omega\rangle$ is a n-ary groupoid. Since $\langle \bar G,\bar\omega\rangle$ is the homotopic image of the Dn-groupoid $\langle G,\omega\rangle$ by the homotopy $\langle \varphi_1^{n+1}\rangle$ it follows that $\langle \bar G,\bar\omega\rangle$ is Dn-groupoid.

THEOREM 1. Let $\langle \bar G,\bar\omega\rangle$ be a homotopic image of Dn-groupoid $\langle G,\omega\rangle$ by homotopy $\langle \varphi_1^{n+1}\rangle$ and let φ_{n+1} be bijection. $\langle \bar G,\bar\omega\rangle$ is a n-ary quasigroup if and only if

$$(\forall i \in J_n)(\forall \langle a_1^{n+1} \overset{i}{|}\rangle \in G^n)\ x_i, y_i \in \overset{i}{\boxed{\omega}}\langle a_1^{n+1} \overset{i}{|}\rangle \Rightarrow \varphi_i x_i = \varphi_i y_i. \quad (2)$$

Proof. If $\langle \bar G,\bar\omega\rangle$ is a n-ary quasigroup, it is easy to verify that (2) holds.

Conversely, let (2) holds, let a_j be a preimage of $\bar a_j$ for the mapping φ_j for every $j = 1,2,\dots,i-1,i+1,\dots,n$ and let x', x'' be preimages of $\bar x'$, $\bar x''$ for the mapping φ_i. Then

$$\bar\omega\langle \bar a_1^n \overset{i}{|} \bar x'\rangle = \bar\omega\langle \bar a_1^n \overset{i}{|} \bar x''\rangle \Rightarrow \bar\omega\langle(\varphi a)_1^n \overset{i}{|} \varphi_i x'\rangle = \bar\omega\langle(\varphi a)_1^n \overset{i}{|} \varphi_i x''\rangle \Rightarrow \varphi_{n+1}\omega\langle a_1^n \overset{i}{|} x'\rangle = \varphi_{n+1}\omega\langle a_1^n \overset{i}{|} x''\rangle \Rightarrow$$

$$\Rightarrow \omega\langle a_1^n \overset{i}{|} x'\rangle = \omega\langle a_1^n \overset{i}{|} x''\rangle \Rightarrow \varphi_i x' = \varphi_i x'' \Rightarrow \bar x' = \bar x'',$$

which completes the proof.

DEFINITION 1. Let $\langle G,\omega\rangle$ be Dn-groupoid and let $\underset{\sim}{a}_i$, $i=1,2,\dots,n$, where $\underset{\sim}{a}_i = \langle a_{i1},\dots,a_{ii-1},a_{ii+1},\dots,a_{in+1}\rangle$, be any elements of the set G^n.

The set $\{\omega\langle a_1^n\rangle : a_1 \in \overset{1}{\boxed{\omega}}\underset{\sim}{a}_1 \wedge a_2 \in \overset{2}{\boxed{\omega}}\underset{\sim}{a}_2 \wedge \dots \wedge a_n \in \overset{n}{\boxed{\omega}}\underset{\sim}{a}_n\}$ is called (1-n)-product of the classes of solutions $\overset{1}{\boxed{\omega}}\underset{\sim}{a}_1, \overset{2}{\boxed{\omega}}\underset{\sim}{a}_2, \dots, \overset{n}{\boxed{\omega}}\underset{\sim}{a}_n$ of Dn-groupoid $\langle G,\omega\rangle$.

THEOREM 2. For every Dn-groupoid $\langle G,\omega\rangle$ these conditions are equivalent:

U_1: There exists a homotopy $\langle \varphi_1^{n+1}\rangle$, where φ_{n+1} is a bijection, such that the homotopic image $\langle \bar G,\bar\omega\rangle$ of $\langle G,\omega\rangle$ by this homotopy is a n-ary quasigroup,

U_2: $(\exists \langle z_1^n \overset{i}{|}\rangle \in G^{n-1})\ \omega\langle z_1^n \overset{i}{|} x\rangle = \omega\langle z_1^n \overset{i}{|} y\rangle \Rightarrow$

$\Rightarrow (\forall \langle z_1^n \overset{i}{|}\rangle \in G^{n-1})\ \omega\langle z_1^n \overset{i}{|} x\rangle = \omega\langle z_1^n \overset{i}{|} y\rangle$

for every $i \in J_n$.

U_3: Every (1-n)-product of the classes of solutions of Dn-groupoid $\langle G,\omega\rangle$ is an one-element set.

Proof. It is enough to prove that $U_1 \Rightarrow U_2 \Rightarrow U_3 \Rightarrow U_1$.

1° ($U_1 \Rightarrow U_2$). If $\omega\langle z_1^n \overset{i}{|} x\rangle = \omega\langle z_1^n \overset{i}{|} y\rangle$, then by Theorem 1. $\varphi_i x = \varphi_i y$. It follows that for every $\langle z_1^n \overset{i}{|}\rangle \in G^{n-1}$

$$\omega\langle z_1^n \overset{i}{|} x\rangle = \varphi_{n+1}^{-1}\varphi_{n+1}\omega\langle z_1^n \overset{i}{|} x\rangle = \varphi_{n+1}^{-1}\bar\omega\langle(\varphi z)_1^n \overset{i}{|} \varphi_i x\rangle = \varphi_{n+1}^{-1}\bar\omega\langle(\varphi z)_1^n \overset{i}{|} \varphi_i y\rangle = \varphi_{n+1}^{-1}\varphi_{n+1}\omega\langle z_1^n \overset{i}{|} y\rangle = \omega\langle z_1^n \overset{i}{|} y\rangle.$$

2° ($U_2 \Rightarrow U_3$). If $\omega\langle x_1^n\rangle$ and $\omega\langle y_1^n\rangle$ are elements of the (1-n)-product of classes of solutions $\overset{1}{\boxed{\omega}}\underset{\sim}{a}_1, \overset{2}{\boxed{\omega}}\underset{\sim}{a}_2, \dots, \overset{n}{\boxed{\omega}}\underset{\sim}{a}_n$, then $\omega\langle(a_{ij})_{j=1}^n \overset{i}{|} x_i\rangle = \omega\langle(a_{ij})_{j=1}^n \overset{i}{|} y_i\rangle$ for every $i \in J_n$. It follows that for every $i \in J_n$

$$(\forall \langle z_1^n \overset{i}{|}\rangle \in G^{n-1})\ \omega\langle z_1^n \overset{i}{|} x_i\rangle = \omega\langle z_1^n \overset{i}{|} y_i\rangle. \quad (3)$$

From (3), taking for i 1, 2, ..., n successively and moreover substituting $z_1,\dots,z_{i-1}$ with $y_1,\dots,y_{i-1}$ respectively, and $z_{i+1},\dots,z_n$ with $x_{i+1},\dots,x_n$ respectively, one obtains the system of n equations

$\omega\langle y_1^{i-1}, x_i^n\rangle = \omega\langle y_1^i, x_{i+1}^n\rangle$, $i = 1,2,\dots,n$, whence it follows that $\omega\langle x_1^n\rangle = \omega\langle y_1^n\rangle$.

3° $(U_3 \Rightarrow U_1)$. Let $\langle a_1^n\rangle$ be a certain element of G^n and let $\overline{\omega}\left\langle \left(\overline{i\omega}_{\langle a_1^n | i\rangle} z_i\right)_{i=1}^n\right\rangle \overset{def.}{=} \omega\langle z_1^n\rangle$ for every $\langle z_1^n\rangle \in G^n$.

First we verify that the implication

$$\left(\overline{1\omega}_{\langle a_2^n\rangle} x_1 = \overline{1\omega}_{\langle a_2^n\rangle} y_1 \wedge \dots \wedge \overline{i\omega}_{\langle a_1^n | i\rangle} x_i = \overline{i\omega}_{\langle a_1^n | i\rangle} y_i \wedge \right.$$

$$\left. \wedge \dots \wedge \overline{n\omega}_{\langle a_1^{n-1}\rangle} x_n = \overline{n\omega}_{\langle a_1^{n-1}\rangle} y_n\right) \Longrightarrow \omega\langle x_1^n\rangle = \omega\langle y_1^n\rangle \quad (4)$$

holds for every $\langle x_1^n\rangle, \langle y_1^n\rangle \in G^n$.

If $\overline{i\omega}_{\langle a_1^n | i\rangle} x_i = \overline{i\omega}_{\langle a_1^n | i\rangle} y_i$, i.e. $\omega\langle a_1^n | i\, x_i\rangle = \omega\langle a_1^n | i\, y_i\rangle$ for every $i \in J_n$, then x_i and y_i are elements of one and the same i-class of solutions of Dn-groupoid $\langle G, \omega\rangle$ for every $i \in J_n$.

Consequently $\omega\langle x_1^n\rangle = \omega\langle y_1^n\rangle$, i.e. implication (4) holds. Since $\overline{i\omega}_{\langle a_1^n | i\rangle}$, $i = 1,2,\dots,n$, are surjections, it follows by Lemma 1. that $\left\langle \left(\overline{i\omega}_{\langle a_1^n | i\rangle}\right)_{i=1}^n, \varepsilon\right\rangle$, where ε is the identity mapping of the set G, is a homotopy of Dn-groupoid $\langle G, \omega\rangle$ onto Dn-groupoid $\langle G, \overline{\omega}\rangle$. Since for every $i \in J_n$ and for any $\langle a_1^{n+1} | i\rangle \in G^n$

$$x_i, y_i \in \overline{\omega}_{\langle a_1^{n+1} | i\rangle} \Rightarrow \omega\langle a_1^n | i\, x_i\rangle = \omega\langle a_1^n | i\, y_i\rangle \Rightarrow$$

$$\Rightarrow \overline{i\omega}_{\langle a_1^n | i\rangle} x_i = \overline{i\omega}_{\langle a_1^n | i\rangle} y_i,$$

it follows by Theorem 1. that $\langle G, \overline{\omega}\rangle$ is a n-ary quasigroup.

Let us exemplify that there exist Dn-groupoids which satisfy the conditions given in Theorem 2.

Let C^* be the set of all nonzero complex numbers, let $\cdot$ denotes the usual multiplication of complex numbers and let for every $x_1, x_2, \dots, x_n \in C^*$ $\omega\langle x_1^n\rangle \overset{def.}{=} (x_1)^{n_1} \cdot (x_2)^{n_2} \cdot \dots \cdot (x_n)^{n_n}$, where $n_1, n_2, \dots, n_n$ are given natural numbers.

It is easy to verify that $\langle C^*, \omega\rangle$ is Dn-groupoid which satisfies the abovementioned conditions.

REFERENCES

1. V.D. Belousov, Osnovy teorii kvazigrupp i lup, Nauka, Moskva, 1967.

2. N.I. Prodan, Nekotorye voprosy teorii gruppoidov s deleniem, Voprosy teorii kvazigrupp i lup, Štiinca, Kišinev, 1971, 104-110.

Ivo Đurović
Fakultet graditeljskih znanosti
51000 Rijeka
Viktora Cara Emina 5

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

T - k - S E M I N E T S

Radoslav Galić

Abstract. In /1/ J.Aczel (1965) investigates in detail 3-nets to which quasigroups are associated and in 1967. V.Havel /4/ defines 3-seminets with injection to which partial groupoids are associated. M.A. Taylor (1971) in /5/ also defines 3-seminets, but with associated multigroupoids. In the monograph /2/ (1971) V.D. Belousov considered k-nets to which correspond an orthogonal system of quasigroups. J.Ušan (1977) in /6/ defines k-seminets to which correspond special an orthogonal system of partial quasigroups.

In this paper we introduce and investigate T-k-seminets, as a generalization of 3-seminets from /5/, to which partial (k-1)-multigroupoids are associated. The relation between T-k-seminets and k-seminets from /4/ and /6/ is also considered.

Let P be a nonempty set, and $X_1,\ldots X_k$ be mutually disjoint partitions of a set P. The sets X_i, $i \in N_k = \{1,2,\ldots, k\}$, will be called classes, their elements $x_i \in X_i$ will be called blocks, and the elements of P will be called points. We will say that the ordered (k+1)-tuple $N=(P, X_1,\ldots X_k)$ is a T-k-seminet if and only if the following properties hold:

This paper is in final form and no version of it will be submitted for publication elsewhere.

T1. If p is a block, then there is a point $p \in P$ such that $p \epsilon b$.

We say that a k-tuple $x_1,\ldots,x_k$ of blocks in a relation and we write $R(x_1,\ldots,x_k)$ if and only if there is a point $p \in P$ such that $p \in x_i$ for each $i \epsilon N_k$.

T2. If b and b' are blocks from the same class and if $R(x_1,\ldots,x_{i-1}, b,\ldots,x_k) \Longleftrightarrow R(x_1,\ldots,x_{i-1}, b',\ldots,x_k)$ for each $i \in N_k$ and for all $x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_k$ concurrent with b or b', then b=b'.

T3. If p and p' are points and $x_1,\ldots,x_k$ are blocks from different classes and if $p \epsilon x_i$, $p' \epsilon x_i$ for each $i \epsilon N_k$, then p=p'. Note that X_i, $i \epsilon N_k$, being partitions of a set P, consist of disjoint blocks.

We say that an T-k-seminet $N=(P,X_1,\ldots,X_k)$ is finite if P is a finite set, i.e $|P| < \infty$. In this paper only finite T-k-seminets are considered.

So, T-k-seminets are generalization of a variant 3-semi-nets in the sense of Taylor /5/.

Example 1. Let $P=\{1,2,3,4,5,6,7,8,9,o\}$ be a set of points and let the blocks and the classes (Fif.1) be given as follows:

$X = \{ x_1=\{1,2,3\}, \quad x_2=\{4,5,6,7,8,9,o\}\}$,

$Y = \{ y_1=\{8\}, \quad y_2=\{1,2,4,5,6,7,9\}, \quad y_3=\{3,o\}\}$,

$Z = \{ z_1=\{1,o\}, \quad z_2=\{2,4,9\}, \quad z_3=\{3,5,6,7,8\}\}$ and

$V = \{ v_1=\{4,7,o\}, \quad v_2=\{1,5\}, \quad v_3=\{2,8\}, \quad v_4=\{3,6,9\}\}$.

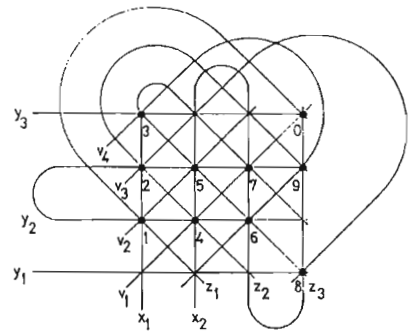


Figure 1.

It is easy to verify that N=(P,X,Y,Z,V) is a T-4-seminet.

Let P be a nonempty set, and $\mathcal{L}$ a nonempty set of subsets of P. Let the sets $X_1,\ldots,X_k$, $k \in N \setminus \{1,2\}$ partition the set $\mathcal{L}$. We say that the elements of P are points, the elements of $\mathcal{L}$ are blocks, and the sets $X_1,\ldots,X_k$ we call classes of blocks. Then we say that $N=(P,X_1,\ldots,X_k)$ is a U-k-seminet if and only if the following condition are satisfied:

U1. Through each point from P passes one and only one block from each of the classes X_i, $i \in N_k$.

U2. Any two blocks from different classes have at most one point in common.

Such a structure is introduced in /6/ where was called simply a k-seminet.

There arises the question of relation between T-k-seminets and U-k-seminets.

From Example 1. it follows already that there exist

T-k-seminets which are not U-k-seminets, since some blocks (x_1 and y_2, for instance) from distinct classes have two points in common.

THEOREM 1. Every U-k-seminet is a T-k-seminet.

Proof. Let $N=(P,X_1,\ldots,X_k)$ be a U-k-seminet. Clearly the sets $X_1,\ldots,X_k$ are mutually disjoint partition of a set P. One has to show that the axioms T1-T3 are satisfied.

Let b be a block, i.e. $b\in X_1\cup\ldots\cup X_k\subset\mathcal{P}(P)\setminus\{\emptyset\}$. Then $b\neq\emptyset$, so that there is $p\in P$ such that $p\in b$, which implies $p\in b$. Thus T1. holds.

Let us prove T2. Take two blocks b,b' from the same class and let it hold $R(x_1,\ldots,x_{i-1},b,x_{i+1},\ldots,x_k)$ if and only if $R(x_1,\ldots,x_{i-1},b',x_{i+1},\ldots,x_k)$ for all $x_1\ldots,x_{i-1},x_{i+1},\ldots,x_k$ concurrent with b or b'. Then, according to the definition of the relation R, there exist points p and p' such that

$$p\in x_1\cap\ldots\cap x_{i-1}\cap b\cap x_{i+1}\cap\ldots\cap x_k \qquad (*)$$

$$p'\in x_1\cap\ldots\cap x_{i-1}\cap b'\cap x_{i+1}\cap\ldots\cap x_k\ .$$

Further, because of U2., for all $j,m\in N_k\setminus\{i\}$, $j\neq m$, we have $|x_j\cap x_m|\leq 1$, and this gives p=p'. Now, from (*), we have $p\in b\cap b'$, which by U1. implies b=b'.

Let p,p' be points and $x_1,x_2,\ldots,x_k$ blocks from different classes such that $p\in x_i$ and $p'\in x_i$ for each $i\in N_k$ so that, in particular, we have $\{p,p'\}\subset x_1\cap x_2$. Now U2. implies p=p' and T3. is proved.

Let S be a nonvoid set, P a nonvoid subset of S^{k-1}, $k\geq 3$ and Z a partition on P such that there exists an injective mapping $\gamma: Z\to S$. Then the ordered triple $N=(S,Z,\gamma)$ is called an H-k-seminet /3/.

In /4/, for k=3, such a structure is called just 3-seminet.

In /3/ it is shown that the H-k-seminet $N=(S,Z,\gamma)$ can be given alternatively $N=(P,X_1,\ldots,X_k)$ so that:
$(\forall x_i\in X_i)(\forall x_j\in X_j)(i\neq j\Rightarrow|x_i\cap x_j|\leq 1)$ holds. In Example 1. T-k-seminet is not H-k-seminet since $|x_1\cap y_2|>1$.

Let $A_1,\ldots,A_k$, A_{k+1} be nonvoid sets and let D be a nonvoid subset of $A_1x\ldots xA_k$. Let $\mathcal{A}$ be any mapping from D into $\mathcal{P}(A_{k+1})$, i.e. $\mathcal{A}: D\to\mathcal{P}(A_{k+1})$.
Then we say that $\mathcal{A}$ is a partial k-multioperation and we write

$$\mathcal{A}(a_1,\ldots,a_k)=\{a_{k+1,j}\}\ ,\ (a_1,\ldots,a_k)\in D,\ \{a_{k+1,j}\}\in\mathcal{P}(A_{k+1})\ (1).$$

The set $\{a_{k+1,j}\}$ is called the product of the elements $a_1,\ldots,a_k$, and for the ordered k-tuple $(a_1,\ldots,a_k)=(a_1^k)$ we say that it belongs to the domain of the partial k-multioperation, which we write as $(a_1,\ldots,a_k)\in D$.

An ordered (k+2)-torku $M=(A_1,\ldots,A_k,A_{k+1},\mathcal{A})$, which satisfies (1), is called partial k-multigroupoid.
If $D=A_1x\ldots xA_k$, then M is called k-multigroupoid.

In order to simplify things we introduce the following notations:

$$\mathcal{A}:\ (\forall u_1\in A_1)\ldots(\forall u_{i-1}\in A_{i-1})(\forall u_{i+1}\in A_{i+1})\ldots(\forall u_k\in A_k)$$

$$(v\in\mathcal{A}(u_1^{i-1},\ a_i,u_{i+1}^k)\iff v\in\mathcal{A}(u_1^{i-1},\ a_i',\ u_{i+1}^k))\ ,$$

$\mathcal{B}$: $\mathcal{A}(a_1^{i-1}, a_i, a_{i+1}^{k}) = \mathcal{A}(a_1^{i-1}, a_i', a_{i+1}^{k})$,

$\mathcal{C}$: $a_i = a_i'$

$\mathcal{D}$: $(a_1,\ldots,a_k) \in D$.

A partial k-multigroupoid $M=(A_1,\ldots,A_k,A_{k+1}, \mathcal{A})$ is said to be i-T-cancellative if and only if the following condition hold:

$$(\forall(a_1^k) \in A_1x\ldots xA_k)(\forall a_i' \in A_i)(\mathcal{D} \Rightarrow (\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C}))) \qquad (2).$$

Further (2) is equivalent to each of the following formulas:

$$(\forall(a_1^k) \in A_1x\ldots xA_k)(\forall a_i' \in A_i)(\mathcal{D} \Rightarrow (\mathcal{A}\wedge\mathcal{B} \Rightarrow \mathcal{C}))^{1)} \qquad (\bar{2}),$$

$$(\forall(a_1^k) \in A_1x\ldots xA_k)(\forall a_i' \in A_i)(\mathcal{D} \Rightarrow (\mathcal{B} \wedge \neg\mathcal{C} \Rightarrow \mathcal{A}))^{2)} \qquad (\bar{\bar{2}}).$$

This follows easily from the following tautologies:

$$(p \Rightarrow (q \Rightarrow r)) \Leftrightarrow (p \wedge q \Rightarrow r),$$

$$(p \Rightarrow q) \Leftrightarrow (\neg q \Rightarrow \neg p) \;i\; \neg(p \Rightarrow q) \Leftrightarrow p \wedge \neg q .$$

If property (2) is fulfilled for each $i \in N_k$, then we say that $M=(A_1,\ldots,A_k,A_{k+1}, \mathcal{A})$ is a T-cancellative partial k-multigroupoid.

A partial k-multigroupoid $M=(A_1,\ldots,A_k,A_{k+1}, \mathcal{A})$ is said to be i-incompressible if and only if it holds:

1^o. For each $a_i \in A_i$ there is a (k-1)-tuple (a_1^{i-1}, a_{i+1}^{k}) such that $(a_1^{i-1}, a_i, a_{i+1}^{k}) \in D$.

2^o. For each $a_{k+1} \in A_{k+1}$ there is a k-tuple $(a_1,\ldots,a_k) \in D$ such that $a_{k+1} \in (a_1,\ldots,a_k)$.

If property (1^o) holds for each $i \in N_k$, then we say that $M=(A_1,\ldots,A_k,A_{k+1}, \mathcal{A})$ is an incompressible partial k-multigroupodis.

THEOREM2. Let $N=(P,X_1,\ldots,X_k)$ be a T-k-seminet. Let be a map from $X_1x\ldots xX_{k-1}$ to $\mathcal{P}(X_k)\setminus\{\emptyset\}$ defined as follows:

$$x_k \in \mathcal{A}(x_1,\ldots,x_{k-1}) \Leftrightarrow R(x_1,\ldots,x_{k-1},x_k). \qquad (3)$$

Then $M=(X_1,\ldots,X_{k-1},X_k, \mathcal{A})$ is a partial (k-1) - multigroupoid which is T-cancellative and incompressible.

Proof. Let $N=(P,X_1,\ldots,X_k)$ be a T-k-seminet. Then, using (3) and (1) we see that $M=(X_1,\ldots,X_{k-1},X_k, \mathcal{A})$ is a partial (k-1)-multigroupoid.

Now, let us prove that M is a T-cancellative partial (k-1)-multigroupoid.

The case $v\,\mathcal{A} \Rightarrow \bot$ is obvious (since $v(\bot \Rightarrow p)^{1)} = \mathbf{T}$).

If $v\,\mathcal{A} = \mathbf{T}$. Then (3) and T2. imply that $v\,\mathcal{C} = \mathbf{T}$. Now, the implication $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})$ is reduced to $\mathbf{T} \Rightarrow (p \overset{2)}{\Rightarrow} \mathbf{T})$ which holds true for every sentence p. Hence our partial (k-1)-multigroupoid is i-T-cancellative for each $i \in N_k$

So it remains to prove incompressibillity, i.e. 1^o and 2^o.

---

1) $p : \mathcal{B} \Rightarrow \mathcal{C}$, 2) $p : \mathcal{B}$

Let $x_i \in X_2$, $i \in N_k$. Then by T1. there exists a point $p \in P$ such that $p \in x_i$. Hence owing to $x_1,\ldots,x_k$ partitions of P there exists a k-tuple of blocks $(x_1^{i-1}, x_i, x_{i+1}^{k}) \in X_1 x \ldots x X_k$ such that $R(x_1,\ldots,x_i,\ldots,x_k)$. Furthermore, by (3) we get $x_k \in \mathcal{L}(x_1^{i-1}, x_i, x_{i+1}^{k-1})$, i.e. $(x_1^{i-1}, x_i, x_{i+1}^{k-1}) \in D$.

We have shown that $M=(A_1,\ldots,A_{k-1},A_k, \mathcal{L})$ is a cancellative incompressible partial (k-1)-multigroupoid, which is said to be associated to the T-k-seminet $N=(P,X_1,\ldots,X_k)$ and which we denote by $\mathcal{M}(N)$.

A partial k-multigroupoid $M=(A_1,\ldots,A_k,A_{k+1}, \mathcal{L})$ is said to be i-cancellative if and only if the following condition hold.

$$(\forall(a_1^k) \in A_1 x \ldots x A_k)(\forall a_i' \in A_i)(\mathcal{D} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})) \qquad (4).$$

THEOREM3. Let $M=(A_1,\ldots,A_k,A_{k+1}, \mathcal{L})$ is a partial i-cancellative k-multigroupoid. Then $M=(A_1,\ldots,A_k,A_{k+1}, \mathcal{L})$ is i-T-cancellative.

Proof. From (4) we find that $\mathcal{A} \Rightarrow (\mathcal{B} \Rightarrow \mathcal{C})$ reduces to $p^{1)} \Rightarrow \mathcal{T}$, $(p : \mathcal{B} \Rightarrow \mathcal{C})$.

Which is true for every sentence $p(=\mathcal{A})$.

THEOREM4. There exist partial k-multigroupoids which are i-T-cancellative but not i-cancellative.

Proof. Let $P=\{1,2,3,4,5,6,7,8,9,o\}$ be a set of points and Let the blocks and the classes (Fig. 2) be given as follows:

$$X = \{x_1 = \{1,2,3,4,\}\ ,\ x_2 = \{5,6,7\}\ ,\ x_3 = \{8,9,o\}\},$$

$$Y = \{y_1 = \{1,4,5,8,\}\ ,\ y_2 = \{2,6,9\}\ ,\ y_3 = \{3\}\ ,\ y_4 = \{o,7\}$$

and

$$Z = \{z_1 = \{5,8,9\}\ ,\ z_2 = \{1,6\}\ ,\ z_3 = \{o,2,4\}\ ,\ z_4 = \{3,7\}\}\ .$$

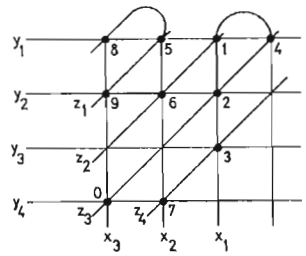


Figure 2.

In figure 2. is depicted a T-3-seminet $N=(P,X,Y,Z)$. According to the theorem 2. it has associated partial i-T-cancellative 2-multigroupoid M, for each $i \in \{1,2,3\}$. This M is not 2-cancellative because.

$$\neg(\forall x \in X)(\forall y_1 \in Y)(\mathcal{L}(x,y_1) = \mathcal{L}(x,y_2) \Rightarrow y_1 = y_2$$

which is equivalent to

$$(\exists x \in X)(\exists y_1 \in Y)(\exists y_2 \in Y)(\mathcal{L}(x,y_1) = \mathcal{L}(x,y_2) \wedge y_1 \neq y_2).$$

This is because we have

$$\mathcal{L}(x_3, y_1) = \mathcal{L}(x_3, y_2) \wedge y_1 \neq y_2.$$

THEOREM5. To every incompressible T-cancellative partial k-multigroupoid a T-(k+1)-seminet is associated.

Proof. Let $M=(A_1,\ldots,A_k,A_{k+1}, \mathcal{L})$ be an incompressible T-cancellative partial k-multigroupoid. NOw we will construct the corresponding T-(k+1)-seminet. Let

$$P = \{p=(a_1,\ldots,a_{k+1}) \in A_1 x \ldots x A_{k+1} : a_{k+1} \in \mathcal{A}(a_1,\ldots,a_k)\} \quad (5)$$

be the set of points of the derived structure. Let us define classes X_i, $i \in N_{k+1}$, where X_i is a collection of the subsets of set P of the following form:

$$x_{i,a} = P \cap (A_1 x \ldots x A_{i-1} x \{a\} x A_{i+1} x \ldots x A_{k+1}) \quad (6)$$

where a run through A_i.

Clearly the sets $x_i(a \in A_i)$ are disjoint and by incompressibility of $\mathcal{A}$ we conclude that they are nonempty and that they cover P, hence X_i is indeed a partition of P.

We have to check that so defined (k+2)-tuple $N=(P,X_1,\ldots,X_{k+1})$ satisfies T1.-T3.

We have already noted that $x_{i,a}$ are nonempty, hence T1. follows.

Let us define an (k+1)-any relation by

$$R(x_1,\ldots,x_k,x_{k+1}) \iff a_{k+1} \in \mathcal{A}(a_1,\ldots,a_k) \quad (7)$$

where $x_i = x_i, a_i$, $i \in N_{k+1}$.

Proof of property T2. Let $x_{i,a}$, $x_{i,a'}$ belong to X_i, $i \in N_{k+1}$, and let it hold

$$R(x_1,\ldots,x_{i,a},\ldots,x_{k+1}) \iff R(x_1,\ldots,x_{i,a'},\ldots,x_{k+1}) \quad (8)$$

for all $x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_{k+1}$ concurrent with $x_{i,a}$ or $X_{i,a'}$. Owing to (6), (7) and i-T-cancellativity of M partial k-multigroupoid (8) is equivalent to (2). This means that $x_{i,a} = x_{i,a'}$.

Let $p=(a_1,\ldots,a_{k+1}) \in P$ and $p'=(a'_1,\ldots,a'_{k+1}) \in P$ be points and let $x_{i,b_i} \in X_i$, $b_i \in A_i$ be blocks such that for every $i \in N_{k+1}$ it holds $p \in x_{i,b_i}$ and $p' \in x_{i,b_i}$.

Then, owing to (6) for every $i \in N_{k+1}$, we have $a_i = b_i$ and $a'_i = b_i$, i.e. $a_i = a'_i$, and this gives p=p'. Thus T1. holds.

Therefore, to any T-cancellative incompressible k-multigroupoid M we can associate a T-(k+1)-seminet which will be denoted by $\mathcal{N}(M)$.

REFERENCES:

/1/ J.Aczel, Quasigroups, nets and nomograms, Advances in Math. 1(1965), 386-450.

/2/ V.A. Belousov, Algebraičeskie seti i kvazigruppy, Kišinev, "Štiinca" 1971.

/3/ R.Galić, H-k-seminets, submitted to Rad JAZU, Zagreb.

/4/ V.Havel, Nets and Quasigroups, Comment. Math. Carolinae 8(1967), 415-451.

/5/ M.A.Taylor, Classical, cartesian and solution nets, Mathematica (Cluj) 13(36)(1971), 151-166.

/6/ J.Ušan, k-seminets, Matem. bilten, Knjiga 1. (XXVII), Skopje 1977, 41-46.

Faculty of civil engineering
University of Osijek

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

SOME CHARACTERIZATIONS OF n-BANDS

Pano Kržovski

Abstract. *An idempotent n-semigroup is called an n-band. Some well-known properties of bands (i.e. of 2-bands) are generalized in this paper.*

0. *First we will state the necessary preliminary definitions and results.*

If $(x_1,\dots,x_n) \mapsto x_1x_2\dots x_n$ is an associative n-ary operation on a set S, then we say that S is an n-semigroup. A subset A of S is called an i-ideal of S iff $s^{i-1}AS^{n-i} \subseteq A$ (as usual, $S^0AS^{n-1}=AS^n$, $S^{n-1}AS^0=S^{n-1}A$); if i=n, then A is called a left ideal, and if i=1 - a right ideal; A is a two-sided ideal iff it is a left and right ideal; A is an ideal iff it is an i-ideal for every $i\in\{1,2,\dots,n\}$. An n-semigroup S is said to be two sided simple (left-simple) if it has no proper two sided ideal (left ideal). An ideal A is said to be completely prime iff: $x_1x_2\dots x_n\in A \Longleftrightarrow (\exists i)x_i\in A$. A filter of S is any subset $B\subseteq S$ which complement in S is a completely prime ideal. If x is a given element of S, then N(x) will denote the intersection of all filters of S which contain x.

An n-semigroup S is called an n-band iff it is idempotent, i.e. iff the identity $x^n=x$ holds in S. If, in addition, S is commutative and for every $i_\nu, j_\nu > 0$ such that

$$i_1 + i_2 + \dots + i_k = j_1 + j_2 + \dots + j_k = n,$$

the identity

$$x_1^{i_1}x_2^{i_2}\dots x_k^{i_k} = x_1^{j_1}x_2^{j_2}\dots x_k^{j_k}$$

holds in S, then we say that S is an n-semilattice. A congruence α in S is called a semilattice congruence iff S/α is an n-semilattice.

We will formulate some results proved in [5] and [6]. Throughout the paper, S will denote a given n-semigroup if it is not said otherwise.

This paper is in final-form and no version of it will be submited for publication elsewher.

0.1. ([5] 3.2) *The relation* η *defined in* S *by*

$$x\eta y \iff N(x) = N(y)$$

is the minimal semilattice congruence on S.

(If $x\in S$, *then the* η*-class which contains* x *will be denoted by* N_x.)

0.2. ([6] 2.2) *If* $x\in S^{n-1}xS^{n-1}$ *for every* $x\in S$, *then*

$$N_x = \{y\in S \mid x\in S^{n-1}yS^{n-1},\ y\in S^{n-1}xS^{n-1}\},$$

also for every $x\in S$.

0.3. ([5] 2.1) *The following conditions on an* n*-semigroup* S *are equivalent.*

(i) Every η*-class of* S *is a left simple* n*-semigroup.*

(ii) For every $x\in S$, $x\in S^{n-1}x^n$ *and* $xS^{n-1}\subseteq S^{n-1}x$.

(iii) For every $x\in S$, $N_x=\{y\in S \mid x\in S^{n-1}y,\ y\in S^{n-1}x\}$.

1. *Now we will give a characterization of* n*-bands by means of the* η*-classes.*

Proposition 1. An n*-semigroup* S *is an* n*-band iff for every* $x\in S$ *the following equality holds:*

$$N_x = \{y\in S \mid x=(xy^{n-1})^{n-1}x,\quad y=(yx^{n-1})^{n-1}y\}. \qquad (1)$$

Proof. Let S be an n-band. Then

$$x = x^n = x^{n-1}x^nx^{n-1}\in S^{n-1}x^nS^{n-1},$$

and so, by 0.2., we have

$$N_x = \{y\in S \mid x\in S^{n-1}yS^{n-1},\ y\in S^{n-1}xS^{n-1}\}.$$

By this it follows that, if $x\in S$ *and* $y\in N_x$, *then there exist* $a_1,\dots,a_{n-1}$, $b_1,\dots,b_{n-1}$ *such that*

$$x = a_1\dots a_{n-1}yb_1\dots b_{n-1}.$$

Therefore:

$$\begin{aligned}
x = xx^{n-1} &= a_1\dots a_{n-1}yb_1\dots b_{n-1}x^{n-1}\\
&= a_1\dots a_{n-1}(yb_1b_2\dots b_{n-1}x^{n-1}) =\\
&= a_1\dots a_{n-1}(yb_1b_2\dots b_{n-1}x^{n-1})^n =\\
&= (a_1a_2\dots a_{n-1}yb_1b_2\dots b_{n-1})x^{n-1}(y\,b_1b_2\dots b_{n-1}x^{n-1})\dots(yb_1b_2\dots b_{n-1}x^{n-1})\\
&= xy^{n-1}(yb_1b_2\dots b_{n-1}x^{n-1})^{n-1} =\\
&= (xy^{n-1})^n(yb_1b_2\dots b_{n-1}x^{n-1})^{n-1} =\\
&= (xy^{n-1})^{n-1}xy^{n-1}(yb_1b_2\dots b_{n-1}x^{n-1})^{n-1} =\\
&= (xy^{n-1})^{n-1}x.
\end{aligned}$$

By symmetry: $y=(yx^{n-1})^{n-1}y$ *and so (1) is proved.*

Conversely, suppose that S *is an* n*-semigroup in which (1) holds. Then, if* $x\in S$, *we have* x, $x^n\in N_x$ *and:*

$$\begin{aligned}
x &= (xx^{n-1})^{n-1}x = x^{n(n-1)+1}\\
x^n &= (x^nx^{n-1})^{n-1}x^n = x^{(2n-1)(n-1)+n} =\\
&= x^{n(n-1)+1}x^{n(n-1)} = x,
\end{aligned}$$

i.e. S *is an* n*-band.* ||

2. *It is well known (see for example ([3] p. 45) that a band is a two-sided simple iff it is a rectangular band, i.e. iff it satisfies the identity* $xyx=x$. *We give a description of two-sided simple* n*-bands, for any* n, *in the following proposition.*

Proposition 2. An n*-semigroup* S *is a two-sided simple* n*-band iff it satisfies the identity*

$$(xy^{n-1})^{n-1}x = x. \qquad (2)$$

Proof. Let S be a two-sided simple n-band and let $x,y\in S$. Then $S^{n-1}yS^{n-1}=S$, by which it follows that there exist $a_1,\dots,a_{n-1}$, $b_1,\dots,b_{n-1}\in S$ such that

$$x = a_1\dots a_{n-1}yb_1\dots b_{n-1}.$$

Using this, we have that:

$$
\begin{aligned}
x &= a_1 \dots a_{n-1} y b_1 \dots b_{n-1} x^{n-1} \\
&= a_1 \dots a_{n-1} (y b_1 \dots b_{n-1} x^{n-1})^n \\
&= a_1 \dots a_{n-1} y b_1 \dots b_{n-1} x^{n-1} (y b_1 \dots b_{n-1} x^{n-1})^{n-1} \\
&= x x^{n-1} (y^n b_1 \dots b_{n-1} x^{n-1})^{n-1} \\
&= x y^{n-1} (y b_1 \dots b_{n-1} x^{n-1})^{n-1} \\
&= (x y^{n-1})^{n-1} x y^{n-1} (y b_1 \dots b_{n-1} x^{n-1})^{n-1} \\
&= (x y^{n-1})^{n-1} x,
\end{aligned}
$$

i.e. that the identity (2) is true.

Conversely, if an n-semigroup S satisfies the identity (2), then by Proposition 1, S is an n-band. Beside this, for all $x,y \in S$ we have

$$y = (y x^{n-1})^{n-1} y \in S^{n-1} x S^{n-1},$$

i.e. $S = S^{n-1} x S^{n-1}$, by which it follows that S is two-sided simple. ||

3. We will give here a description of one more class of n-bands.

Proposition 3. If S is an n-band, then the following statements are equivalent:

(i) The identity $xy^{n-1} = x$ holds in every n-class of S.

(ii) For every $x \in S$, $xS^{n-1} \subseteq S^{n-1}x$.

(iii) For every $x \in S$, $N(x) = \{y \in S \mid xy^{n-1} = x\}$.

(iv) S satisfies the identity

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

Proof. (i) $\Longrightarrow$ (ii). It is clear that if an n-semigroup satisfies the identity $xy^{n-1} = x$ then it is left-simple. Thus, by 0.3., one obtains that (i) implies (ii).

(ii) $\Longrightarrow$ (iii). Let $xS^{n-1} \subseteq S^{n-1}x$ for every $x \in S$. Since $x = x^n = x^{n-1}x = x^{n-1}x^n \in S^{n-1}x^n$, by 0.3 we obtain that

$$N_x = \{y \in S \mid x \in S^{n-1} y,\ y \in S^{n-1} x\}.$$

By this, it follows that if $y \in N_x$, then there exist $a_1, \dots, a_{n-1} \in S$, such that $x = a_1 a_2 \dots a_{n-1} y$. Therefore

$$x = x^{n-1} a_1 \dots a_{n-1} y = x^{n-1} a_1 \dots a_{n-1} y^n = x y^{n-1}.$$

We will prove now that the set $T = \{y \in S \mid x \in S^{n-1} y\}$ is a filter.

Let $u_1 u_2 \dots u_n \in T$. Then

$$x \in S^{n-1} u_1 u_2 \dots u_n = S^{n-1} u_1 u_2 \dots u_i^{n-i+1} u_i^{i-1} \dots u_n \subseteq S^{n-1} u_1 u_2 \dots u_{i-1} u_i^{n-i+1} S^{n-1}$$
$$\subseteq S^{n-1} u_1 u_2 \dots u_i^{n-i+1} \subseteq S^{n-1} u_i.$$

Therefore $u_i \in T$ for $i = 1, 2, \dots, n$.

Conversely, let $u_1, u_2, \dots, u_n \in T$. Then $x \in S^{n-1} u_1$, $x \in S^{n-1} u_2, \dots, x \in S^{n-1} u_n$ and so, using (ii),

$$x \in S^{n-1} x^n \subseteq S^{n-1} S^{n-1} u_1 S^{n-1} u_2 \dots S^{n-1} u_n \subseteq$$
$$\subseteq S^{n-1} u_1 S^{n-1} u_2 \dots S^{n-1} u_{n-1} u_n \subseteq \dots \subseteq$$
$$\subseteq S^{n-1} u_1 u_2 \dots u_n.$$

Therefore $u_1 u_2 \dots u_n \in T$, and since $x = x^n \in S^{n-1} x$, it follows that $N(x) \subseteq T$.

Let $y \in T$. Then $x = a_1 a_2 \dots a_{n-1} y \in N(x)$, and since $N(x)$ is a filter, it follows that $y \in N(x)$ which means that $T \subseteq N(x)$. Hence $T = N(x)$, i.e. $N(x) = \{y \in S \mid x \in S^{n-1} y\}$.

But, $x \in S^{n-1} y$ iff $x = x y^{n-1}$, and therefore we have $N(x) = \{y \in S \mid x = x y^{n-1}\}$.

(iii) $\Longrightarrow$ (iv). The set $N(xy^{n-1})$ is a filter of S. By the assumption,

$$N(xy^{n-1}) = \{z \in S \mid xy^{n-1} = xy^{n-1} z^{n-1}\}.$$

Since $x, y \in N(xy^{n-1})$, it follows that $xy^{n-1} = xy^{n-1}x^{n-1}$ and $y^{n-1}x = y^{n-1}xy^{n-1}$ which implies that

$$xy^{n-1} = xy^{n-1}x^{n-1} = xy^{n-1}xx^{n-2} = xy^{n-1}xy^{n-1}x^{n-2} = \dots =$$
$$= (xy^{n-1})^{n-1} x.$$

(iv) $\Longrightarrow$ (i). If S is an n-band, then for every $x \in N_x$, by Proposition 1, we have

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

4. We will show now that the n-semilattices are, in fact, usual binary semilattices (i.e. commutative idempotent semigroups).

Proposition 4. An n-semigroup S is an n-semilattice iff there exists a binary operation "$\cdot$" on S such that $(S;\cdot)$ is a semilattice and the following identity is satisfied:

$$x_1x_2\dots x_n = x_1\cdot x_2\cdot\dots\cdot x_n. \tag{4.1}$$

Proof. Suppose first that S is an n-semilattice and define a binary operation "$\cdot$" on S by

$$x\cdot y = xy^{n-1}. \tag{4.2}$$

Then, $(S;\cdot)$ is a commutative groupoid and

$$(x\cdot y)\cdot z = xy^{n-1}z^{n-1},$$

$$x\cdot(y\cdot z) = x(yz^{n-1})^{n-1} = xy^{n-1}(z^{n-1})^{n-1}$$

$$= xy^{n-1}z^{n-2}z^{1+(n-2)(n-1)} =$$

$$= xy^{n-1}z^{n-1};$$

thus $(S;\cdot)$ is a semilattice. Also we have that:

$$x_1\cdot x_2\cdot\dots\cdot x_n = x_1x_2^{n-1}x_3^{n-1}\dots x_n^{n-1} =$$

$$= x_1x_2^{n-1}\dots x_{n-2}^{n-1}(x_{n-1}^{n-1}x_n)x_n^{n-2} =$$

$$= x_1x_2^{n-1}\dots x_{n-2}^{n-1}x_{n-1}x_n^{n-1}x_n^{n-2} = \dots =$$

$$= x_1x_2x_3\dots x_{n-2}x_{n-1}x_n^{1+(n-2)(n-1)} =$$

$$= x_1x_2\dots x_n,$$

i.e. (4.1) is true.

If (S,o) is a semilattice such that

$$x_1x_2\dots x_n = x_1ox_2o\dots ox_n,$$

then

$$xoy = xoyoyo\dots oy = xy^{n-1},$$

i.e. $xoy = x\cdot y$. ||

5. The following problem is considered in the paper [4; pp. 138-139]: given a class $\mathcal{C}$ of semigroups, find a "reasonable" definition of the corresponding class $\mathcal{C}(n)$ of n-semigroups. One of the possible solutions is to say that:

"An n-semigroup S belongs to $\mathcal{C}(n)$ iff there exists a semigroup $(S;\cdot)\in\mathcal{C}$ such that the identity (4.1) is satisfied".

The proposition 4 gives the possibility to characterize in such a way the class of n-semilattices, but we should note that this kind of defining classes of n-semigroups is not suitable.

In order to illustrate this assertion we will consider the symmetric group of permutations $G=\{(1),(12),(13),(23),(123),(132)\}$. The set of transpositions, $S=\{(12),(13),(23)\}$ is a ternary semigroup with respect to superposition of mappings; moreover, this 3-semigroup is a 3-band and a 3-group. But, there is no binary semigroup $(S;\cdot)$ in which (4.1) would hold.

We mention that the Propositions 1, 2 and 3 are well known for $n=2$. (See, for example, [3].) This propositions suggest to call S a rectangular n-band iff S satisfies the identity (2). For example, the 3-semigroup $S=\{(12),(13),(23)\}$ satisfies this identity, because $(xy^2)^2x=x^2x=x$, and so we can consider S as a rectangular 3-band.

Note that if we want to carry over the property of anticommutativity of rectangular bands to the n-ary case, then we come to another class of n-semigroups as it is shown in [1]. Namely, one obtains that an n-semigroup S satisfies the quasiidentity

$$xz_1\dots z_{n-1}y = yz_1\dots z_{n-1}x \Longrightarrow x=y$$

iff there exists a binary rectangular band $(S;\cdot)$ such that $x_1\dots x_n = x_1\cdot x_n$.

REFERENCES

/1/ Б.Трпеновски: Антикомутативни n-групоиди. Годишен зборник на Електро-машински факултет на Универзитетот - Скопје, 1967, (33-36)

/2/ M.Petrich: The maximal semilattice decomposition of a semigroup, Math. Zeitschrift 85, 1964 (68-82)

/3/ M. Petrich: Introduction to semigroup, Charles E.Merill publ. Co Columbus, Ohio, 1973.

/4/ G.Čupona, N.Celakoski: Polyadic subsemigroups of semigroups, Algebraic Conference, Skopje, 1980 (131-152)

/5/ P.Kržovski: The maximal semilattice decomposition an n-semigroup. Algebraic Conference, Novi Sad 1981, (93-107)

/6/ P.Kržovski: Semilattice of simple n-semigroup, Algebra and Logic", Zagreb, 1984 (83-88)

Kržovski Pano
Mašinski fakultet
91000 Skopje
Yugoslavia

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

INDEX OF IRREDUCIBILITY IN THE FORMAL POWER SERIES RING

Aleksandar Lipkovski

Abstract. In the present note the index of irreducibility of a given formal power series is introduced. Freely speaking, it is the smallest degree of its homogeneous form which is an obstacle for reducibility. Some examples are given. A natural conjecture about this number is stated, together with some supporting arguments.

As it is known, the ring $A=K[[x_1,\dots,x_n]]$ of formal power series in n indeterminates over a field K is a unique factorisation domain. In author's recent work the notion of strong irreducibility has been introduced in connection with geometrical and combinatorial properties of corresponding Newton polyhedra, and some families of strongly irreducible elements have been found (see [2] part II and also [3]). In this note an attempt to introduce an integer parameter for irreducible elements is made, which leads to an interesting and natural problem. Its proof would provide us with nice stratification of the set of irreducible formal power series.

Let $f=\sum a_i x^i \in A$ (i is a multiindex). $f_k=\sum_{|i|=k} a_i x^i$ will denote the homogeneous form of f of degree k, ord f is the degree of the initial form of f. $\mathfrak{M}=(x_1,\dots,x_n)$ is the maximal ideal of the local ring A. If ord f=0, then f is a unit, if ord f=1, then f is irreducible. We shall always assume that d=ord $f \geqslant 2$.

DEFINITION 1. f is reducible modulo $k \in \mathbb{N}$ if there is a $g \in \mathfrak{M}^k$ such that f+g is reducible. Otherwise f is irreducible modulo k.

DEFINITION 2. Index of irreducibility of the series f is the number (or $+\infty$) $i(f)=\sup\{k \in \mathbb{N} \mid f \text{ reducible modulo } k\}$.

This paper is in final form and no version of it will be submitted for publication elsewhere.

Remarks. 1. f reducible mod k $\Rightarrow$ f reducible mod $l \leq k$.
2. f reducible $\Rightarrow$ f reducible mod k for all k.
3. $i(f)=\inf\{k\in\mathbb{N} \mid f \text{ irreducible mod } k\}-1$.

Before stating examples, let us recall some notions and properties from [2]. For $f\in A$, its support is the set $\operatorname{supp} f = \{i\in\mathbb{Z}_0^n \mid a_i\neq 0\}$. $N(f)=\operatorname{conv}(\operatorname{supp} f+\mathbb{R}_0^n)$ is the Newton polyhedron of f. We say that f is strongly irreducible if its Newton polyhedron cannot be decomposed in the sum of such polyhedra. Since $N(fg)=N(f)+N(g)$, strongly irreducible elements are irreducible. One sufficient condition of indecomposability will be used here, namely if N(f) has an indecomposable face which intersects all coordinate hyperplanes, then N(f) is indecomposable (see [2] part II, §1-2).

Example 1. For $f=xy+z^m\in K[[x,y,z]]$ we have $i(f)=m$. More generally, for $f=x^k y^l+z^m$ with $M(k,l,m)=1$ we have $i(f)=\max(k+l,m)$. Indeed, under this condition f is (strongly) irreducible: N(f) has an edge with vertices $(k,l,0)$, $(0,0,m)$. If $p>\max(k+l,m)$, this edge appears also in $N(f+g)$ for all $g\in\mathfrak{M}^p$. Therefore, $i(f)\leq\max(k+l,m)$. On the other hand, if $p\leq\max(k+l,m)$, we have two possibilities. If $\max(k+l,m)=k+l$, then $p\leq k+l$ and $x^k y^l\in\mathfrak{M}^p$; if $\max(k+l,m)=m$, then $p\leq m$ and $z^m\in\mathfrak{M}^p$. In both cases f is reducible modulo p. This means exactly that $i(f)=\max(k+l,m)$.

Example 2. For $f=x^k+y^l+z^m$ with $k<l\leq m$ and $M(k,l)=1$, we have $i(f)=l$. Indeed, f is (strongly) irreducible, since N(f) has an edge with vertices $(k,0,0)$, $(0,l,0)$. If $p>l$, then for any $g\in\mathfrak{M}^p$, $f+g=x^k+y^l+h$ where $h\in\mathfrak{M}^{l+1}$ and N(f+g) also has that edge. Therefore, $i(f)\leq l$. On the other hand, if $p\leq l$, then $y^l+z^m\in\mathfrak{M}^p$ and f is reducible modulo p. Therefore, $i(f)=l$.

Given $f\in A$, let $S_k(f)$ denote the system

$$\begin{cases} g_1h_1 = f_2\\ g_1h_2+g_2h_1 = f_3\\ \cdots\cdots\cdots\\ g_1h_{k-1}+\ldots+g_{k-1}h_1 = f_k \end{cases}$$

with indeterminate homogeneous forms g_i, h_i of degree i $(1\leq i\leq k-1)$.

Remark. $S_k(f)$ has a solution $\Rightarrow$ $S_l(f)$ has a solution for all $l\leq k$.

PROPOSITION 1. i(f) is the least number k for which the system $S_{k-1}(f)$ has no solution.

Proof. Obviously, f reducible mod k $\Leftrightarrow$ $S_{k-1}(f)$ has a solution. Therefore we have $i(f)=\sup\{k \mid f \text{ reducible mod } k\}=$
$=\sup\{k \mid S_k(f) \text{ has a solution}\}+1=\inf\{k \mid S_k(f) \text{ has no solutions}\}$.

Remarks. 1. If $S_k(f)$ has a solution and $f'\in f+\mathfrak{M}^{k+1}$, then $S_k(f')$ has also a solution. Indeed, $S_k(f)=S_k(f')$.
2. If $i(f)=m$, then for all $f'\in f+\mathfrak{M}^{m+1}$, $i(f')=m$.

We see that if i(f) is finite, then f is irreducible. One may ask, under what conditions the converse holds?

THEOREM 1. If f is strongly irreducible and regular with respect to all indeterminates, then i(f) is finite.

Proof. Under the conditions stated, there is an $k\in\mathbb{N}$ such that all vertices of N(f) lay under the hyperplane $x_1+\ldots+x_n=k$. Then $N(f+g)=N(f)$ for all $g\in\mathfrak{M}^k$. But f is strongly irreducible and so is f+g. This means that $i(f)\leq k$.

It seems acceptable that the condition of regularity may be dropped, since adding a $g\in\mathfrak{M}^k$ to f (not necessarily regular) will change only some unbounded faces of N(f) and for a sufficiently large k will not change the indecomposable skeleton of N(f) (see [3]). So we arrive to

CONJECTURE 1. f is strongly irreducible $\Rightarrow$ i(f) is finite.

Since the definition of i(f) does not involve the notion of Newton polyhedra and strong irreducibility, one may state even stronger hypothesis.

CONJECTURE 2. f is irreducible $\Rightarrow$ i(f) is finite.

This seems to be very natural. In fact, if $i(f)=+\infty$, then for all k we have a solution of $S_k(f)$ or equivalently,

(1) for all $k\in\mathbb{N}$, $f\equiv g^{(k)}h^{(k)} \bmod \mathfrak{M}^k$.

The problem is to patch this solutions together, to obtain a factorisation f=gh in A. Unfortunately, the ring A is not compact in $\mathfrak{M}$-adic topology (otherwise we could pick out a convergent subsequence of $g^{(1)}, g^{(2)}, \ldots$ to obtain g). Instead of compactness, we have a weaker property of linear compactness

(see [1]ch.III,§2,7 and §2 ex.14,15), which means that only the filters in A with basis of affine linear sets (i.e. sets of the form a+I where I is an ideal in A) must have an adherent point. In fact, this property is a consequence of completness (ibid. ex.22) and is not particularly useful for us. The conjecture 2 would follow from a (stronger) statement about the sequence $g^{(\kappa)}$:

(2) for all k exists an $l > k$, such that $g^{(l)} - g^{(\kappa)} \in \mathfrak{M}^{\kappa}$,

which would enable us to pick out a convergent subsequence. However, statement (2) seems to be too strong; it is not clear why should for each $g^{(\kappa)}$ exist an $g^{(l)}$ $(l > k)$ with the same k-jet. It would be, maybe, possible to find, by some kind of diagonal argument, a new sequence $\overline{g}^{(\kappa)}$ which fulfills (2) and still has the property (1).

Note. Conjecture 1 is proved in [3].

REFERENCES

1. N.Bourbaki, Commutative algebra (russian transl.), Mir, Moscow, 1971.
2. A.Lipkovski, Unibranched singularities and irreducibility in the formal power series rings, Thesis, University of Belgrade, 1985.
3. A.Lipkovski, Newton polyhedra and irreducibility, to appear.

Institut za matematiku
Prirodno matematicki fakultet
Studentski trg 16
11000 Beograd
Jugoslavija

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

SEMIGROUPS WHOSE SUBSEMIGROUPS ARE LEFT UNITARY

Todor Malinović

Abstract. We give the definition of strongly left regular semigroup and we characterize the semigroups S having one of the following properties: (a) every left (right) ideal of S is left unitary, (b) every one-sided ideal of S is left unitary, (c) every subsemigroup of S is left unitary.

Troughout this paper let Z^+ denote the set of all positive integers.

A nonempty subset A of a semigroup S is left unitary if $x \in S$ and $a, ax \in A$ imply $x \in A$; right unitary is defined dually; A is unitary if it is both left and right unitary. A semigroup S is regular if $a \in aSa$ for every $a \in S$; left (right) regular if $a \in Sa^2 (a \in a^2S)$ for every $a \in S$.

For nondefined notions we refer to [1], [2] and [3]

DEFINITION 1. A semigroup S is strongly left regular if

$$(\forall a,b \in S)(a \in Sab \vee a \in Sba).$$

A strongly right regular semigroup is defined dually.

THEOREM 1. A semigroup S is strongly left regular if and only if every left ideal of S is left unitary.

Proof. Let S be a strongly left regular semigroup and let L be a left ideal of S. If $a, x \in S$ arbitrary element, then

$$x \in Sax \vee x \in Sxa$$

This paper is in final form and no version of it will be submitted for publication elsewhere.

and so

(1) $x=yax \vee x=zxa$

for some $z,y \in S$. If $a,ax \in L$, then $xa \in L$ and from (1) we have that

$$x=yax \in SL \subseteq L$$

or

$$x=zxa \in SL \subseteq L.$$

Hence, L is left unitary and thus every left ideal of S is left unitary.

Conversely, let every left ideal of S is left unitary and let $x,a \in S$. If L(ax) and L(xa) are the left ideals of S generated by elements ax and xa, respectively, then

$$L=L(ax) \cup L(xa)$$

is a left ideal of S and so

(2) $L=ax \cup xa \cup Sax \cup Sxa.$

From this we have that

(3) $xa,\ xax \in L$

and thus

(4) $x \in L,$

since L is left unitary. By (2) and (4), it follows that

$$x=ax \vee x=xa \vee x \in Sax \vee x \in Sxa.$$

If x=ax, then

$$x=a^2x=a(ax) \in Sax.$$

Now, consider case x=xa. Since $axa \in Sxa$ and

$$axa^2=a(xa)a=axa \in Sxa$$

we must have $a \in Sxa$. Hence,

$$a,axa \in Sxa$$

and thus

$$x=xa \in Sxa,$$

since Sxa is left unitary. Consequently we conclude that

$$x \in Sxa \vee x \in Sax$$

and thus S is strongly left regular.

Remark It is clear that, if R is proper right ideal then R is not left unitary.

THEOREM 2. Every one-sided ideal of a semigroup S is left unitary if and only if S is a right group.

Proof. Let every one-sided ideal of S is left unitary. Then, by Remark 1, we must have S is right simple and thus

(5) $(\forall a \in S)(aS=S).$

On the other hand

(6) $(\forall a \in S)(a \in Sa^2),$

since S is strongly left unitary (Theorem 1).
From (5) and (6) it follows that

$$(\forall a \in S)(a \in aSa^2)$$

and thus S is a union of groups. Since S is right simple we have that S is a right group.

Conversely, let S be a right group and let L be an arbitrary left ideal of S. If $a,ax \in L$ for some $x \in S$, then, by Theorem IV. 3.9. [3], we have that S is regular and thus

(7) $ax=(ax)y(ax)$

for some $y \in S$. Since S is left cancellative so by (7), it follows that

$$x=(xy)(ax) \in SL \subseteq L$$

Hence, L is left unitary and thus every left ideal of S is left unitary.

LEMMA 2. Every two-sided ideal of a semigroup S is left unitary if and only if S is simple.

Proof. Let every two-sided ideal of S is left unitary and let I be an arbitrary two-sided ideal of S. If $a \in I$ is an arbitrary element, then

(10) $(\forall x \in S)(ax \in I).$

Since I is left unitary so $x \in I$ wich together with (10) implies I=S and thus S is simple.

Since the converse is obvious, the lema is proved.

THEOREM 3. Every subsemigroup of a semigroup S is left unitary if and only if S is a periodic right group.

Proof. Let every subsemigroup of S is left unitary. Then by Theorem 2, we have that S is a right group.

Let a be an arbitrary element of S. Then

$$\langle a \rangle = \{a, a^2, a^3, \dots\}$$

is a subsemigroup of S generated by a. If $\langle a \rangle$ is infinite, then

$$A = \{a^2, a^3, \dots\} \tag{11}$$

is a subsemigroup of S. Since A is left unitary so

$$a^3, a^3 a \in A \Rightarrow a \in A$$

which together with (11) implies

$$a = a^k$$

for some $k \in Z^+$ and $k \geqslant 2$. Hence, S is periodic.

Conversely, let S be a periodic right group. If A is a subsemigroup of S, then A is periodic and thus A is a union of disjoint groups. Since S is right simple it follows that every idempotent of S is a left identity. Suppose now that

$$a, ax \in A \tag{12}$$

for some $x \in S$. Let $a' \in A$ be an inverse of a in a subgroup G_a of A. Then

$$a'ax \in A \tag{13}$$

and from this we have that

$$x \in A. \tag{14}$$

From (12) and (14), it follows that A is a left unitary, and thus every subsemigroup of S is a left unitary.

COROLLARY Every subsemigroup of a semigroup S is unitary if and only if S is a periodic group.

Proof. Follows immediately from the Theorem 3.

REFERENCES

[1] S. Bogdanović, Semigroups with a system of subsemigroups, Inst. of math., Novi Sad 1985.

[2] A.H. Clliford and G.B. Preston, The algebraic theory of semigroups (in Russian) "MIR", Moskow 1972.

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

Lenjinova 4/16
17500 - Vranje,
Yugoslavia

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

ON THE NUMBER OF ω_1-LIKE EXTENSIONS OF COUNTABLE MODELS OF PA

Žarko Mijajlović

Abstract

Using first-order logic with the additional quantifier "there exist uncountably many x", we show that there are 2^{ω_1} ω_1-like extensions of countable models of formal arithmetics.

We propose a method for counting ω_1-like elementary end-extensions (abr. e.e. extensions) of countable models of Peano arithmetic (abr. PA). Gaifman's approach by using minimal types, gives a powerful method for determining the number of end-extensions of models of PA. On the other hand, R. Kossak was the first who studied the problem of determining the number of ω_1-like extensions which satisfy additional properties (for example models which are recursively saturated), cf. [3], [5]. The method in this paper is based on the logic L(Q), where Q denotes the quantifier "there exist uncountably many ", and end-extensional types introduced in [1]. When we are dealing with L(Q), we shall assume the notation as it is introduced in [2], and when we speak about models of PA we shall use the notation and terminology as in [1] and [7]. However, minor changes are possible. For example, we shall assume throughout that Qx satisfies the fifth Keisler's axiom K5, i.e. $Qx(x=x)$. Therefore, the standard models of L(Q) are uncountable. The reader is warned that standard models of logic L(Q) are nonstandard models of PA in first order logic. The quantifier $\exists x$ is defined by: $\exists x\varphi \leftrightarrow \neg Qx\varphi$. Thus $L(\exists)$ is an extension of first order logic with equality obtained by adding a new quantifier $\exists x$. Obviosly, properties of this quantifier can be easily deduced from the properties of the quantifier Qx, see e.g. [6]. Models will be denoted by letters A,B,C,..., and their domains by A,B,C,... respectively.

This paper is in final form and no version of it will be submitted for publication elsewhere.

First we state some results on the logic L(Q) and models of PA. By PA(Q) we denote Peano arithmetic in L(Q), but with induction scheme applied to all formulas $L_{PA}(Q)$, where L_{PA} denotes the usual language of formal arithmetic. We remind that an ω_1-like model of PA is such a model M in which every initial segment is countable, but M itself is uncountable. If M is a model of PA, then the quantifier Qx over M defined by

(1) $M \models Qx\varphi x \leftrightarrow \forall y\, \exists x(y<x \wedge \varphi x)$

satisfies all the Keisler's axioms K1-K5:

K1. $\neg Qx(x=y \vee x=z)$,

K2. $\forall x(\varphi \rightarrow \psi) \rightarrow (Qx\varphi \rightarrow Qx\psi)$,

K3. $Qx\varphi x \leftrightarrow Qy\varphi y$, y does not occur in φx,

K4. $Qy\,\exists x\varphi xy \rightarrow \exists x Qy\varphi xy \vee Qx\exists y\varphi xy$,

K5. $Qx(x=x)$.

For so introduced quantifier Q, the following theorem shows that ω_1-like models can be characterized in L(Q).

THEOREM 1. A model M of PA is an ω_1-like model iff M is a standard model of PA(Q).

Proof ($\rightarrow$) Suppose M is an ω_1-like model of PA. Then for any formula φ of $L_{PA}(Q)$ the following holds:

$M \models Qx\varphi x$ iff there are uncountably many $a \in M$ such that $M \models \varphi a$
iff there are cofinally many $a \in M$ such that $M \models \varphi a$
iff $M \models \forall y\, \exists x(y<x \wedge \varphi x)$

i.e. M satisfies (1). Thus M is a model of PA(Q) since the natural ordering $<$ defines the quantifier which satisfies Keisler's axioms. We see that M is a standard model of PA(Q) since $M \models Qx(x=x)$.

($\leftarrow$) Suppose M is a standard model of PA(Q). As $M \models Qx(x=x)$, M is uncountable. Further, we show

Claim $PA(Q) \vdash \forall y\, \exists x(x<y)$.

We prove the claim by induction in PA(Q):

As $\forall x(x<0 \rightarrow x=0) \rightarrow (\exists x(x=0) \rightarrow \exists x(x<0))$, we have

(1) $PA(Q) \vdash \exists x(x<0)$.

Further, $\exists x(x<y') \leftrightarrow \exists x(x<y \vee x=y)$
$\leftrightarrow \exists x(x<y) \wedge \exists x(x<0)$,

so by induction hypothesis and (1), the following holds

(2) $PA(Q) \vdash \exists x(x<y) \rightarrow \exists x(x<y')$.

Therefore, $M \models \forall y\, \exists x(x<y)$, hence every initial segment of M is countable. ∎

Now we shall review some general lemmas from [2] about the logic L(Q) in order to apply them later on to PA(Q). For the moment, let L denote an arbitrary first order language. Following the notation in [2], if F is an arbitrary set of formulas of L(Q), then $\neg F = \{\neg\varphi : \varphi \in F\}$. A F-type is a subset $P \subseteq F \cup \neg F$ such that for all $\varphi \in F$, either $\varphi \in P$ or $\neg\varphi \in P$. If A is a model of L, then F(A) denotes the set of all types realized in A. The following lemma will play the main role in counting ω_1-like models.

LEMMA 2. (Lemma 5.4. in [2]). Let Γ be a set of sentences and F(x) a set of formulas of L(Q), and let $\sum_0(x_0)$, $\sum_1(x_1)$, ... be countably many sets of formulas of L(Q). Suppose Γ has a standard model A such that A omits each set $\sum_n(x_n)$ and F(A) is uncountable. Then there is a set M of standard models models of Γ such that $|M| = 2^{\omega_1}$, and each $B \in M$ omits each set $\sum_n$, and for any two distinct models $B, C \in M$, we have $F(B) \neq F(C)$, and in fact:

(1) neither $F(B) \subseteq F(C)$ nor $F(C) \subseteq F(B)$.

Now it should be clear what is our strategy for constructing a large number of ω_1-like models (possibly with some special properties, e.g. recursively saturated models) extending given countable model M of PA: we shall construct an ω_1-like model N extending M, and which realizes uncountably many types, and then apply above lemma. The model N will be obtained as a union of a continious ω_1-chain of e.e. extensions starting from M. To ensure a sufficient number of types realized in M, we shall use Gaifman's results on end-extension types. For the reader's convenience we recall the definition of end-extension types, cf [1] p. 242-243. A type t(v) over a model M, say of PA, is unbounded if $(\underline{a}<v) \in t(v)$ for every $a \in M$. t(v) is an end-extension type if it is unbounded, and if t' is a type over M and $t \subseteq t'$ then M(t') (M(t') is a model $N \supseteq M$ of PA generated by $M \cup \{b\}$, where b realizes t' in N) is an end-extension of M. In the next we shall use some properties of end-extension types, as they are stated in [1].

LEMMA 3. Let M be a countable model of PA. Then there is an ω_1-like model N such that $M \prec_e N$, and M realizes uncountably many types over M.

Proof Let A be a minimal model of PA such that $A \prec M$ (such a model exists since PA has built in Skolem functions). By Corollary 2.20 in [1] there are $|A|^{\omega}$ end-extension types over A, so there is a sequence $\langle t_\xi(v) : \xi < \omega_1 \rangle$ of end-extension types over A such that for $\xi, \zeta < \omega_1$

$t_\xi(v) \cup t_\zeta(v)$ is inconsistent. We now construct simultaneously two ω_1-sequences of types s_ξ and models M_ξ as folows. First we take $M_0 = M$, and $s_0(v) = t_0(v) \cup \{\underline{a} < v: a \in M_0\}$. We see that $s_0(v)$ is consistent as otherwise there are $a_1, \ldots, a_n \in M \setminus A$ such that

$$t_0(v) \vdash \neg(\underline{a}_1 < v \wedge \ldots \wedge \underline{a}_n < v), \quad \text{i.e.}$$

$$t_0(v) \vdash \neg \exists y_1 \ldots y_n (y_1 < v \wedge \ldots \wedge y_n < v).$$

But this is a contradiction since $t_0(v)$ is unbounded.

Further, for $\xi < \omega_1$ define $M_{\xi+1} = M_\xi(s_\xi)$, and at limit stages take $M_\xi = \bigcup_{\zeta<\xi} M_\zeta$, while $s_\xi(v) = t_\xi(v) \cup \{\underline{a} < v: a \in M_\xi\}$ for all $\xi < \omega_1$. By [1] $s_\xi(v)$ are end-extension types, so for $K = \bigcup_\xi M_\xi$ we have:

1° K is an ω_1-like model.

2° $M \prec_e K$.

3° K realizes uncountably many types over M (these are $s_\xi(v), \xi < \omega_1$). ∎

THEOREM 4. Every countable model of PA has 2 ω_1-like e.e extensions.

Proof If M is a countable model of PA, then by Lemma 3 there is an ω_1-like model which is an e.e. extension of M and which realizes uncountably many types over M. By Theorem 1, N is a standard model of PA(Q). Since $M \prec_e N$, the model N omits all types:

(1) $\sum_a(x) = \{x \neq \underline{b}: b < a\} \cup \{x < a\}, \quad a \in M.$

Therefore, by Lemma 2, there is a family T of size 2^{ω_1} of standard models of $PA(Q) \cup Th(M,m)_{m \in M}$ such that each $N \in T$ omits all types (1), i.e. $M \prec_e N$, and for distinct $B, C \in T$, $F(B) \neq F(C)$, i.e. $B \not\cong C$. By Theorem 1, models in T are ω_1-like. ∎

With litle change in the proof one can show the following variant of the above theorem.

THEOREM 5. If M is a countable model of PA then there is a family T of size 2^{ω_1} such that:

Each $A \in T$ is an ω_1-like e.e.extension of M.

If $A, B \in T$ and $A \neq B$ then neither A is embeddable in B nor B is embeddable in A.

This fact follows from the condition (1) of Lemma 2.

Now, one can try to obtain Kossak's result in [5]:

(K) There are 2^{ω_1} ω_1-like recursively saturated e.e. extensions of every countable recursive model.

In such an attempt we take the theory PA(S), cf [4], consisting of PA, induction scheme for all formulas of $L_S = L_{PA} \cup \{S\}$, S is an additional unary predicate symbol saying that S is a satisfaction class. Then by Theorem 1.4. in [4], countable models of PA(S) are exactly recursively saturated models of PA. Therefore, if M is a countable model of PA(S) and t is an end-extension type, then M(t) is recursively saturated. Then one would expect that the family T constructed as in Theorem 4 furnishes Kossak's result. But it may appear that reducts of models of T to the language L_{PA} are isomorphic, so the question of obtaining (K) in this way remains open. However, this attack rises the following question.

Let us introduce the equivalence relation in T defined by $A \sim B$ iff $A \restriction L_{PA} = B \restriction L_{PA}$, and let $\{T_i : i \in I\}$ be the corresponding partition of T. If $k = |I|$, then we have the following possibilities, assuming that 2^{ω_1} is a regular cardinal (like in the case of GCH for example):

1° If $k = 2^{\omega_1}$ then there are 2^{ω_1} nonisomorphic recursively saturated models extending M, i.e. Kossak's result follows immediately.

2° If $k < 2^{\omega_1}$ then there is a class T_i of the cardinality 2^{ω_1}, i.e.

(I) There is an ω_1-like model of PA with 2^{ω_1} inductive satisfaction classes.

Now we rise the problem: is (I) true?

References

1. H. Gaifman, Models and types of Peano's arithmetic, Annals of Mathematical Logic, 9(1976), 223-306.
2. H.J.Keisler, Logic with the Quantifier "there exist uncountably many", Annals of Mathematical Logic, 1(1970), 1-93.
3. R.Kossak, $L_{\infty\omega_1}$-elementary equivalence of ω_1-like models of PA, Fundamenta Mathematicae, CXXIII(1984), 123-131.
4. R.Kossak, A Note on Satisfaction Classes, Notre Dame Jour. of Formal Logic, Vol. 26(1985), No.1, 1-8.
5. R.Kossak, Recursively Saturated ω_1-like Models of Arithmetic, Notre Dame Jour. of Formal Logic, Vol. 26(1985), No. 4, 413-422.
6. Z.Mijajlovic, On the definability of the quantifier "there exist uncountably many", Studia Logica, XLIV, 3(1985), 258-264.
7. C.Smorinski, Recursively saturated nonstandard models of arithmetic, The Journal of Symbolic Logic, Vol. 46(1981), 259-286.

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

О БАЗИСЕ И ДЕФОРМАЦИЯХ НЕКОТОРЫХ АЛГЕБР ЛИ [I, 2]

Душан Пагон

Резюме. В статье рассматриваются деформации по Герстенхаберу одного класса градуированных алгебр Ли, близких к свободной алгебре Ли. Предлагается удобный алгоритм для построения базиса свободной алгебры Ли. Результаты, полученные ранее для почти свободных алгебр с одним определяющим соотношением второй степени, обобщены на случай одного однородного соотношения произвольной степени.

Введение. Известно, что классы изоморфизма нильпотентных алгебр Ли фиксированной размерности над некоторым полем определяются наборами параметров – элементов этого поля. Подходящим средством для изучения этих классов представляется понятие деформации алгебры, которое ввел М. Герстенхабер [I]. Это особого вида формальные степенные ряды, являющиеся такими же инвариантами алгебр Ли, как и их автоморфизмы или дифференцирования. Общих результатов о деформациях алгебр, к сожалению, пока получено сравнительно мало, хотя они изучались для различных классов алгебр Ли. В частности, нами исследованы деформации некоторых алгебр Ли, для которых можно в явном виде построить удобный для вычислений базис [2]. Для этого необходимо упорядочить множество образующих свободной алгебры Ли $L: e_1 < e_2 < \ldots < e_n$. Назовем число образующих, входящих в произвольное ассоциативное

I/ Статья печатается в окончательном виде и никакой ее вариант другим изданиям предлагаться не будет.

2/ Автор благодарит за помощь "Разисковална скупност Словение", контракт № CI-0501-101-8.

слово $u = e_{i_1} e_{i_2} \dots e_{i_k}$, его длиной: $|u| = k$ и пусть слова длины больше I будут упорядочены лексикографически. Будем к тому же считать каждое слово меньше любого его начала.

ОПРЕДЕЛЕНИЕ I. Ассоциативное слово u называется правильным, если для любого его разбиения $u = u'u''$ на два непустых подслова, имеет место неравенство $u > u''u'$.

Справедливо следующее утверждение, доказанное А.И. Ширшовым [3] :

УТВЕРЖДЕНИЕ I. Пусть L свободная алгебра Ли с образующими $e_1, e_2, \dots, e_n$ и $B \subset L$ ее подмножество, обладающее следующими свойствами:
(I) для любого $x \in B$ ассоциативное слово $\hat{x}$, полученное из x отбрасыванием скобок, является правильным;
(2) любой элемент множества B, длина которого больше I, является коммутатором двух элементов из B;
(3) если элемент $x \in B$ имеет вид $x = [[y,z],t]$, то $\hat{z} \leq \hat{t}$.
Тогда множество B является базисом алгебры L.

Оказывается, что на каждом правильном ассоциативном слове можно единственным образом расставить скобки так, чтобы получился некоторый элемент базиса B [3].

I. В дальнейшем нам понадобятся следующие два свойства ассоциативных слов:

ЛЕММА I. Любой конец произвольного правильного слова строго меньше этого слова.

Доказательство. Предположим, что конец слова u совпадает с некоторым началом этого слова:
а) $u = u'vu'$. Тогда из правильности слова u вытекает, что $u'u'v < u = u'vu'$ и $u'v < vu'$. Значит $u = u'vu' < vu'u'$ - противоречие.
б) $u = v'vv''$, где $v'v = vv'' = u'$. Отсюда $u'v' < u = u'v''$ и $v' < v''$. Поэтому получаем, что $u = v'u' = v'v'v < v''v'v$,

а это противоречит правильности слова u.

ЛЕММА 2. Если к произвольному правильному слову добавляется другое правильное слово, которое к тому же меньше первого, то полученное слово тоже будет правильным.

Доказательство. Рассмотрим отдельно каждый из трех возможных типов разбиения полученного слова.
а) $uv = u'u''v$ и согласно лемме I имеем $u''vu' < uvu' < uv$, что и требовалось доказать.
б) Аналогично в случае $uv = uv'v''$ получаем, что $v''uv < vu$.
в) Осталось убедиться, что $vu < uv$. Если слово v короче слова u, то это очевидно: $vu < uvu < uv$. В противоположном случае $v = v'v''$, где $|v'| = |u|$ и мы, применяя еще раз лемму I, получаем, что $vu = v'v''u \leq uv''u < uvu < uv$, чем доказательство леммы полностью закончено.

Теперь мы укажем эффективный алгоритм для построения определенного выше базиса B свободной алгебры Ли L, который заключается в последовательном получении базисных элементов произвольной длины.

ТЕОРЕМА I. Пусть уже построены все элементы базиса B, длина которых не превышает некоторого натурального числа k, и пусть u произвольное правильное слово длины $k+1$. Тогда элемент $x = [y,z] \in L$, для которого $\hat{x} = u$, принадлежит множеству B если и только если $\hat{z}$ самое длинное правильное слово, которое можно получить из u отнятием какого-то его начала, а y и z при этом принадлежат базису B.

Доказательство. Согласно утверждению I мы должны убедиться, что слово $\hat{y}$ также будет правильным, а элемент x будет удовлетворять пункту (3) этого утверждения.
Заметим, что неправильное слово может получиться из правильного слова u после отнятия какого-то его конца v только в следующих случаях:
а) $u = u'u' \dots u'v$, где u' - правильное слово строго больше v;
б) $u = u'u''u'v$, где u', u'' - правильные слова и $u' > u'' > v$.

Но в обоих случаях применяя лемму 2 получаем, что слово $u'v$ является правильным, а его длина строго больше длины слова $V = \hat{z}$, что противоречит предположениям теоремы.
Точно к такому же противоречию мы приходим, допуская что $y = [y', y'']$, $\widehat{y''} > \hat{z}$ и применяя еще раз лемму 2. Поэтому можем считать, что теорема полностью доказана.

2. Наша следующая цель найти удобный базис в алгебре $L_e = L / I(e)$, где $I(e)$ - идеал, порожденный произвольным нормированным однородным соотношением степени $d \geq 2$:

$e = \sum_{i=l}^{m} \alpha_i e_i = 0$, e_i при $i > n$ - лексикографически упорядоченные элементы базиса B , длина которых не убывает.

ОПРЕДЕЛЕНИЕ 2. Назовем элемент $x \in L$ регулярным, если он сам, а также все элементы, произведением которых он является, дают при отбрасывании скобок правильные ассоциативные слова.

ЛЕММА 3. Произвольный регулярный элемент $x \in L$ выражается через базисные элементы в следующем виде:

$x = e_i + \sum_{j<i} \pm e_j$, где $\hat{e}_i = \hat{x}$.

Доказательство. В ходе разложения элемента x по базису B нам приходится применять тождество Якоби и закон антикоммутативности, имеющие место в алгебрах Ли. В первом случае мы заменяем выражение $[[y', y''], z]$, где $\widehat{y''} > \hat{z}$ на сумму $[[y', z], y''] + [y', [y'', z]]$. Здесь второе слагаемое дает при опускании скобок то же правильное слово, что и исходное выражение. Из первого же слагаемого получается строго меньшее слово, поскольку согласно лемме 2 $zy'' < y''z$, а значит и $y'zy'' < y'y''z$. По той же причине мы получим слова меньше $\hat{x}$ и если будем применять правило антикоммутативности.

СЛЕДСТВИЕ 1. Заменим каждый из базисных элементов e_i , для которого $\hat{e}_m$ является подсловом $\hat{e}_i$, на элемент e_i', полученный из e_i в результате следующих действий:

(а) сдвиг левых скобок, не содержащихся в e_m , но находящихся внутри выражения $q < e_i$, $\hat{q} = \hat{e}_m$, в начало этого выражения;

(б) добавление в начале выражения q стольких левых скобок, сколько их было сдвинутых, и в конце q такого же количества правых скобок;

(в) замена вхождений элемента e_m на элемент e ;

(г) отбрасывание двойных скобок, если они образовались.

Полученное таким образом из B множество B' также будет базисом алгебры L .

Доказательство. Это вытекает непосредственно из утверждения I и леммы 3 .

Воспользуемся теперь еще одним утверждением, доказанным А.И. Ширшовым [4]:

УТВЕРЖДЕНИЕ 2. Если элемент $x \in L$ принадлежит идеалу $I(e)$, то старшее асоциативное слово, полученное после разложения x по базису B , и отбрасывания скобок, содержит слово $\hat{e}_m$.

На основании следствия I и последнего утверждения получаем следующее описание базиса алгебры L_e :

СЛЕДСТВИЕ 2. Множество $\widetilde{B}$, полученное из B' отбрасыванием элементов e_i' , будет базисом подпространства $\widetilde{L} \subset L$, изоморфного пространству алгебры L_e .

Обозначим через x_0 и x_I $I(e)$- и $\widetilde{L}$-компоненты произвольного элемента $x \in L$, и пусть π будет канонический эпиморфизм алгебры L на алгебру L_e . Прообраз произвольного элемента $a \in L_e$ при этом отображении будем обозначать через $a^{-1} \in \widetilde{L}$, а в качестве базиса алгебры L_e мы выберем множество $B_e = \pi(\widetilde{B}) = \{E_i = \pi(e_i) : e_i \in \widetilde{B}\}$.

3. Теперь мы в состоянии приступить к изучению деформаций алгебры L_e. Пусть $f \in C^2(L_e, L_e)$ будет произвольная градуированная 2-коцепь, а φ линейное отображение алгебры L_e в себя, определенное нами следующим образом: ограничение φ на подпространство элементов длины I - $\varphi^* = \varphi / L_1$ - это некоторый эндоморфизм этого пространства, а для других базисных элементов $E_i = [E_{i'}, E_{i''}] \in B_e$ полагаем

$\varphi(E_i) = [\varphi(E_{i'}), E_{i''}] + [E_{i'}, \varphi(E_{i''})] - f(E_{i'}, E_{i''})$.

Тогда коцепь $\tilde{f} = f - \delta\varphi$ будет действовать нулевым образом на парах слов $(E_i, E_j) \in B_e \times B_e$, $E_i > E_j$, таких что $[E_i, E_j]$ принадлежит B_e. Кроме того, если $E_m = [E_{m'}, E_{m''}]$, то мы имеем: $\tilde{f}(E_{m'}, E_{m''}) = f(E_{m'}, E_{m''}) - [\varphi(E_{m'}), E_{m''}] - [E_{m'}, \varphi(E_{m''})] - \sum_{i=l}^{m-1} \alpha_i \varphi(E_i)$.

Следовательно, размерность пространства
$V_d = \left\langle \tilde{f}(E_{m'}, E_{m''}) : \tilde{f} \in C^2_{gr}(L_e, L_e) / B^2_{gr}(L_e, L_e) \right\rangle$
равна
$M = \dim L_d - \dim \left\langle [\varphi(E_{m'}), E_{m''}] + [E_{m'}, \varphi(E_{m''})] + \sum_{i=l}^{m-1} \alpha_i \varphi(E_i) : \varphi^* \in End(L_1) \right\rangle$.

Наша цель доказать, что дополнительные условия, наложенные на коцепь $\tilde{f}$ в предположении, что она является коциклом, служат исключительно для определения значения $\tilde{f}$ на парах базисных слов $(E_i, E_j) \neq (E_{m'}, E_{m''})$, $E_i > E_j$, $[E_i, E_j] \notin B_e$, то есть имеет место следующая

ТЕОРЕМА 2. $H^2_{gr}(L_e, L_e) = M$.

Доказательство. Заметим сначала, что из тривиальности второй группы градуированных когомологий для свободной нильпотентной алгебры Ли [5] вытекает, что $f(E_i, E_j) = 0$ на парах $(E_i, E_j) : |\hat{e}_i| + |\hat{e}_j| < d$, для любого $f \in H^2_{gr}(L_e, L_e)$. Определим для произвольного элемента $y \in V_d$ линейный оператор $A_y \in End(L)$, который переводит каждый из базисных элементов e_i' в сумму элементов, полученных из e_i' заменой какого-то вхождения элемента e на элемент y, а на базисных элементах $e_i \in \tilde{B}$ действует нулевым образом. Докажем, что тогда 2-коцепь f^y, определенная как $f^y(E_i, E_j) = \pi A_y [e_i, e_j]$, является коциклом. Для этого заметим, что

$[\pi A_y [e_i, e_j], E_k] = \pi [A_y [e_i, e_j], e_k] = \pi A_y [[e_i, e_j]_0, e_k]$

и $[E_i, E_j]^{-1} = [e_i, e_j]_1$, поэтому

$\pi A_y [[E_i, E_j]^{-1}, e_k] + [\pi A_y [e_i, e_j], E_k] = \pi A_y [[e_i, e_j], e_k]$.

Отсюда применяя тождество Якоби получаем, что

$(f^y \circ F + F \circ f^y)(E_i, E_j, E_k) = \pi A_y (F \circ F(e_i, e_j, e_k)) = 0$,

где $f \circ g(x, y, z) = f(g(x, y), z) + f(g(y, z), x) + f(g(z, x), y)$

и $F(x, y) = [x, y]$. Следовательно $f^y \in Z^2_{gr}(L_e, L_e)$.

Пусть теперь $\{y_1, y_2, \ldots, y_M\}$ - какой-то базис пространства V_d. Докажем, что тогда $\{f^{y_1}, f^{y_2}, \ldots, f^{y_M}\}$ будет базисом пространства $H^2_{gr}(L_e, L_e)$. Линейная независимость указанных коциклов, очевидно, вытекает из того, что $f^{y_i}(E_{m'}, E_{m''}) = y_i$. Проверим, что они являются полной системой. Возьмем произвольный нетривиальный градуированный коцикл f, для которого $f(E_{m'}, E_{m''}) = 0$. Мы уже знаем, что $f(L_{k'}, L_{k''}) = 0$, если $k' + k'' < d$. Покажем, что $f(L_k, L_{d-k}) = 0$. Если $E_i = E_n$, $E_j = E_n^{d-2} E_{n-1}$, то либо $[E_i, E_j] \in B_e$, либо $[E_i, E_j] = E_m$, значит $f(E_i, E_j) = 0$. То же самое рассуждение применимо если $E_i > E_j$ и $|E_i| = 1$, или $E_i = [E_{i'}, E_{i''}]$, $E_{i''} \leq E_j$. В оставшемся случае, когда $[E_i, E_j] \notin B_e$, из условия коцикличности получаем

$f(E_i, E_j) = f([E_{i'}, E_j], E_{i''}) + f(E_{i'}, [E_{i''}, E_j])$.

Внутренние коммутаторы раскладываются по базисным элементам, строго большим E_j, поэтому для завершения доказательства достаточно применить индукцию по высоте элемента E_j. Рассмотрим, наконец, случай $k' + k'' > d$. Применим основную индукцию по суммарной длине слов E_i, E_j и дополнительную по высоте слова $\hat{e}_i \hat{e}_j$. Основание для дополнительной индукции у нас тоже имеется, поскольку $\pm E_1^t E_2$ либо элемент базиса, либо 0. Согласно индуктивным предположениям:

$f([E_{i'}, E_{i''}], E_j) = f(E_{i'}, [E_{i''}, E_j])$ и

$f(E_i, [E_{j'}, E_{j''}]) = f([E_i, E_{j'}], E_{j''})$.

Поскольку коммутатор $[E_i, E_j] = [[E_{i'}, E_{i''}], E_j]$, где $E_{i''} > E_j$, приводится к $[E_{\tilde{i}}, E_{\tilde{j}}] \in B_e$, то для таких пар $f(E_i, E_j) = 0$. Если же в слово $\hat{e}_i \hat{e}_j$ входит $\hat{e}_m$, то мы сначала можем добиться того, чтобы оно полностью входило либо в $\hat{e}_i$, либо в $\hat{e}_j$, а за-

тем мы, заменяя его суммой $\sum_{s=\ell}^{m-1}(-\alpha_s)\,e_s$, согласно лемме 3, понизим высоту $\hat{e}_i\hat{e}_j$, попадая тем самым в условия дополнительной индукции. Значит, теорема полностью доказана.

4. В заключение рассмотрим вопрос о продолжаемости найденых локальных деформаций алгебры L_e.

ТЕОРЕМА 3. Для любого элемента $y \in V_d$ коцикл f^y продолжаем, причем s-тое продолжение задается формулой

$$f_s^y\,(E_i,\ E_j) = \pi A_y^s [e_i,\ e_j] .$$

Доказательство. Согласно отмеченным выше свойствам отображений π и A_y, получаем что

$$\pi A_y^s [[e_i, e_j], e_k] =$$

$$= \pi A_y^s [[e_i, e_j]_I, e_k] + \pi A_y^s [[e_i, e_j]_0, e_k] =$$

$$= f_s^y([E_i, E_j], E_k) + \pi A_y^{s-1}[A_y[e_i, e_j], e_k] =$$

$$= f_s^y(F(E_i, E_j), E_k) + f_{s-1}^y(f_1^y(E_i, E_j), E_k) + \pi A_y^{s-1}[(A_y[e_i, e_j]_0, e_k] =$$

$$= \ldots = \sum_{r=0}^{s} f_{s-r}^y(f_r^y(E_i, E_j), E_k).$$

Поэтому, воспользовавшись тождеством Якоби, получим требуемый результат:

$$\sum_{r=0}^{s} f_{s-r}^y \circ f_r^y\,(E_i, E_j, E_k) = \pi A_y^s\, FoF(e_i, e_j, e_k) = 0 .$$

ЛИТЕРАТУРА

1. M. Gerstenhaber, On the deformation of rings and algebras, Ann. of Math. 1 (1964), 59-103 .
2. Д. Пагон, Градуированные деформации почти свободных алгебр Ли, Вестн. Моск. ун-та. Матем., механ. 5(1982), 66-70.
3. А.И. Ширшов, О свободных кольцах Ли, Мат. сб.2 (1958), 113-122.
4. А.И. Ширшов, Некоторые алгоритмические проблемы для алгебр Ли, Сиб. мат. жур. 2 (1962), 292-296.
5. Д. Пагон, О деформациях нильпотентных градуированных алгебр Ли, Вестн. Моск. ун-та. Матем., механ. 4 (1981), 50-54 .

DUŠAN PAGON
Pedagoška fakulteta
62000 MARIBOR

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

ON ADDITIVE POWER MAPS OF RINGS

Veselin Perić, Sarajevo

Abstract. Let R be an associative nonzero ring with additive power map $f_m: x \mapsto x^m$ ($x \in R$) for some natural number $m > 1$. It can be elementary prowed that the set N of all nilpotent elements in R is an ideal of R [8]. This fact and also the commutativity of the ring R/N follows immediately from a nontrivial result of I. N. Herstein [5], [6] (see also [1], [2]). Moreover, it is easy to see that if R is locally unitary then R is of squere-free characteristic char(R) dividing k^m-k for all positive integers k, hence for all prime factors p of char(R), p-1 divides m-1. Assuming that R is locally unitary and that, for every prime factor p of char(R), there is a natural number $m(p) > 1$ such that $f_{m(p)}$ is additive, we prove here: i) If m(p) is not a p-power then the ring R/N is a subdirect sum of finite fields R_i ($i \in I$) whose characteristics p_i ($i \in I$) divide char(R), hence also $k^{m(p)}-k$ for all posiive integers k and all prime factors p of char(R); ii) If, especially, m(p) is not divisible by p, then N = 0; iii) In both cases i) and ii) R is periodical, in fact there exists an integer $n > 1$ such that, for all x in R, $x^{mn} = x^m$ in the case i), and $x^n = x$ in the case ii), where $m = \max\{m(p): p \text{ prime factor of } \mathrm{char}(R)\}$; iv) For R as in i) and m as in iii), $S := \{x^m + y: x \in R,\ y \in N\}$ is a locally unitary subring of R and the restriction of f_m on S is a ring endomorphism. The results i), ii) and iii) improve some recent results of the author [9], and iv) gives a partial answer to a question recently posed by H. Bell [4].

1. INTRODUCTION

We consider here an associative nonzero ring R and denote by N the set of all nilpotent elements of R. We will frequently assume that R is locally unitary, i.e. for every x in R there is an idempotent e_x in R such that $e_x.x = x.e_x = x$.

This paper is in final form and no version of it will be submitted for publication elsewhere.

This research was supported by SIZ nauke SR BiH.

Subject class.: 16 A 70.

Key words: Additive power map; subdirest sum of finite fields; periodical ring.

For our purpose the idempotency of e_x is not essencial and thus "locally unitary" will actually means the same as "s-unitary".
We assume that there exists a natural number $m>1$ such that the power map $f_m: x \mapsto x^m$ $(x \in R)$ is additive, i.e. such that R satisfies the identity

(1) $$(x + y)^m = x^m + y^m .$$

The following wellknown result is due to I. N. Herstein [5], [6]. His proof is not elementary at all (see also [1], [2]).

THEOREM A. If an associative ring R satisfies the identity (1) for a given natural number $m>1$, then the commutator ideal of R is a nil ideal, i.e. N is an ideal of R and the ring R/N is commutative.

In [8] we gave an elementary proof of the following lemma.

LEMMA B. Let R be an associative ring satisfying the identity (1). If $m>1$, then N is an ideal of R.

Recently we proved in [9] also in an elementary manner, the following propositions.

THEOREM C. Let an associative locally unitary nonzero ring R satisfy the identity (1) for some integer $m>1$ not a prime power. Then N is an ideal of R and the ring R/N is a subdirect sum of finite fields R_i $(i \in I)$ whose characteristics p_i $(i \in I)$ divide 2^m-2.

THEOREM D. Let R be an associative locally unitary nonzero ring satisfying the identity (1). If $m>1$ is relatively prime to $2^m - 2$, then $N = 0$ and R is a subdirect sum of finite fields R_i $(i \in I)$ whose characteristics p_i $(i \in I)$ divide $2^m - 2$.

THEOREM E. Let an associative locally unitary nonzero ring R satisfy the identity (1) for two values of m: $m = s>1$ and $m = t>1$. If s, t, $2^s - 2$ and $2^t - 2$ are relatively prime, then $N = 0$ and R is a subdirect sum of finite fields R_i $(i \in I)$ whose characteristics p_i $(i \in I)$ divide $2^s - 2$ and $2^t - 2$.

THEOREM F. Let R be a ring as in theorem D or E. Then there is a natural number $n>1$ such that $x^n = x$ for all x in R.

THEOREM G. Let R be a ring as in theorem C. Then there is a natural number $n>1$ such that $x^{mn} = x^m$ for all x in R.

In the proof of theorem C actually was proved the following lemma.

LEMMA H. Let an associative locally unitary nonzero ring R satisfy the identity (1) for some natural number $m>1$. Then R has a nonzero characteristic char(R) dividing $k^m - k$ for all integers $k>1$. Moreover, N is an ideal of R and the ring R/N is a subdirect sum of (noncommutative) integral domains R_i $(i \in I)$ whose characteristics p_i $(i \in I)$ divide char(R).

The proposition 2 in [9] could be stated as this lemma.

LEMMA K. Let R be an integral domain satisfying the identity (1). If $m>1$ is not a p-power for $p = \mathrm{char}(R)$, then R is a finite field of characteristic p dividing $k^m - k$ for all integers $k>1$.

In the Section 2 we improve theorem C proving theorems 2 and 5. Similarly we improve also theorems D and E (see theorems 4 and 6). In the Section 3 we extend the assertion of theorems F and G to the situation of theorems 4, 6 and 2, 5 respectively (see theorems 7 and 8).
In the last Section 4 of this note we consider a question recently posed by H. Bell [4] and give a partial answer to this question (see theorem 11).

2. ADDITIVE POWER MAPS AND SUBDIRECT SUM REPRESENTATIONS

We start with the following lemma.

LEMMA 1. Let R be an associative locally unitary nonzero ring satisfying the identity (1) for some integer $m>1$. Then N is an ideal of R and R is of nonzero characteristic char(R) satisfying condition

(2) char(R/N) = char(R) *divides* k^m-k *for all* $k>1$. *Moreover, for every prime factor* p *of* char(R), p-1 *divides* m-1 *and* m_p-1, *where*

$$m = p^{k_p}.m_p,\ p \nmid m_p.$$

If m *is even, then* char(R) = 2.

Proof. By lemma B, N is an ideal of R, and in view of lemma H, R has a nonzero characteristic char(R) which divides k^m-k for all integers $k>1$. To prove (2) it suffices to prove that

$$\text{char}(R/N).x = 0 \quad (x \in R).$$

In one hand

$$(\text{char}(R/N).e_x)^k = 0 \quad (k = k(x) \text{ an integer}),$$

since $\text{char}(R/N).e_x \in N$ for all x in R. But since $m>1$, this will be valid for some m-power $k = m^j$ (j = j(m) an integer). On the other hand, in view of (1),

$$(\text{char}(R/N).e_x)^{m^j} = \text{char}(R/N).e_x^{m^j},$$

hence

$$\text{char}(R/N).x = (\text{char}(R/N).e_x)^{m^j}.x = 0$$

for all x in R.

We prove now that char(R) is squere-free. In fact, for q the product of all different prime factors of 2^m-2, q is squere-free and by (1)

$$(q.e_x)^m = q.e_x^m \quad (x \in R).$$

But,

$$(q.e_x)^m = q^m.e_x^m = 0 \quad (x \in R),$$

since 2^m-2 divides q^m. Hence,

$$q.e_x^m = 0, \text{ i.e. } q.x = 0 \quad (x \in R).$$

Since char(R) divides q, char(R) is also squere-free.

Finally, for every prime factor p of char(R), p divides $k^m-k = k.(k^{m-1}-1)$ for all integers $k>1$. For p = 2, then surely p-1 divides m-1 and m_p-1. For p odd, p must divides $k^{m-1}-1$, hence p-1 divides m-1 if we take k of the order p-1 in the multiplicative group Z_p^*. From

$$m - 1 = p^{k_p}.m_p - 1 = p^{k_p}(m_p-1) + p^{k_p} - 1$$

follows that p-1 divides m_p-1 too.

If m is even, then for no odd prime p, p-1 can divide m-1,

hence in this case char(R) = 2. But we can conclude also in the following manner. For m even, from (1) it follows $2e_x^m = 0$, hence 2x = 0 for all x in R, and thus char(R)=2.

Now we can state the following improvment of theorem C.

THEOREM 2. *Let* R *be an associative locally unitary nonzero ring satisfying the identity* (1) *for some integer* $m>1$. *If* m *is a* p*-power for no prime factor* p *of* char(R), *then* N *is an ideal of* R *and the ring* R/N *is a subdirect sum of finite fields* R_i $(i \in I)$ *whose characteristics* p_i $(i \in I)$ *divide* char(R), *hence also* k^m-k *for all integers* $k>1$.

Proof. According to lemma H, N is an ideal of R and R/N is a subdirect sum of (noncommutative) integral domains R_i $(i \in I)$ whose characteristics p_i $(i \in I)$ divide char(R). By the assumption, $m>1$ is not a p_i-power $(i \in I)$, hence in view of lemma K, R_i $(i \in I)$ is a finite field and p_i divides k^m-k for all integers $k>1$.

COROLLARY 3. *Let* R *be an associative locally unitary nonzero ring satisfying the identity* (1) *for some integer* $m>1$. *If* m *iz even, but not of the form* 2^j $(j=1,2,\ldots)$, *then* N *is an ideal of* R *and the ring* R/N *is a subdirect sum of finite fields* R_i $(i \in I)$ *of characteristics* $p_i=2$ $(i \in I)$. *For* m = 2, R *is commutative*.

Proof. If m is even, then char(R) = 2 by lemma 1. If moreover m is not of the form 2^j $(j=1,2,\ldots)$, then by theorem 2, N is an ideal of R and the ring R/N is subdirect sum of finite fields R_i $(i \in I)$ of characteristics $p_i = 2$ $(i \in I)$. For m=2, we cannot use theorem 2. But in this case R is commutative, because of $(x+y)^2 = x^2+y^2$, i.e. xy + yx = 0 for all x,y in R and char(R) being equal to 2.

Let now R be an associative locally unitary nonzero ring with nonzero characteristic char(R). If R satisfies the identity (1) for some integer $m>1$ such that R is m-torsion free, then all condition of theorem 2 are fulfiled. Namely, in this case $p \nmid m$ for all prime factors p of char(R). Suppo-

se, that $p \mid m$ for some prime factor p of char(R). Then there exists an y in R such that $p^{-1}\text{char}(R).y \neq 0$. But in this case, for $x = p^{-1}\text{char}(R).y$ we have $x \neq 0$ and $mx = (mp^{-1})\text{char}(R).y = 0$, which is not possible, since R is m-torsion free.
Moreover, in this special case we have also N = 0. In fact, as in the proof of ([9], Th. 3) we have mx = 0 for all x in R with $x^2 = 0$.
Hence we have proved the following result.

THEOREM 4. Let an associative locally unitary nonzero ring R satify the identity (1) for some integer $m>1$. If R is m-torsion free, then N = 0 and R is a subdirect sum of finite fields R_i $(i \in I)$ whose characteristics p_i $(i \in I)$ divide char(R), hence also k^m-k for all integers $k>1$.

It is well known that, under conditions of theorem 4, N=0 and the ring R is commutative (see for inst. [4], L. 1(c)). The proof of this fact is not elementary, since it make use of a nontrivial result of H. Bell ([3], Th. 5). We remark, that this fact can be also derived from theorem A. But this fact is a corollary of our elementary proved theorem 4.

Since an associative locally unitary nonzero ring R satisfying the identity (1) for some integer $m>1$ is surely m-torsion free if m is relatively prime to 2^m-2, theorem D is also a corollary of theorem 4. Moreover, instead of primness of m to 2^m-2, it suffices that m, 2^m-2, 3^m-3, ... are relatively prime to conclude that R is m-torsion free.

Let now R be an associative locally unitary nonzero ring of nonzero characteristic char(R). Suppose that for every prime factor p of char(R) there exists an integer $m(p)>1$ not a p-power such that the power map $f_{m(p)}$ is additive on R. Then by notations of lemma H and in view of lemma K, each of the integral domains R_i $(i \in I)$ is a finite field of characteristic p_i $(i \in I)$ dividing char(R), hence also $k^{m(p)}-k$ for all integers $k>1$ and all prime factors p of char(R). Thus, the following theorem is valid.

THEOREM 5. Let R be an associative locally unitary nonzero ring of characteristic char(R). Suppose that for every prime factor p of char(R) there is an integer $m(p)>1$ not a p-power such that the power map $f_{m(p)}$ is additive on R. Then N is an ideal of R and the ring R/N is a subdirect sum of finite fields R_i $(i \in I)$ whose characteristics p_i $(i \in I)$ divide char(R), hence also $k^{m(p)}-k$ for all prime factors p of char(R) and all integers $k>1$.

For $\{m(p)$: p prime factor of char(R)$\}$ a singleton $\{m\}$, we are in the situation of theorem 2, which is a special case of theorem 5.

Let now by notations of theorem 5, for every prime factor p of char(R), $m(p)>1$ be not divisible by p. Then, for every x in R with $x^2 = 0$ we derive $m(p).x = 0$ for all prime factors p of char(R), and from this it follows that x = 0. Hence we have the following theorem.

THEOREM 6. Let R be an associative locally unitary nonzero ring of nonzero characteristic char(R). Suppose that for every prime factor p of char(R) there is an integer $m(p)>1$ not divisible by p, such that the power map $f_{m(p)}$ is additive on R. Then N = 0 and R is a subdirect sum of finite fields R_i $(i \in I)$ whose characteristics p_i $(i \in I)$ divide char(R), hence also $k^{m(p)}-k$ for all prime factors p of char(R) and all integers $k>1$.

For $\{m(p)$: p prime factor of char(R)$\}$ a singleton $\{m\}$, from theorem 6 imediately follows theorem 4. But theorem E is also a corollary of theorem 6. Namely, in the situation of theorem E we can take m(p) = s or m(p) = t, since every prime factor p of char(R) divide 2^s-2 and 2^t-2, hence $p \nmid s$ or $p \nmid t$ in view of the fact that s, t, 2^s-2 and 2^t-2 are relatively prime.

3. ADDITIVE POWER MAPS AND PERIODICITY OF RINGS

Our purpose is to prowe that a ring R satisfying condition in any of theorems 2, 4, 5 or 6 is periodical. More preci-

sely, we will prove the following two theorems.

THEOREM 7. For a ring R as in theorem 4 or 6 there is a natural number $n>1$ such that $x^n = x$ for all x in R.

THEOREM 8. For a ring R as in theorem 2 or 5 there is a natural number $n>1$ such that $x^{mn} = x^m$ for all x in R, where $m = \max\{m(p)$: p prime factor of char(R)$\}$ in the case of theorem 5.

The proof of theorem 7 is the same as the proof of theorem D ([9], Th. 6) and will be omited.

For the proof of theorem 8, which is similar to the proof of theorem G ([9], Th. 7), we need the following lemma.

LEMMA 9. If R is a ring as in theorem 2 or 5, then $x^m = 0$ for all x in N, where $m = \max\{m(p)$: p prime factor of char(R)$\}$ in the case of theorem 5.

The above lemma follows from the next somewhat more general result.

LEMMA 10. Let an associative locally unitary nonzero ring R satisfy the following conditions:

i) There is a sqere-free positive integer q such that $qx = 0$ for all nilpotent elements x in R;

ii) For every prime factor p of q there exist integral numbers $a_1, a_2, \ldots, a_{r(p)}$ (depending on p and) not all divisible by p, such that

$$a_1x + a_2x^2 + \ldots + a_{r(p)}x^{r(p)} = 0$$

for all nilpotent elements x in R.

Then $x^r = 0$ for all nilpotent elements x in R, where $r = \max\{r(p)$: p prime factor of q$\}$.

Proof. Let x be an arbitrary element in N. If $x = 0$ it is nothing to prove. Assume that $x \neq 0$. The subring X of R generated by x is (commutative and) of nonzero characteristic char(X) dividing q. Hence, because of i), X is a direct sum $X = X_1 \dotplus \ldots \dotplus X_k$ of rings X_j of prime characteristics p_j dividing q. Since $x = x_1 + \ldots + x_k$ $(x_j \in X_j)$ we have $x^r = x_1^r + \ldots + x_k^r$, and it suffices to show that

$x_j^r = 0$ $(j=1,2,\ldots,k)$. Every x_j is of course nilpotent. Thus, by ii), there exist integral numbers $a_1,\ldots,a_{r(p_j)}$ not all divisible by p_j, such that

$$a_1x_j + \ldots + a_{r(p_j)}x_j^{r(p_j)} = 0.$$

If a_i is the first coefficient which is not divisible by p_j, then using the above equation we can express x_j^i as a linear combination with integral coefficients of $x_j^{i+1}, \ldots, x_j^{r(p_j)}$. But this implies that $x_j^i = 0$, nence $x_j^r = 0$.

In the case of theorem 2 or 5 the conditions i) and ii) are satisfied, since by lemma 1 we can take $q = \mathrm{char}(R)$, $r(p) = m(p) - 1$, $a_1 = \binom{m(p)}{1}, \ldots, a_{r(p)} = \binom{m(p)}{r(p)}$.

The idea of the proof of lemma 10 is essentially that of ([4], L. 1(b)), a result similar to lemma 9 and stated for $m>1$ not a prime power.

Now we can return to the proof of theorem 8. As in the proof of ([9], Th. 6) we can see that there is an integer $n>1$ such that $x - x^n \in N$ for all x in R. In view of (1) and lemma 9 this implies $x^m = (x^n + y)^m = x^{mn} + y^m = x^{mn}$ for all x in R, where $y = x - x^n \in N$.

The assertion in lemma 9 can be sharped in the following manner.

LEMMA 9′. Let R be a ring as in theorem 2 or 5 and let

$$m(p) = p^{k_p}.m_p, \quad p \nmid m_p$$

for every prime factor p of char(R). Then $x^{m'} = 0$ for all nilpotent elements x in R, where $m' = \max\{p^{k_p}$: p prime factor of char(R)$\}$.

Proof. By lemma 1, char(R) is a product of differnt prime factors, say $\mathrm{char}(R) = p_1.p_2\ldots p_k$. Hence, R is a direct sum $R = R_{p_1} \dotplus \ldots \dotplus R_{p_k}$ of associative locally unitary nonzero rings R_{p_j} $(j=1,2,\ldots,k)$ of characteristics p_j $(j=1,2,\ldots,k)$.

We will show that, for every prime factor p of char(R),

$$x^{p^{k_p}} = 0 \quad (x \in N_p),$$

where N_p is the set of all nilpotent elements in R_p.

Namely, for $x \in R_p$,

$$(x^{p^{k_p}})^{m_p} + (e_x^{p^{k_p}})^{m_p} = x^{m(p)} + e_x^{m(p)} = [(x+e_x)^{p^{k_p}}]^{m_p} =$$

$$= (x^{p^{k_p}} + e_x^{p^{k_p}})^{m_p},$$

since x and e_x commute in R_p and $\mathrm{char}(R_p) = p$. Suppose that $x^{p^{k_p}} \neq 0$. Then there is a positive integer t such that

$$(x^{p^{k_p}})^t = 0, \text{ and } (x^{p^{k_p}})^{t-1} \neq 0.$$

But from

$$[(x^{t-1})^{p^{k_p}} + (e_x^{t-1})^{p^{k_p}}]^{m_p} = [(x^{t-1})^{p^{k_p}}]^{m_p} + [(e_x^{t-1})^{p^{k_p}}]^{m_p}$$

and $(x^{p^{k_p}})^t = 0$ it follows

$$m_p \cdot (x^{p^{k_p}})^{t-1} = 0.$$

Since $p \nmid m_p$, this implies

$$(x^{p^{k_p}})^{t-1} = 0,$$

hence a contradiction.

We remark that $m' < m = \max\{m(p)$: p prime factors of $\mathrm{char}(R)\}$ in the case of theorem 2 or 5, and $m' = 1$ in the case of theorem 4 or 6 in according with $N = 0$.

4. ADITIVE POWER MAPS AND RING ENDOMORPHISMS

If an associative ring R with additive power map f_m $(m > 1)$ is commutative, then f_m is obviously a ring endomorphism. For instance, this is the case if R is as in theorem 4 or 6. It may be somewhat interesting the question recently posed by H. Bell [4]: when an additive power map f_m $(m > 1)$ of an associative ring R is a ring endomorphism.

We list and comment here some results of H. Bell concerning this question.

By a result of Hirano and Tominaga ([7], L. 1), for an additive power map f_m $(m > 1)$ of an associative ring R there is a positive integer k such that $[x,y]^k = 0$ for all x,y in R, where $[x,y]$ denotes the commutator $xy-yx$ of x and y. Using this result H. Bell proved for an associative ring R with additive power map f_m $(m > 1)$ the folloving propositions:

(a) There exists a positive integer k for which f_m^k is a ring endomorphism ([4], Th. 1);

(b) If R is unitary and m is not of the form 2^j $(j \geq 2)$, then f_m^2 is a ring endomorphism ([4], Th. 3);

(c) f_m is a ring endomorphism if and only if $x^m \in Z$ the centrum of R for all x in R, assuming that R is unitary and

i) R is 2-torsion free ([4], L. 3) or

ii) m is odd ([4], Th. 2);

(d) If R is unitary and m is odd and squere-free, then f_m is a ring endomorphism ([4], Th. 4).

As mentioned by Bell ([4], Remark 5), the above propositions "R is unitary" can be replaced by " R is s-unirary". We remark that the proof of (a) and also of the "only if" part in (c) make use of the nontrivial theorem A. For (b) and the "if" part in (c) ii) it was used the in theprem 4 elementary proved fact ([4], L. 1(c)) that in the case of this theorem the ring R is commutative. For (b) was also used a fact ([4], L. 1(b)) following from the elementary lemma 9. For (d), besides of some elementary resoning, was used only "if" part of (c) in ii).

Hence, (b), (d) and the "if" part in (c) can be proved elementary too.

Now we can prove in an elementary manner the following theorem giving a partial answer to the above question of H. Bell. Let as mention that, in the case of theorem 5, $m = \max\{m(p)$: p prime factor of $\mathrm{char}(R)\}$ is not of the form 2^j $(j \geq 1)$. Namely, for $m = 2^j$ $(j \geq 1)$, $\mathrm{char}(R) = 2$ and $m = m(2)$ is not a 2-power, hence we are then in the situation of theorem 2.

THEOREM 11. Let R be asin theorem 2 or 5. In the situation of theorem 5 we denote by m the $\max\{m(p)$: p prime factor of $\mathrm{char}(R)\}$. Them S: $\{x^m+y$: $x \in R$, $y \in N\}$ is a locally unitary nonzero subring of R and the restriction of f_m on S is a ring endomorphism.

Proof. By theorem 2 or 5, N is an ideal of R and the ring R/N is commutative. Hence,

$$x^m.y^m = (xy)^m + z$$

for x,y in R and for appropriate z in N. Thus, S is closed under multiplication. From

$$(x-y)^m = x^m - y^m \quad (x,y \in R)$$

and the fact that N is an ideal of R folows that S is a subring of R.

Obvously, S is nonzero and locally unitary.

Let now $u = x^m + y$, $v = x_1^m + y_1$ $(x,x_1 \in R,\ y,y_1 \in N)$ be arbitrary elements in S. Then clearly

$$(u + v)^m = u^m + v^m.$$

But also

$$(uv)^m = u^m v^m.$$

Namely,

$$(uv)^m = (x^m x_1^m + x^m y_1 + y x_1^m + y y_1)^m = (x^m x_1^m)^m =$$

$$= ((xx_1)^m + z)^m = (xx_1)^{m^2},$$

since $x^m y_1 + y x_1^m + y y_1 \in N$ and $z^m = 0$ for all $z \in N$ by lemma 9. In the case of theorem 5, m is surely not of the form 2^j $(j \geq 1)$, and in the case of theorem 5, as allready mentioned m is also not of this form. Therefore, in view of (b)

$$(xx_1)^{m^2} = x^{m^2} x_1^{m^2} = (x^m + y)^m.(x_1^m + y_1)^m = u^m v^m,$$

hence $(uv)^m = u^m v^m$.

Remark 12. In the situation of theorem 11, by theorem 8 there is an integer $n > 1$ such that $x = x^n + y$ for all x in R and an appropriate y in N depending on x. From this easily follows that

$$x = x^{k.(n-1)+1} + y_k$$

for all positive integers k, where y_k is an appropriate element in N depending on x and k. If $k.(n-1)+1$ is a multiple of m for some positive integer k, then the above equation implies that S = R. Hence, in this cas, f_m is a ring endomorphism of R.

REFERENCES

1. H. E. Bell, On commutativity theorem of Herstein, Arhc. Math. 21(1970), 265-267.
2. _____, On some commutativity theorems of Herstein, Arch. Math. 24(1973), 34-38.
3. _____, On the power map and ring commutativity, Cand. Math. Bull. 21(1978), 399-404.
4. _____, On power endomorphism of the additive group of a ring, Math. Japonica, 29(1984), 419-426.
5. I. N. Herstein, Power maps in rings, Michigan Math. J. 8(1961), 29-32.
6. _____, A remark on rings and algebras, Michigan Math. J. 10(1963), 269-272.
7. Y. Hirano and M. Tominaga: Some commutativity theorems for rings, Hiroshima Math. J. 11(1981), 457-464.
8. V. Perić, A note on the radical N of a certain ring R and a subdirect sum representation of the ring R/N, Acta Math. Hung. 46(3-4)(1985, 233-237.
9. _____, On rings with additive power maps, Radovi matematički, 1(2)(1985), 199-211.

Odsjek za matematiku
Prirodno-matematički fakultet
YU 71000 SARAJEVO

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

WARD DOUBLE QUASIGROUPS

Mirko Polonijo

Abstract. If $(Q,\cdot)$ and $(Q,:)$ are quasigroups which satisfy $(a\cdot c):(b\cdot c) = a:b$ then $(Q,\cdot,:)$ is said to be a Ward double quasigroup. We prove that for any Ward double quasigroup $(Q,\cdot,:)$ there is a group $(Q,\circ)$ and bijections ρ,ν on Q such that $x\cdot y = x\rho(\nu(y))^{-1}$, $x:y = \rho(x\circ y^{-})$.

J.M.Cardoso and C.P.da Silva introduced the notion of Ward quasigroup (briefly W-quasigroup; cf. [1],[8]) and the author proved in [5] that W-quasigroup could be defined as a quasigroup $(Q,\cdot)$ which satisfies the law of right transitivity, i.e.

$$(W) \qquad (a\cdot c)\cdot(b\cdot c) = a\cdot b$$

Since the right transitivity is the (13)-conjugate of the associativity (see[3]), it follows that $(Q,\cdot)$ is a W-quasigroup iff its (13)-conjugate is a group.

Let us mention that H.Furstenberg in [4] used the word half-group for a right transitive groupoid and K.P. Chinda in [2] called it a hemigroup. Further, in [6] it was shown that the existence of W-quasigroup is equivalent to the existence of a so-called Desargues system (cf.[7]).

In the present note we define Ward double quasigroup and describe its structure (Theorem, Remark 2).

DEFINITION. We say that $(Q,\cdot,:)$ is a Ward double quasigroup (briefly Wd-quasigroup) if $(Q,\cdot)$ and $(Q,:)$ are

---

This paper is in final form and no version of it will be submitted for publication elsewhere.

quasigroups satisfying

(Wd) $(a\cdot c):(b\cdot c) = a:b$

for all $a,b,c \in Q$.

Hence, W-quasigroup is a special case of a Wd-quasigroup.

Example. Let $(Q,\cdot)$ be a group and $(Q,:)$ its (13)-conjugate, i.e. $a:b = c$ iff $c\cdot b = a$, i.e. $a:b = a\cdot b^{-1}$, where b^{-1} is the inverse of b in the group $(Q,\cdot)$. Then $(Q,\cdot,:)$ is a Wd-quasigroup. Indeed, since $(a:b)\cdot b = a$, we have $a\cdot c = [(a\cdot c):(b\ c)]\cdot(b\cdot c) = \{[(a\cdot c):(b\cdot c)]\cdot b\}\cdot c$ and (Wd) follows.

LEMMA. If $(Q,\cdot,:)$ is a Wd-quasigroup, then

(1) $a:a = b:b$, i.e. $(Q,:)$ is unipotent

(2) $a:u = b:v$ and $c:u = d:v$ imply $a:c = b:d$

(3) $a:b = c:d$ implies $b:a = d:c$

Proof. (1) For any two $a,b \in Q$, there is $c \in Q$ such that $a = b\cdot c$ and therefore $a:a = (b\cdot c):(b\cdot c) = b:b$.

(2) Let $a:u = b:v$, $c:u = d:v$ and w defined by $u\cdot w = v$. Hence $b:v = a:u = (a\cdot w):(u\cdot w) = (a\cdot w):v$ and $d:v = (c\cdot w):v$, i.e. $b = a\cdot w$ and $d = c\cdot w$ which implies $a:c = (a\cdot w):(c\cdot w) = b:d$.

(3) is a direct consequence of (1) and (2).

COROLLARY 1. Let $(Q,\cdot,:)$ be a Wd-quasigroup.

(1) If $(Q,:)$ has a right unit, then $(Q,:)$ is a W-quasigroup.

(2) If $(Q,\cdot)$ is unipotent, then $(Q,\cdot)$ is a W-quasigroup.

Proof. (1) Let 1 be a right unit for $(Q,:)$, i.e. $x:1 = x$ for all $x \in Q$. Then $a:c = (a:c):1$, $b:c = (b:c):1$ for all $a,b,c \in Q$ and therefore $a:b = (a:c):(b:c)$ by Lemma.

(2) Let $(Q,\cdot)$ be unipotent, i.e. there is $1 \in Q$ such that $x\cdot x = 1$ for all $x \in Q$. Hence $a:b = (a\cdot b):1$ and therefore $a\cdot b = c\cdot d$ iff $a:b = c:d$, which implies (W) by (Wd).

Remark 1. Obviously, any W-quasigroup is unipotent (Lemma) and has a right unit.

PROPOSITION. If $(Q,\cdot,:)$ is a Wd-quasigroup, $1 \in Q$ a fixed element and $\circ$ a binary operation on Q defined by the equivalence $x\circ y = z$ iff $z:y = x:1$, then $(Q,\circ)$ is a group.

Proof. Obviously $(Q,\circ)$ is a quasigroup. Further, for $a,b,c \in Q$ let $a\circ b = u$, $u\circ c = v$, $b\circ c = w$. To prove associativity we have to show that $a\circ w = v$ holds. Since $u:b = a:1$, $v:c = u:1$, $w:c = b:1$ it follows $u:b = a:1$ and $v:w = u:b$ which gives $v:w = a:1$ i.e. $a\circ w = v$.

COROLLARY 2. Let $(Q,\cdot,:)$ be a Wd-quasigroup and $(Q,:)$ the (13)-conjugate of $(Q,\cdot)$. Then $(Q,\cdot)$ is a group (compare with the given example).

Proof. $(Q,:)$ is unipotent and put $x:x = 1$. Let $(Q,\circ)$ be a group defined in the Proposition. Since $1\cdot x = x$ it follows $x:1 = (x\cdot 1):(1\cdot 1) = (x\cdot 1):1$, i.e. $x\cdot 1 = x$, i.e. $x:1 = x$. Hence, $x\cdot y = z$ iff $z:y = x = x:1$ iff $x\circ y = z$, i.e. $(Q,\cdot)$ is a group.

THEOREM. For any Wd-quasigroup $(Q,\cdot,:)$ there is a group $(Q,\circ)$ and bijections ρ,ν on Q such that

$$x\cdot y = x\circ(\nu(y))^{-1}$$
$$x:y = \rho(x\circ y^{-1})$$

for all $x,y \in Q$, where y^{-1} is the inverse of y with respect to the group operation $\circ$.

Proof. Let $(Q,\cdot,:)$ be a Wd-quasigroup and $(Q,\circ)$ a group defined by $(x\circ y):y = x:1$, for a fixed element 1 in Q, as it was done in the Proposition. Element 1 is the unit of the group, because $x:1 = x:1$ and $x:x = 1:1$. Further, if y^{-1} is the inverse of y in $(Q,\circ)$ then it is defined by $1:y^{-1} = y:1$, which is equivalent to $1:y = y^{-1}:1$. Now, from $(x\circ y^{-1}):y^{-1} = x:1$ and $1:y^{-1} = y:1$ it follows $x:y = (x\circ y^{-1}):1$. If we define ρ,ν by $\rho(x) = x:1$ and $\nu(x)\cdot x = 1$, we get $x:y = \rho(x\circ y^{-1})$ and $x:\nu(y) = (x\cdot y):(\nu(y)\cdot y) = (x\cdot y):1$ i.e. $x\cdot y = x\circ(\nu(y))^{-1}$.

Remark 2. Evidently, if $(Q,\circ)$ is a group and ρ,ν bijections on Q and $\cdot,:$ binary operations on Q defined by $x\cdot y = x\circ(\nu(y))^{-1}$, $x:y = \rho(x\circ y^{-1})$, then $(Q,\cdot,:)$ is a Wd-quasigroup.

COROLLARY 3. Let $(Q,\cdot,:)$ be a Wd-quasigroup.

(1) If $(Q,:)$ has a right unit, then there is a group $(Q,\circ)$ and a bijection ν on Q such that

$$x\cdot y = xo(v(y))^{-1}$$
$$x:y = xoy^{-1}$$

(2) If $(Q,\cdot)$ is unipotent, then there is a group (Q,o) and a bijection ρ on Q such that

$$x\cdot y = xoy^{-1}$$
$$x:y = \rho(xoy^{-1})$$

Proof. (1) Take a right unit of $(Q,:)$ for a fixed element 1 in the proof of Theorem, which implies $\rho(x) = x$ (compare with Corollary 1, statement (1)).

(2) Take $x\cdot x$ (which is a constant) as a fixed element 1 in the proof of Theorem, which implies $v(x) = x$ (compare with Corollary 1, statement (2)).

COROLLARY 4. If $(Q,\cdot)$ is a W-quasigroup, then it is the (13)-conjugate of a group.

Proof. $(Q,\cdot)$ is unipotent by Lemma and (13)-conjugate of a group (Q,o) by Corollary 3.

REFERENCES:

1. J.M.Cardoso, C.P.da Silva, On Ward quasigroups, An.Stiint. Univ. "Al.I.Cuza" Iasi Sect I a Math. 24(1978), 231-233.
2. K.P.Chinda, Some theorems on hemigroups, Aequationes Math. 20 (1980), 198-223.
3. J.Denes, A.D.Keedwell, Latin squares and their applications, Akademiai Kiado, Budapest, 1974.
4. H.Furstenberg, The inverse operation in groups, Proc.Amer. Math.Soc. 6(1955), 991-997.
5. M.Polonijo, A note on Ward quasigroups, An.Stiint.Univ. "Al.I.Cuza" Iasi Sect I a Math. to appear.
6. M.Polonijo, Desargues systems and Ward quasigroups, to appear.
7. D. Vakarelov, Dezargovi sistemi, Annuaire Univ. Sofia Fac. Math. 64 (1969/1970), 227-235.
8. M.Ward, Postulates for the inverse operations in a group, Trans.Amer.Math.Soc. 32 (1930), 520-526.

Mirko Polonijo
Department of Mathematics
University of Zagreb
p.o.box 187
41001 Zagreb, Yugoslavia

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

THE LATTICE OF r-SEMIPRIME IDEMPOTENT-SEPARATING CONGRUENCES ON r-SEMIGROUP

Protić Petar

Abstract. In this paper we consider some idempotent-separating congruences on a π-regular semigroup. In this way we obtain a generalization of results of D. Krgović |9|. R. Feigenbaum described in |6| the lattice $\mathcal{C}(S)$ of idempotent-separating congruences on a regular semigroup S. Here we describe the lattice $\mathcal{C}(S)$ of r-semiprime idempotent-separating congruences on an r-semigroup S.

1. Preliminary results and definitions

A semigroup S is π-regular if for every $a\in S$ there exists a positive integer m such that $a^m \in a^m S a^m$. We denote by RegS the set of all regular elements of S. An element a' is an inverse of a if $a=aa'a$ and $a'=a'aa'$. As usually we shall denote by V(a) the set of all inverses of a. A semigroup S is π-orthodox if S is π-regular and the set E(S) of all idempotents of S is a subsemigroup of S |2|.

On a π-regular semigroup S we define a mapping $r : S \longrightarrow \mathrm{Reg}S$ by $r(a)=a^m$, where m is the smallest positive integer such that $a^m \in \mathrm{Reg}S$.

DEFINITION 1.1 |12| S is an r-semigroup if it is π-regular and $r(ab)=r(a)r(b)$ for all $a,b\in S$.

LEMMA 1.1 |12| Let S be an r-semigroup. Then RegS is a subsemigroup of S and r is homomorphism.

DEFINITION 2.1 |12| A relation ρ on a π-regular semigroup S is r-semiprime if $a\,\rho\, r(a)$ for all $a\in S$.

" This paper is in final form and no version of it will be submitted for publication elsewhere " .

If ρ is an r-semiprime relation on a $\mathcal{T}$-regular semigroup S, then $a \rho b \iff r(a) \rho r(b)$ for all $a,b \in S$.

Define on a $\mathcal{T}$-regular semigroup S the equivalence relations $\mathcal{L}^*$ ($\mathcal{R}^*$) by

$a \mathcal{L}^* b \iff Sr(a)=Sr(b)$ ($a \mathcal{R}^* b \iff r(a)S=r(b)S$)

and $\mathcal{H}^* = \mathcal{L}^* \cap \mathcal{R}^*$ |8|. Each $\mathcal{H}^*$-class contains at most one idempotent |8|.

PROPOSITION 1.1 |8| Let a and b be elements of a $\mathcal{T}$-regular semigroup S. Then

(i) $(a,b) \in \mathcal{L}^* \iff (\exists a' \in V(r(a)))(\exists b' \in V(r(b)))$ $a'r(a)=b'r(b)$.

(ii) $(a,b) \in \mathcal{H}^* \iff (\exists a' \in V(r(a)))(\exists b' \in V(r(b)))$ $a'r(a)=b'r(b)$, $r(a)a'=r(b)b'$.

The subsemigroup K of a semigroup S is full if $E(S) \subseteq K$.

For an eq-uivalence relation α on a semigroup S, we define the kernel and the trace of α by

$\ker\alpha = \{ a \in S : (\exists e \in E(S))\ a \alpha e \}$ and $tr\alpha = \alpha|_{E(S)}$ respectively.

For nondefinied notions we refer to |1,3,4|.

2. Some idempotent-separating congruences on a $\mathcal{T}$-regular semigroup

The next lemma follows from Proposition 1.1.

LEMMA 2.1 Let α be an equivalence relation on a $\mathcal{T}$-regular semigroup S. Then

(i) $\alpha \subseteq \mathcal{L}^* \implies \ker\alpha = \{a \in S : (\exists a' \in V(r(a)))\ a \alpha a'r(a)\}$.

(ii) $\alpha \subseteq \mathcal{H}^* \implies \ker\alpha = \{a \in S : (\exists a' \in V(r(a)))\ a \alpha a'r(a),\ a'r(a)=r(a)a'\}$.

The subsemigroup K of a $\mathcal{T}$-regular semigroup S is inverse-closed if $V(regK) \subseteq regK$ where $regK = K \cap RegS$ and $V(regK) = \cup\{V(a) : a \in regK\}$ |12|.

PROPOSITION 2.1 Let K be a full, inverse-closed subsemigroup of a $\mathcal{T}$-regular semigroup S and α an equivalence relation on S such that $\alpha \subseteq \mathcal{L}^*$. The relation (K_α) defined on S by

(1) $a(K_\alpha)b \iff a \alpha b \wedge (\ b' \in V(r(b)))\ r(a)b' \in K$

is an equivalence relation on S for which $reg(\ker(K_\alpha)) = K \cap reg(\ker\alpha)$ and $tr(K_\alpha) = tr\alpha$.

The subsemigroup K of a $\mathcal{T}$-regular semigroup S is

r-semiprime if $r(a) \in K \implies a \in K$ |12|.

COROLLARY 2.1 Let K be a full, inverse-closed r-semiprime subsemigroup of a $\mathcal{T}$-regular semigroup S and α an r-semiprime equivalence on S such that $\alpha \subseteq \mathcal{L}^*$. The relation (K_α) defined on S by (1) is an r-semiprime equivalence on S and $\ker(K_\alpha) = K \cap \ker\alpha$, $tr(K_\alpha) = tr\alpha$.

THEOREM 2.1 |13| If S be a $\mathcal{T}$-regular semigroup, then an r-semiprime congruence ρ on S is idempotent-separating if and only if $\rho \subseteq \mathcal{H}^*$.

The maximum idempotent-separating congruence μ on a $\mathcal{T}$-regular semigroup S is described in |5| and |13|. The congruence μ cn an r-semigroup S is an r-semiprime congruence |13|. The following theorem describes r-semiprime idempotent-separating congruences on an r-semigroup.

THEOREM 2.2 Let ρ be an r-semiprime idempotent-separating congruence on an r-semigroup S. The following statements are equivalent.

(i) $a \rho b$;

(ii) $a \mu b \wedge (\exists b' \in V(r(b)))\ r(a)b' \in \ker\rho$;

(iii) $a \mathcal{H}^* b \wedge (\exists b' \in V(r(b)))\ r(a)b' \in \ker\rho$;

(iv) $(\exists a' \in V(r(a)))(\exists b' \in V(r(b)))(\ a'r(a)=b'r(b)$, $r(a)a'=r(b)b'$, $r(a)b' \in \ker\rho$).

Proof. (i) $\implies$ (ii) Let $a \rho b$ and $b' \in V(r(b))$. Then $r(a) \rho a \rho b \rho r(b)$ and $r(a)b' \rho r(b)b'$, and so $r(a)b' \in \ker\rho$.

(ii) $\implies$ (iii) By Theorem 2.1.

(iii) $\implies$ (iv) By Proposition 1.1.

(iv) $\implies$ (i) Let $a'r(a)=b'r(b)$, then $Sr(a)=Sr(b) \iff a \mathcal{L}^* b$. Simil-arly, $a'S=b'S \iff a' \mathcal{L}^* b'$. Since $r(a)b'r(b)a'r(a)b' = r(a)a'r(a)a'r(a)b'=r(a)b'$, we have $r(a)b' \in RegS$. Now $Sr(a)b' = Sr(b)b' \iff r(a)b' \mathcal{L}^* r(b)b'$. Simil-arly, $r(a)a'S=r(a)b'S \iff r(a)a' \mathcal{R}^* r(a)b'$. Hence, $r(a)b' \mathcal{H}^* r(b)b'$. But $r(a)b' \in \ker\rho$ implies that $r(a)b' \rho e$ for some $e \in E(S)$. Then $r(a)b' \mathcal{H}^* e$, which implies $r(b)b'=e$. Therefore $r(a)b' \rho r(b)b'$ so that $r(a)=r(a)a'r(a) = r(a)b'r(b) \rho r(b)$. Hence, $a \rho b$.

The following corollary describes the r-semiprime idempotent-separating congruences on a $\mathcal{T}$-regular semigroup.

COROLLARY 2.2 Let ρ be an r-semiprime idempotent-separating congruence on a $\mathcal{T}$-regular semigroup S. The following statements are equivalent.

(i) $a\rho b$;

(ii) $a\mathcal{K}^*b \wedge (\exists b'\in V(r(b)))\ r(a)b'\in \ker\rho$;

(iii) $(\exists a'\in V(r(a)))(\exists b'\in V(r(b)))(\ a'r(a)=b'r(b),$
$r(a)a'=r(b)b',\ r(a)b'\in \ker\rho\ )$.

The following corollary describes the maximum idempotent-separating congruence μ on an r-semigroup.

COROLLARY 2.3 Let S be an r-semigroup. The following statements are equivalent.

(i) $a\mu b$;

(ii) $a\mathcal{K}^*b \wedge (\exists b'\in V(r(b)))\ r(a)b'\in \ker\mu$;

(iii) $(\exists a'\in V(r(a)))(\exists b'\in V(r(b)))(\ a'r(a)=b'r(b),$
$r(a)a'=r(b)b',\ r(a)b'\in \ker\mu\ )$.

The relation ν defined on r-semigroup S by

$$\nu=\{\ (a,b)\in SxS\ :\ r(a)=r(b)\ \}$$

is the minimum r-semiprime idempotent-separating congruence on S|13|. The following corollary gives a new description of ν on an r-semigroup.

COROLLARY 2.4 Let S be an r-semigroup. The following statements are equivalent.

(i) $a\nu b$;

(ii) $a\mathcal{K}^*b \wedge (\exists b'\in V(r(b)))\ r(a)b'\in \ker\nu$;

(iii) $(\exists a'\in V(r(a)))(\exists b'\in V(r(b)))(\ a'r(a)=b'r(b),$
$r(a)a'=r(b)b',\ r(a)b'\in \ker\nu\ )$.

A semigroup S is orthodox if S is regular and E(S) is a subsemigroup of S.

THEOREM 2.3 Let S be a $\mathcal{K}$-regular semigroup. The following statements are equivalent.

(i) RegS is orthodox semigroup;

(ii) S is $\mathcal{K}$-orthodox semigroup;

(iii) $(\forall a,b\in RegS)(\forall a'\in V(a))(\forall b'\in V(b))(b'a'\in V(ab))$;

(iv) If $e\in E(S)$, then $V(e)\subseteq E(S)$ and RegS is a subsemigroup of S.

The subset K of a $\mathcal{K}$-regular semigroup S is self-conjugate if $a'(regK)a\subseteq regK$ for all $a\in RegS$ and for all $a'\in V(a)$|12|. The subsemigroup K of a $\mathcal{K}$-orthodox semigroup S is normal if K is full, self-conjugate and inverse-closed. If ρ is a (r-semiprime) congruence on a $\mathcal{K}$-orthodox semigroup S then $\ker\rho$ is a (r-semiprime) normal subsemigroup of S, |12|.

THEOREM 2.4 Let K be a normal r-semiprime subsemigroup of a $\mathcal{K}$-orthodox r-semigroup S and ρ a (r-semiprime) congruence on S such that $\rho\subseteq\mathcal{K}^*$. The relation (K_ρ) defined on S by

$$a(K_\rho)b \iff a\rho b \wedge (\exists b'\in V(r(b)))\ r(a)b'\in K$$

is a (r-semiprime) congruence on S for which $reg(\ker(K_\rho))=K\cap reg(\ker\rho)$ ($\ker(K_\rho)=K\cap\ker\rho$) and $tr(K_\rho)=tr\rho$.

Proof. According to Proposition 3.1 and Corollary 3.1, it suffices to prove that (K_ρ) is compatible. Let $a(K_\rho)b$ and $c\in S$, then by $\rho\subseteq\mathcal{K}^*$ we have that there exists $a'\in V(r(a))$ such that $a'r(a)=b'r(b)$. Let $c'\in V(r(c))$, then

$$r(ac)c'b'=r(a)r(c)c'b'r(b)b'=r(a)r(c)c'a'r(a)b'\in$$
$$r(a)Ka'\cdot K\subseteq K.$$

Since $c'b'\in V(r(b)r(c)=r(bc))$ and since ρ is a congruence, we have $ca(K_\rho)cb$.

The following theorem describes an r-semiprime idempotent-separating congruence on a $\mathcal{K}$-orthodox r-semigroup.

THEOREM 2.5 Let K be a normal r-semiprime subsemigroup of a $\mathcal{K}$-orthodox r-semigroup S such that $K\subseteq\ker\mu$. The relation $(K\mu)$ defined on S by

$$a(K\mu)b \iff a\mu b \wedge (\exists b'\in V(r(b)))\ r(a)b'\in K$$

is an r-semiprime idempotent-separating congruence on S and $K=\ker(K\mu)$.

Conversely, if ρ is an r-semiprime idempotent-separating congruence on S then $\ker\rho$ is a normal r-semiprime subsemigroup of S, $\ker\rho\subseteq\ker\mu$ and $\rho=(K\mu)$, where $K=\ker\rho$.

Proof. The direct part follows from Theorem 2.4. According to Theorem 2.2 , the converse is true.

3. The lattice

Let $\mathcal{T}(S)$ be a set of all r-semiprime idempotent-separating congruences on an r-semigroup S. By Corollary 2.2 μ is the greatest and by Corollary 2.4 ν is the least element in $\mathcal{T}(S)$. Hence, $\mathcal{T}(S)$ is a complete lattice. The main theorem will characterize lattice $\mathcal{T}(S)$.

Let Sbean r-semigroup, then let us denote with $\mathcal{T}(RegS)$ the lattice of idempotent-separating congruences on the regular subsemigroup RegS.

LEMMA 3.1 Let S be an r-semigroup and let ρ be a congruence on a regular semigroup RegS. Then the relation on S defined by

(2) $$a\,\tilde{\rho}\,b \iff r(a)\,\rho\,r(b)$$

is an r-semiprime congruence on S.

Proof. It is clear that $\tilde{\rho}$ is an equivalence. Let

$$a\,\tilde{\rho}\,b \iff r(a)\,\rho\,r(b),\quad c\,\tilde{\rho}\,d \iff r(c)\,\rho\,r(d),$$

then $r(ac)=r(a)r(c)\,\rho\,r(b)r(d)=r(bd)$ so it follows that $ac\tilde{\rho}\,bd$ (by (3)). Hence, $\tilde{\rho}$ is a congruence on S and it is r-semiprime.

COROLLARY 3.1 Let S be an r-semigroup and $\rho\in\mathcal{C}(\mathrm{Reg}S)$, then $\tilde{\rho}\in\mathcal{C}(S)$ ($\tilde{\rho}$ defined by (3)).

THEOREM 3.1 Let S be an r-semigroup. If ρ_1 and ρ_2 are r-semiprime congruences on S and $\rho_1|_{\mathrm{Reg}S}=\rho_2|_{\mathrm{Reg}S}$, then $\rho_1=\rho_2$.

Conversely, if ρ_1 and ρ_2 are congruences on RegS and $\tilde{\rho}_1=\tilde{\rho}_2$, then $\rho_1=\rho_2$.

Proof. Let a,b∈S, then

$$a\,\rho_1\,b \iff r(a)\,\rho_1 r(b) \iff r(a)\,\rho_1|_{\mathrm{Reg}S}\,r(b)$$
$$\iff r(a)\,\rho_2|_{\mathrm{Reg}S}\,r(b) \iff r(a)\,\rho_2 r(b) \iff a\,\rho_2\,b$$

and so $\rho_1=\rho_2$.

Conversely, let a,b∈RegS, then

$$a\,\rho_1\,b \iff a=r(a)\,\tilde{\rho}_1\,r(b)=b \iff a\,\tilde{\rho}_2\,b \iff a\,\rho_2\,b$$

and so $\rho_1=\rho_2$.

COROLLARY 3.2 If S is an r-semigroup, ρ an r-semiprime congruence on S and $\bar{\rho}=\rho|_{\mathrm{Reg}S}$, then $\rho=\tilde{\bar{\rho}}$.

THEOREM 3.2 Let S be an r-semigroup, then the mapping $h:\mathcal{C}(\mathrm{Reg}S)\longrightarrow\mathcal{C}(S)$ defined by $h(\rho)=\tilde{\rho}$ is an isomorphism.

Proof. Let $\rho\in\mathcal{C}(S)$, then $\bar{\rho}=\rho|_{\mathrm{Reg}S}\in\mathcal{C}(\mathrm{Reg}S)$ and by Corollary 3.2 $\rho=\tilde{\bar{\rho}}$. Hence, $h(\bar{\rho})=\rho$ and the map h is onto.

Let $\rho_1,\rho_2\in\mathcal{C}(\mathrm{Reg}S)$ and $h(\rho_1)=\tilde{\rho}_1=\tilde{\rho}_2=h(\rho_2)$, then by Theorem 3.1 $\rho_1=\rho_2$ and the map h is an injection.

Let a,b∈S, $\rho_1,\rho_2\in\mathcal{C}(\mathrm{Reg}S)$ and $\rho_1\subseteq\rho_2$, then

$$a\,\tilde{\rho}_1\,b \iff r(a)\,\rho_1\,r(b) \Longrightarrow r(a)\,\rho_2\,r(b) \iff a\,\tilde{\rho}_2\,b$$

and so $\tilde{\rho}_1\subseteq\tilde{\rho}_2$. Hence, the map h is order preserving.

The map $h^{-1}:\mathcal{C}(S)\longrightarrow\mathcal{C}(\mathrm{Reg}S)$ defined by $h^{-1}(\rho)=\bar{\rho}=\rho|_{\mathrm{Reg}S}$ is an inverse for the map h. Really, if $\rho\in\mathcal{C}(S)$ then by Corollary 3.2 we have

$$(h\circ h^{-1})\rho=h(h^{-1}(\rho))=h(\bar{\rho})=\tilde{\bar{\rho}}=\rho.$$

Similarly, $(h^{-1}\circ h)\rho=\rho$, where $\rho\in\mathcal{C}(S)$. Also, if $\rho_1,\rho_2\in\mathcal{C}(S)$ and $\rho_1\subseteq\rho_2$ then $\bar{\rho}_1=\rho_1|_{\mathrm{Reg}S}\subseteq\rho_2|_{\mathrm{Reg}S}=\bar{\rho}_2$, and so $h^{-1}(\rho_1)\subseteq h^{-1}(\rho_2)$. Hence, the map h^{-1} is order preserving. By Lemma 2.2.3 |1| we have that the map h is an isomorphism and the lattices $\mathcal{C}(S)$ and $\mathcal{C}(\mathrm{Reg}S)$ are isomorphic.

Let S be an r-semigroup and

(3) $$\mathcal{C}=\{(a,b)\in S\times S : (\exists a'\in V(r(a)))(\exists b'\in V(r(b)))$$
$$a'r(a)=b'r(b),\ r(a)a'=r(b)b',\ r(a)b',a'r(b)\in\ker\mu\},$$

then, clearly, $\mathcal{C}\equiv\mu$.

J. Meakin |10| and R. Feigenbaum |6| have described the maximum idempotent-separating congruence μ on a regular semigroup.

THEOREM 3.3 |6| The maximum idempotent-separating congruence on a regular semigroup S is given by

$$\mu=\{(a,b)\in S\times S : (\exists a'\in V(a))(\exists b'\in V(b))\ a'a=b'b,$$
$$aa'=bb',\ ab',a'b\in\ker\mu\}.$$

If S is an r-semigroup and μ the maximum idempotent-separating congruence on S, μ_1 the maximum idempotent-separating congruence on regular semigroup RegS, then

$$\mu=\tilde{\mu}_1\quad(h(\mu_1)=\mu)\quad\text{and}\quad\mu_1=\mu|_{\mathrm{Reg}S}.$$

Similarly, if i° is an identity relation on RegS, then

$$\nu=\tilde{i^\circ}\quad(h(i^\circ)=\nu)\quad\text{and}\quad i^\circ=\nu|_{\mathrm{Reg}S}.$$

Also, $\ker\mu_1=\ker\mu\cap\mathrm{Reg}S$. Since RegS is a subsemigroup on S and $a',r(a),b',r(b)\in\mathrm{Reg}S$ we have by (3)

(4) $$\mu=\{(a,b)\in S\times S : (\exists a'\in V(r(a)))(\exists b'\in V(r(b)))$$
$$a'r(a)=b'r(b),\ r(a)a'=r(b)b',\ r(a)b',a'r(b)\in\ker\mu_1\}$$

and so μ is the maximum (r-semiprime) idempotent-separating congruence on S.

DEFINITION 3.1 |6| Let S be a regular semigroup and A a subset of S.

(i) A will be called L-closed (R-closed) if $a,b\in A$ with $L_a\le L_b$ ($R_a\le R_b$) implies $ab,ba\in A$. If A is both L-closed and R-closed, A is said to be L-R-closed.

(ii) A will be called L-self-conjugate (R-self-conjugate) if $a\in A$ and $x\in S$ with $L_a\le L_x$ ($R_a\le R_x$) implies $xax'\in A$ ($x'ax\in A$) for all $x'\in V(x)$. If A is both L-self-conjugate and R-self-conjugate, A is said to be L-R-self-conjugate.

(iii) A will be called H-regular if for each $a\in A$

$$V(a)\cap H_a\cap A\neq\emptyset\ .$$

In Definition 3.1 the clases of known Green relation are denoted by L,R and H.

Let S be a regular semigroup. In |6| is defined set

$$\mathcal{A}=\{A\subseteq S : E(S)\subseteq A\subseteq \ker\mu \text{ and } A \text{ is L-R-closed, L-R-self-conjugate, H-regular subset of } S\}$$

where μ is the maximum idempotent-separating congruence on S.

THEOREM 3.4 |6| Let S be a regular semigroup. The map

$$A\longrightarrow (A)=\{(a,b)\in SxS : (\exists a'\in V(a))(\exists b'\in V(b)) \ a'a=b'b,\ aa'=bb',\ ab',a'b\in A\}$$

is a 1:1 order preserving map of $\mathcal{A}$ onto the set of idempotent-separating congruences on S.

Let S be an r-semigroup, μ_1 the maximum idempotent-separating congruence on RegS and

$$\mathcal{A}=\{A\subseteq RegS : E(S)\subseteq A\subseteq \ker\mu_1 \text{ and } A \text{ is L-R-closed, L-R-self-conjugate, H-regular subset of } RegS\}\ .$$

By the following theorem we describe the lattice $\mathcal{T}(S)$.

THEOREM 3.5 Let S be an r-semigroup. The map

$$A\longrightarrow (A)=\{(a,b)\in SxS : (\exists a'\in V(r(a)))(\exists b'\in V(r(b))) \ a'r(a)=b'r(b),r(a)a'=r(b)b',\ r(a)b',a'r(b)\in A\}$$

is a 1:1 order preserving map of $\mathcal{A}$ onto the set of r-semiprime idempotent-separating congruences on S.

Proof. Let $A\in\mathcal{A}$, then by Theorem 3.4 the relation

$$(A)_1=\{(a,b)\in RegSxRegS : (\exists a'\in V(a))(\exists b'\in V(b)) \ a'a=b'b,\ aa'=bb',\ ab',a'b\in A\}$$

is an idempotent-separating congruence on RegS, i.e. $(A)_1\in\mathcal{T}(RegS)$. By Corollary 3.1 relation (A) defined on S by $a(A)b \Longleftrightarrow r(a)(A)_1r(b)$ is an r-semiprime idempotent-separating congruence on S, i.e. $(A)\in\mathcal{T}(S)$, and clearly

$$(A)=\{(a,b)\in SxS : (\exists a'\in V(r(a)))(\exists b'\in V(r(b))) \ a'r(a)=b'r(b),r(a)a'=r(b)b',r(a)b',a'r(b)\in A\}\ .$$

By Theorem 3.4 the map $A\longrightarrow (A)_1$ is a 1:1 order preserving of $\mathcal{A}$ onto $\mathcal{T}(RegS)$ and by Theorem 3.2 the map $(A)_1\longrightarrow (A)$ is a 1:1 order preserving of $\mathcal{T}(RegS)$ onto $\mathcal{T}(S)$. Hence, the map $A\longrightarrow (A)$ is a 1:1 order preserving of $\mathcal{A}$ onto $\mathcal{T}(S)$.

REFERENCES

1. G. Birkhoff, "Lattice theory", Amer. Math. Soc. Colloq. Publ. vol. 25, New York, 1984.
2. S. Bogdanović, Power regular semigroups, Zbornik radova PMF u Novom Sadu, Vol. 12 (1982), 417-428.
3. S. Bogdanović, "Semigroups with a system of subsemigroups", Novi Sad, 1985.
4. A.H. Clifford, G.B. Preston, "The algebraic theory of semigroups", Amer. Math. Soc., Providence, R.I., Vol.I,1961.
5. P.M. Edwards, Eventually regular semigroups, Bul. Austral. Math. Soc. Vol. 28 (1983), 23-38.
6. R. Feigenbaum, Kernels of regular semigroup homomorphism, Doctoral dissertacion, University of South Carolina, 1975.
7. R. Feigenbaum, Kernels of orthodox semigroup homomorphism, J. Austral. Math. Soc. 22 (Series A) (1976), 234-245.
8. J.L. Galbiati, M.L. Veronesi, Sui semigruppi quasi regolari, Instituto Lombardo (Rend. Sc.) A Vol. 116 (1982).
9. D. Krgović, Idempotent separating congruences on a regular semigroups, Third algebraic conference, Beograd, 1982,85-92.
10. J. Meakin, The maximum idempotent-separating congruence on a regular semigroup, Proc. Edin.Math.Soc.18(1972-73),85-92.
11. P. Protić, Kongruencije na π-regularnim polugrupama, Doktorska disertacija, Novi Sad, 1986.
12. P. Protić, S. Bogdanović, Some congruences on a strongly π-inverse r-semigroup, Zbornik radova PMF u Novom Sadu (to appear).
13. P. Protić, S. Bogdanović, Some idempotent-separating congruences on a π-regular semigroup, Note di matematika, Lece (to appear).

Građevinski fakultet
Beogradska 14
18000 Niš
Jugoslavija

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

CONSTRUCTIVE ASPECTS OF ABELIAN GROUPS

Daniel A. Romano

Abstract. This paper contains a constructive development, in Bishop's sense, of facts about subgroups and cosubgroups of groups in general nondiscrete case. It contains criteria for direct sums of groups, and examples of subgroups of groups for which there exist compatible cosubgroups.

0. Introduction. For all notions of constructive mathematics the reader is referred to [1],[2],[6],[7],[8] and [9]. The papers [3],[4] and [5] consist of elementary definitions, notation, terminology and basic facts about sets and algebraic structures in Bishop's constructive mathematics which will be used here.

Throughout this paper all groups will be understood to be commutative.

1. Preliminaries

DEFINITION 1. Let $(M,=_M,\neq_M,+)$ be a group and let $(H,=_M,\neq_M)$ be a subset of M.

a) For H we say that it is a subgroup of the group M iff

$$o \in H,$$
$$x \in H \wedge y \in H \Longrightarrow x+y \in H,$$
$$x \in H \Longrightarrow -x \in H.$$

b) For H we say that it is cosubgroup of the group M iff

$$o \notin H,$$
$$x+y \in H \Longrightarrow x \in H \vee y \in H,$$
$$-x \in H \Longrightarrow x \in H.$$

AMS Subject Classification (1980): Primary 03 F 65; Secondary 20 A 99, 20 K 99.

This paper is in final form and no version of it will be submitted for publication elsewhere.

DEFINITION 2. Let $(M,=_M,\neq_M,+)$ be a group and let R be a relation on M.

a) We say that R is a congruity relation on M iff

$(\forall x\in M)((x,x)\in R)$,

$(\forall xy\in M)((x,y)\in R \Longrightarrow (y,x)\in R)$,

$(\forall xyz\in M)((x,y)\in R \wedge (y,z)\in R \Longrightarrow (x,z)\in R)$,

$(\forall xyuv\in M)((x,y)\in R \wedge (u,v)\in R \Longrightarrow (x+u,y+v)\in R)$.

b) We say that R is a cocongruity relation on M iff

$(\forall x\in M)((x,x)\notin R)$,

$(\forall xy\in M)((x,y)\in R \Longrightarrow (y,x)\in R)$,

$(\forall xyz\in M)((x,z)\in R \Longrightarrow (x,y)\in R \vee (y,z)\in R)$,

$(\forall xyuv\in M)((x+u,y+v)\in R \Longrightarrow (x,y)\in R \vee (u,v)\in R)$.

PROPOSITION 1. Let $(M,=_M,\neq_M,+)$ be a group and let R be a relation on M. Then a relation R is a congruity (cocongruity) relation on M iff the set $H \equiv \{x\in M:(x,o)\in R\}$ is a subgroup (cosubgroup) of M and $(x,y)\in R \Longleftrightarrow x-y\in H$.

COROLLARY 1.1. Let $(M,=_M,\neq_M,+)$ be a group. Then

i) A relation $=_M$ is a congruity relation on M and the set $(o) \equiv \{x\in M:x =_M o\}$ is a subgroup of the group M.

ii) A relation $\neq_M$ is a cocongruity relation on M and the set $M_o \equiv \{x\in M:x \neq_M o\}$ is a cosubgroup of the group M.

DEFINITION 3. a) Let R and C be, respectively, a congruity and a cocongruity relation on the group M. We say that R and C are compatible iff

$(\forall xy\in M)\neg((x,y)\in R \wedge (x,y)\in C)$,

$(\forall xyz\in M)((x,y)\in R \wedge (y,z)\in C \Longrightarrow (x,z)\in C)$.

b) Let H and P be a subgroup and a cosubgroup, respectively, of the group M. We say that H and P are compatible iff

$(\forall x\in M)\neg(x\in H \wedge x\in P)$,

$(\forall xy\in M)(x\in H \wedge y\in P \Longrightarrow x+y\in P)$.

LEMMA 2. Let $(M,=_M,\neq_M,+)$ be a group and let R and C be a congruity and a cocongruity relation, respectively, on M, and let H and P be a subgroup and a cosubgroup of M corresponding to R and C, respectively. Then R and C are compatible iff H and P are compatible.

Proof. i) The first condition for compatibility follows

from the second: Suppose $(x,y)\in R$ and $(x,y)\in C$. Then $(y,x)\in C$ and

$$(x,y)\in R \wedge (y,x)\in C \Longrightarrow (x,x)\in C$$

what it is impossible. So

$$\neg((x,y)\in R \wedge (x,y)\in C).$$

ii) Let R and C be compatible. Then

$$x\in H \wedge y\in P \Longleftrightarrow (x,o)\in R \wedge (y,o)\in C \Longleftrightarrow$$

$$\Longleftrightarrow (x,o)\in R \wedge (o,-y)\in C \Longrightarrow (x,-y)\in C \Longleftrightarrow x+y\in P.$$

iii) Let H and P be compatible. Then

$$(x,y)\in R \wedge (y,z)\in C \Longleftrightarrow x-y\in H \wedge y-z\in P \Longrightarrow$$

$$\Longrightarrow x-y+y-z\in P \Longleftrightarrow x-z\in P \Longleftrightarrow (x,z)\in C.$$

2. The main results

2.1. Construction of subgroups. For a cosubgroup P of the group $(M,=_M,\neq_M,+)$ we can construct compatible subgroup of M. The set $\emptyset$ we will understood as its cosubgroup compatible with M.

PROPOSITION 3. Let $(M,=_M,\neq_M,+)$ be a group and let C be a cocongruity on M. Then a relation $\neg C$ defined by

$$(x,y)\in \neg C \Longleftrightarrow \neg((x,y)\in C)$$

is a congruity relation on M compatible with C.

Proof.

$$(x,x)\notin C \Longleftrightarrow (\forall(u,v)\in C)((u,v)\neq_d (x,x)) \Longrightarrow$$

$$\Longrightarrow (\forall(u,v)\in C)\neg((u,v)=_d (x,x)) \Longleftrightarrow$$

$$\Longleftrightarrow \neg(\exists(u,v)\in C)((u,v)=_d (x,x)) \Longleftrightarrow$$

$$\Longleftrightarrow \neg((x,x)\in C) \Longleftrightarrow (x,x)\in \neg C.$$

$$(x,y)\in \neg C \Longleftrightarrow \neg((x,y)\in C) \Longrightarrow \neg((y,x)\in C) \Longleftrightarrow (y,x)\in \neg C.$$

$$(x,y)\in \neg C \wedge (y,z)\in \neg C \Longleftrightarrow \neg((x,y)\in C) \wedge \neg((y,z)\in C) \Longrightarrow$$

$$\Longrightarrow \neg((x,y)\in C \vee (y,z)\in C) \Longrightarrow \neg((x,z)\in C) \Longleftrightarrow (x,z)\in \neg C.$$

$$(x,y)\in \neg C \wedge (u,v)\in \neg C \Longleftrightarrow \neg((x,y)\in C)\wedge\neg((u,v)\in C) \Longrightarrow$$

$$\Longrightarrow \neg((x,y)\in C \vee (u,v)\in C) \Longrightarrow \neg((x+u,y+v)\in C) \Longleftrightarrow$$

$$\Longleftrightarrow (x+u,y+v)\in \neg C.$$

$$(x,y)\in \neg C \wedge (y,z)\in C \Longleftrightarrow$$

$\Longleftrightarrow$ $(x,y)\in \neg C \wedge ((y,x)\in C \vee (x,z)\in C) \Longrightarrow (x,z)\in C$.

COROLLARY 3.1.([6],[9]) Let $(M,=_M,\neq_M,+)$ be a group and let P be a cosubgroup of M. Then a set $\neg P \equiv \{x\in M:\neg(x\in P)\}$ is a stable subgroup of M compatible with P.

COROLLARY 3.2. Let $(M,=_M,\neq_M,+)$ be a group. Then a set $\neg M_o$ is a subgroup of M compatible with M_o and we have $(o)\subseteq \neg M_o$.

PROPOSITION 4. Let $(M,=_M,\neq_M,+)$ be a group and let P be a cosubgroup of M. Then a set

$$\overline{P} \equiv \{x\in M:x \notin P\}$$

is a subgroup of M compatible with P and we have $\overline{P}\subseteq \neg P$.

Proof.

i) $o \notin P \Longleftrightarrow o\in\overline{P}$.

ii) Let $x\in\overline{P} \wedge y\in\overline{P}$, i.e. $x \notin P \wedge y \notin P$. Surely it holds $\neg(x+y\in P)$. Let $z\in P$ be an arbitrary element. Then

$$z\in P \Longleftrightarrow z-x-y+x+y\in P \Longrightarrow z-x-y\in P \vee x+y\in P \Longrightarrow$$

$$\Longrightarrow z-x-y\in P \neq o \Longrightarrow z-x-y \neq_M o \Longleftrightarrow z \neq_M x+y.$$

So $x+y \notin P$, i.e. $x+y\in\overline{P}$.

iii) $x\in\overline{P} \Longleftrightarrow x \notin P \Longleftrightarrow (\forall u\in P)(x \neq_M u) \Longleftrightarrow$

$$\Longleftrightarrow (\forall u\in P)(-x \neq_M -u) \Longrightarrow (\forall v\in P)(v \neq_M -x) \Longleftrightarrow -x \notin P \Longleftrightarrow$$

$$\Longleftrightarrow -x\in\overline{P}.$$

iv) $P\cap\overline{P} = \emptyset$;

$$x\in\overline{P} \wedge y\in P \Longleftrightarrow x \notin P \wedge y\in P \Longleftrightarrow x \notin P \wedge x+y-x\in P$$

$$\Longrightarrow x \notin P \wedge (x+y\in P \vee -x\in P) \Longrightarrow x+y\in P.$$

v) $x\in\overline{P} \Longleftrightarrow x \notin P \Longleftrightarrow (\forall u\in P)(u \neq_M x) \Longrightarrow$

$$\Longrightarrow (\forall u\in P)\neg(u =_M x) \Longleftrightarrow \neg(\exists u\in P)(x =_M u) \Longleftrightarrow \neg(x\in P) \Longleftrightarrow$$

$$\Longleftrightarrow x\in\neg P.$$

COROLLARY 4.1.Let $(M,=_M,\neq_M,+)$ be a group. Then a set $\overline{M}_o$ is a subgroup of the group M compatible with M_o and we have $(o)\subseteq \overline{M}_o \subseteq \neg M_o$.

2.2. Examples of constructions of cosubgroups. There exists examples of subgroups of the group M for which we can construct compatible cosubgroups in M.

PROPOSITION 5. Let $(M,=_M,\neq_M,+)$ be a group. Then

a) The set $M[n] \equiv \{x\in M:nx =_M o\}$ is a subgroup of M;

b) The set $C[n] \equiv \{x\in M:nx \neq_M o\}$ is a cosubgroup of M;

c) M[n] and C[n] are compatible in M.

Proof.

b) $(x\in C[n] \Longleftrightarrow nx \neq_M o \Longrightarrow x \neq_M o) \Longrightarrow o \notin C[n]$;

$$x+y\in C[n] \Longleftrightarrow n(x+y) \neq_M o \Longleftrightarrow nx+ny \neq_M o \Longrightarrow$$

$$\Longrightarrow nx \neq_M o \vee ny \neq_M o \Longleftrightarrow x\in C[n] \vee y\in C[n];$$

$$-x\in C[n] \Longleftrightarrow n(-x) \neq_M o \Longrightarrow nx \neq_M o \Longleftrightarrow x\in C[n];$$

c) $x\in M[n] \wedge y\in C[n] \Longleftrightarrow nx =_M o \wedge ny \neq_M o \Longrightarrow$

$$\Longrightarrow n(x+y) \neq_M o \Longleftrightarrow x+y\in C[n].$$

DEFINITION 4. A group M is a direct sum of the subgroups S and T (denoted by $M = S \oplus T$) iff

(1) $(\forall x\in M)(\exists s\in S)(\exists t\in T)(x =_M s+t)$,

(2) $(\forall s\in S)(\forall t\in T)(s+t =_M o \Longrightarrow s =_M o \wedge t =_M o)$,

(3) $(\forall s\in S)(\forall t\in T)(s \neq_M o \vee t \neq_M o \Longrightarrow s+t \neq_M o)$.

Note. Let M be a group, and let S and T be its subgroups. We write

$$C_S \equiv \{s+t\in S+T:t \neq_M o\}, \qquad C_T \equiv \{s+t\in S+T:s \neq_M o\}.$$

THEOREM 6. Let M be a group and let S and T be its subgroups. Then $M = S \oplus T$ iff

(4) $M = S + T$,

(5) $S\cap T = (o)$,

(6) $C_S \cup C_T = M_o$.

Proof.

a) Let $M = S \oplus T$.

i) It is obvious that $M = S + T$;

ii)

$$x\in S\cap T \Longleftrightarrow (\exists s_x\in S)(\exists t_x\in T)(x =_M s_x + t_x)\begin{cases}\in S\\ \in T\end{cases}$$

$$\Longrightarrow \begin{cases} (-x+s_x)+t_x =_M o \\ s_x+(-x+t_x) =_M o \end{cases} \Longrightarrow s_x =_M x \wedge t_x =_M o \wedge s_x =_M o \wedge t_x =_M x$$

$\Longrightarrow x =_M o$.

iii) $M_o \ni x =_M s_x+t_x \neq_M o \Longrightarrow s_x \neq_M o \vee t \neq_M o \Longleftrightarrow$

$\Longleftrightarrow x \in C_T \vee x \in C_S \Longleftrightarrow x \in C_S \cup C_T$.

b) Let the properties (4) - (6) hold. Then

iv) $(\forall x \in M)(\exists s \in S)(\exists t \in T)(x =_M s+t)$;

v) $(\forall s \in S)(\forall t \in T)(s+t =_M o \Longrightarrow s =_M -t \in S \cap T = (o) \Longrightarrow$

$\Longrightarrow s =_M t =_M o)$;

vi) $(\forall s \in S)(\forall t \in T)(s \neq_M o \vee t \neq_M o \Longleftrightarrow$

$\Longleftrightarrow s+t \in C_T \vee s+t \in C_S \Longleftrightarrow s+t \in C_S \cup C_T = M_o \Longrightarrow s+t \neq_M o)$.

COROLLARY 6.1. Let $M = S \oplus T$. Then

a) The set C_S is a cosubgroup of M compatible with S;

b) $C_S \equiv \{x \in M : x \notin S\}$.

Proof.

a) $(t \neq_M o \Longrightarrow s+t \neq_M o) \Longrightarrow o \notin C_S$;

$-x \in C_S \Longleftrightarrow -x =_M s+t \in C_S \Longleftrightarrow t \neq_M o \Longrightarrow -t \neq_M o \Longrightarrow$

$\Longrightarrow x = -s-t \in C_S$;

$x =_M s_x+t_x \wedge y =_M s_y+t_y \wedge x+y \in C_S \Longleftrightarrow t_x+t_y \neq_M o \Longrightarrow$

$\Longrightarrow t_x \neq_M o \vee t_y \neq_M o \Longleftrightarrow x \in C_S \vee y \in C_S$;

$x \in S \wedge y \in C_S \Longleftrightarrow x =_M s_x+t_x \in S \wedge y =_M s_y+t_y \in C_S \Longleftrightarrow$

$\Longleftrightarrow t_x =_M o \wedge t_y \neq_M o \Longrightarrow t_x+t_y \neq_M o \Longleftrightarrow x+y \in C_S$.

b) $x =_M s_x+t_x \in C_S \Longleftrightarrow t_x \neq_M o \Longrightarrow t_x+(s_x-u) \neq_M o \ (u \in S)$

$\Longleftrightarrow s_x+t_x \neq_M u \ (u \in S) \Longleftrightarrow x \notin S$;

$x \notin S \Longleftrightarrow x =_M s_x+t_x \neq_M (u \in S) \Longrightarrow s_x+t_x \neq_M s_x \Longleftrightarrow$

$\Longleftrightarrow t_x \neq_M o \Longleftrightarrow x \in C_S$.

COROLLARY 6.2. Let $f : M \longrightarrow H$ be an onto homomorphism Then Kerf is a direct summand of M.

Proof. As f is an onto homomorphism, then there exists a homomorphism $h : H \longrightarrow M$ such that $f.h = Id_H$. Then:

i) $x \in M \Longrightarrow f(x) \in H \Longrightarrow f(x) =_H (f.h)(f(x)) \Longleftrightarrow$

$\Longleftrightarrow f(x-hf(x)) =_H o \Longleftrightarrow x-hf(x) \in Kerf$

and

$x =_M x-hf(x) + hf(x) \in Kerf + \{hf(x) \in M : x \in M\}$;

ii) If $x \in Kerf \cap T$, where $T \equiv \{hf(x) \in M : x \in M\}$, we have $f(x) =_H o$ and $(\exists y \in H)(x =_M h(y))$. Then

$x =_M h(y) =_M h((f.h)(y)) =_M hf(h(y)) =_M hf(x) =_M o$.

So $Kerf \cap T = (o)$.

iii) Let $C_{Kerf} \equiv \{x \in M : hf(x) \neq_M o\}$ and $C_T \equiv \{x \in M : x \neq_M hf(x)\}$. Then

$o \neq_M x =_M x - hf(x) + hf(x) \Longrightarrow x \neq_M hf(x) \vee hf(x) \neq_M o$

$\Longleftrightarrow x \in C_T \vee x \in C_{Kerf} \Longleftrightarrow x \in C_T \cup C_{Kerf}$.

So $M_o = C_T \cup C_{Kerf}$.

PROPOSITION 7. Let $(M, =_M, \neq_M, +)$ be a group and let (H_1, P_1) and (H_2, P_2) be two pairs consisting of compatible subgroups and cosubgroups of the group M, such that $H_1 \cap P_2 \neq \emptyset$. If H_2 is a subgroup of the group H_1 and $P_1 \subseteq P_2$, then the set

$$P_1/(H_2, H_1 \cap P_2) \equiv \{x+H_2 \in M/(H_2, P_2) : x \in P_1\}$$

is a cosubgroup of the group $M/(H_2, P_2)$ compatible with the subgroup $H_1/(H_2, P_2 \cap H_1)$ in $M/(H_2, P_2)$.

Proof.

$x+H_2 \in P_1/(H_2, P_2 \cap H_1) \Longleftrightarrow x \in P_1 \subseteq P_2 \Longrightarrow x+H_2 \neq_2 H_2$;

$(x+H_2)+'(y+H_2) \in P_1/(H_2, P_2 \cap H_1) \Longleftrightarrow$

$\Longleftrightarrow x+y+H_2 \in P_1/(H_2, P_2 \cap H_1) \Longleftrightarrow x+y \in P_1 \Longrightarrow x \in P_1 \vee y \in P_1 \Longleftrightarrow$

$\Longleftrightarrow x+H_2 \in P_1/(H_2, P_2 \cap H_1) \vee y+H_2 \in P_1/(H_2, P_2 \cap H_1)$;

$-'(x+H_2) \in P_1/(H_2, P_2 \cap H_1) \Longleftrightarrow -x+H_2 \in P_1/(H_2, P_2 \cap H_1) \Longleftrightarrow$

$\Longleftrightarrow -x \in P_1 \Longrightarrow x \in P_1 \Longleftrightarrow x+H_2 \in P_1/(H_2, P_2 \cap H_1)$;

$x+H_2 \in H_1/(H_2, P_2 \cap H_1) \wedge y+H_2 \in P_1/(H_2, P_2 \cap H_1) \Longleftrightarrow$

$\Longleftrightarrow x \in H_1 \wedge y \in P_1 \Longrightarrow x+y \in P_1 \Longleftarrow x+y+H_2 \in P_1/(H_2, P_2 \cap H_1)$.

COROLLARY 7.1.(The Isomorphism Theorem) Let $(M,=_M,\neq_M,+)$ be a group and let (H_1,P_1) and (H_2,P_2) be two pairs consisting of compatible subgroups and cosubgroups of the group M such that $P_2 \cap H_1 \neq \emptyset$, and let H_2 be a subgroup of the group H_1 and $P_1 \subseteq P_2$. Then there exists an isomorphism

$$f: M/(H_1,P_1) \longrightarrow (M/(H_2,P_2))/(H_1/(H_2,P_2\cap H_1),P_1/(H_2,P_2\cap H_1)).$$

Proof.

The isomorphism f is defined with

$$x+H_1 \longmapsto (x+H_2)+H_1/(H_2,P_2\cap H_1).$$

REFERENCES

[1] E.Bishop, Foundations of constructive analysis; McGraw-Hill New York 1967.

[2] W.Julian, R.Mines and F.Richman, Algebraic numbers, a constructive development; Pacific Journal of Mathematics, (74)1(1978),91 - 102.

[3] D.A.Romano, Equality and diversity in constructive mathematics; Publikacija Više tehničke škole u Bihaću, Serija A: Matematika, 1(1985), 1 - 14.

[4] ----------, Constructive algebra - algebraic structures; Ph D. Tesis. University of Belgrade, 1985/86.

[5] ----------, Ringa and fields, a constructive view; To appear in Zeitschift fur Mathematische Logik und Grundlagen der Mathematik.

[6] W.B.G.Ruitenburg, Intuitionistic Algebra; Ph.D.Tesis. University of Uresht, 1982.

[7] D.S.Scott, Identity and existence in intuitionistic logic; Springer Lecture Notes in Mathematics, 753(1979), 660 - 696.

[8] A.S.Troelstra, Principles of intuitionism; Springer Lecture Notes in Mathematics, 95(1969).

[9] A.S.Troelstra and D. van Dalen, Constructivism in Mathematics, An introduction (Preliminary draft of Chapter VIII: Algebra).

Daniel A. Romano

77ooo BIHAĆ
Ozimice, TO-10, ulaz 1, stan 13/IV
Yugoslavia

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

CONTRAINTUITIONIST LOGIC AND SYMMETRIC SKOLEM ALGEBRAS - CONTINUATION 1

Kajetan Šeper

Abstract. Classical logic is conceptually symmetric although its various presentations are generally asymmetric. Constructive logic, intuitionist as well as contraintuitionist, is conceptually asymmetric and its presentations are necessarily more or less asymmetric. As early as 1917 Skolem, [1], originated and investigated a conceptually and presentationally symmetric system of "logic of classes", by quite formal algebraic means, as a more general system than the classical system of Boolean algebras. Later on, the system was called variously: implicative-subtractive Skolem algebras (Curry) or semi-Boolean algebras and Heyting-Brouwer logic (Rauszer), and investigated by various methods (Rauszer). Some decades ago appeared a number of more or less symmetric and constructive systems of "logic with strong negation" (Fitch,Nelson, Markov, Vorob'ev, and others), culminating in Zaslavskiĭ's, [2], "symmetric constructive logic". Here we propose a system, NS, of "constructive symmetrist logic", CSL, which is traditionally constructive, totally symmetric, and free from strong negation. The system is founded on general symmetrist ideas and stipulations. It unifies both systems, those of intuitionist and contraintuitionist logic, and extends each of them conservatively. It is closely related to and more general than the systems mentioned above.

0. INTRODUCTION. In the previous paper, [3], a direct unification of the asymmetric systems of intuitionist and contraintuitionist logic was sketched and only fragments of the resulting systems of "symmetric intuitionist logic", SJL, and "absolute symmetric Skolem algebras", SA, were stated. In these continuations we wish to improve the deficiency by stating the systems in their entirety.

To realize this program we have, in the first place, to make it precise how to handle logical deductions involving assumptions as well as contraassumptions simultaneously. This is done in this continuation.

This paper is in final form and no version of it will be submitted for publication elsewhere.

As we imagine a logician in the role of a constructive (effective, or operative) symmetrist constructing the system, we prefer calling it from now on more appropriately and specificly constructive symmetrist logic, CSL.

In the continuations to come we intend to elaborate suitable algebraic and topological representations.

1. CONSTRUCTIVE SYMMETRISM. To begin with, a symmetrist associates to each formula, especialy to each schematic formula involving a connective, its positive (or t-) and its negative (or f-) meaning. For a constructive symmetrist, the former is to be intuitionist, modeled by constructions (or proofs), and the latter containtuitionist, modeled by contraconstructions (disproofs, or refutations). A formula is considered to represent a true statement, or a false statement, if it is capable of being intuitionistically constructed, or contraintuitionistically constructed (or contraconstructed), respectively. The truth criteria will be specified by downwards applicable natural deduction rules and the falsity criteria by upwards applicable ones. As we proceed we shall generalize these stipulations.

The problem of generalization of the stipulations arises, e.g., if we wish to handle the intuitionist $\supset$ as a f-connective. To fix its meaning in that case we have to state sufficient and necessary conditions under which, possibly simultaneously from some assumptions (or t-assumptions) and contraassumptions (or f-assumptions), a $\supset$-formula A $\supset$ B is to be considered as capable of being contraconstructed i.e. as representing a false statement. The conditions are: under all the given t- and f-assumptions, A is to be true and B false. Therefore, the natural deduction rule should involve a certain mixture of downwards applicable rules (or t-rules) and upwards applicable rules (or f-rules) combined together. Such a situation appears neither in intuitionist nor in contraintuitionist logic, but it does appear quite normally in constructive symmetrist logic.

Similarly, the same problem arises if we wish to handle the contraintuitionist $\not\subset$ as a t-connective.

The acceptance of symmetrist attitude makes it possible and initiates, for completing the intuitionist and contraintuitionist connectives, new connectives to be introduced. The new connectives should be introduced in the constructive manner of intuitionist-like, or contraintuitionist-like, or by combined constructions.

E.g., the abjunction A $\searrow$ B (read as "sine" or "but false") is introduced as a t-connective by the same conditions as for $\supset$ as a f-connective, but if we treat it as a f-connective, the conditions are quite different from those for $\supset$ as a t-connective: A $\searrow$ B is considered to represent a false statement if either A is false or B is true. Hence, $\searrow$ and $\supset$ are only "partially cross-expressible" by each other; more exactly, $\searrow$ as a t-connective and $\supset$ as a f-connective are expressible by each other only.

Regarding its logical dual, the contraabjunction B $\nwarrow$ A (right-to-left reading applied, and read as "contrasine" or "but true"), both $\searrow$ and $\nwarrow$ are "totally cross-expressible" by each other: $\searrow$ as a t-connective and $\nwarrow$ as a f-connective, as well as $\searrow$ as a f-connective and $\nwarrow$ as a t-connective, are expressible by each other.

The role of these "mixed" junctions is analogous to that of "pure" junctions $\wedge$ and $\vee$.

The constructive symmetrist introduces also new logically dual "mixed" plications, t-plication $\curvearrowright$ and f-plication $\curvearrowleft$ (right-to-left reading applied), the conditions for and the role of which being analogous to those of "pure" plications $\supset$ and $\not\subset$.

For a constructive symmetrist, the t- and f-meanings associated to formulas, and schematic formulas involving connectives, are not meant as being separated from each other — the former being understood by an intuitionist and the latter by a contraintuitionist — but rather as being simultaneously present. From a constructive symmetrist's viewpoint the t-meaning is to be modeled on intuitionist-like s-constructions (st-constructions) which include the intuitionist ones, and the f-meaning on contraintuitionist-like s-constructions (sf-constructions) which include the contraintuitionist ones. Both s-construction modelings will be realized by a kind of natural s-deduction. Consequently, for formulas of particular form their s-truth and s-falsity criteria will be specified by simultaneously downwards and upwards applicable natural s-deduction rules.

2. s-RULES. The general multiple form of simple (or local) natural s-deduction rules (or s-rules) is

$$\frac{\text{t-premises} \quad \text{f-conclusions}}{\text{t-conclusions} \quad \text{f-premises}}$$

Any s-rule is quadripartite: one distinguishes its left (or t-) and its right (or f-) part; and, for each of these parts, one distinguishes its premise and its conclusion part.

Any s-rule is bidirected: for each of its parts, either left or right, one distinguishes the direction from premises to conclusions.

The complex (or global) s-rules may be assumed by additional information of various types which alter the applicability stipulations with respect to simple s-rules.

The notion of s-deduction generated by the multiple rules could be inductively defined (and visually represented) by a kind of bidirected quadripartite graphs (or s_m-graphs) or by a kind of bidirected dichromatic bipartite graphs (or $s_m^{(o)}$-graphs) (both being closely related to and generalizing Shoesmith and Smiley's bipartite graphs).

However, for the sake of simplicity in this paper we shall use only strictly singular form of s-rules i.e.

st-rules: $\dfrac{A_1 \dots A_n}{B \mid C_p \dots C_1}$

and

sf-rules: $\dfrac{A_1 \dots A_n \quad D}{C_p \dots C_1}$

The complex s-rules we shall use in this paper are all of the same type: to any t-premise formula a formula may be indicated in brackets and placed above or on the right-hand-side of it; to any f-premise formula a formula may be indicated in brackets and placed bellow or on the left-hand-side of it.

Thus, the notion of s-duduction generated by the singular rules is inductively defined by means of bidirected trees (or s-trees) as follows.

3. s-RULE APPLICATION. 3.1. The basis of induction consists of exhibiting the most elementary s-deductions associated to formulas.

Any formula A supplied with an indication of its t- or f-status is a s-deduction; more exactly, the elementary s-deduction of the form

A

is a st-deduction of A from itself as a t-assumption, and the elementary s-deduction of the form

A

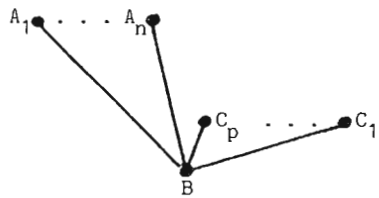
is a sf-deduction of A from itslef as a f-assumption.

3.2. The inductive step depends on the rule chosen, and consists of extending given s-deductions so to form a new s-deduction according to the rule. The step may be called the rule application, and the new deduction its result.

Capital Greek letters possibly with sub- and super-scripts

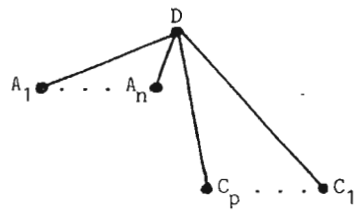
denote as usually formula sequences.

3.2.1. For any chosen simple st-rule, given st-deductions of A_i ($i=1,\dots,n$) from t-assumptions Γ_i and f-assumptions Δ_i, and given sf-deductions of C_k ($k=1,\dots,p$) from t-assumptions Γ'_k and f-assumptions Δ'_k, the extended s-deduction of the form



(B being bellow all A_i and C_k) is a st-deduction of B from t-assumptions $\Gamma \equiv \Gamma_1, \dots, \Gamma_n, \Gamma'_1, \dots, \Gamma'_p$ and f-assumptions $\Delta \equiv \Delta_1, \dots, \Delta_n, \Delta'_1, \dots, \Delta'_p$.

3.2.2. Similarly, for any chosen simple sf-rule, under the same conditions as above, the extension



(D being above all A_i and C_k) is a sf-deduction of D from t-assumptions Γ and f-assumptions Δ.

3.2.3. In both cases of a s-deduction the repetition of assumption formulas is allowed to be omitted.

3.2.4. If the chosen s-rule is complex, then any of its indicated formulas placed above or on the left-hand-side of a premise formula P is meant to be a t-assumption of the given s-deduction of P; otherwise, if it is placed bellow or on the right-hand-side of P, it is meant to be a f-assumption of the given s-deduction of P.

The complex s-rule prescribes the indicated assumption formulas to count no more as such but as "discharged" by the application.

4. s-DEDUCIBILITY. As a consequence of the definition of s-deduction one defines as usually two kinds of s-deducibility relations i.e.

st-deducibility: $\Gamma[\Delta \vdash B$

and

sf-deducibility: $D \dashv \Gamma]\Delta$

or, more compactly,

$\Gamma[\Delta \vdash B[$ and $\Gamma[\Delta \vdash [D,$

respectively.

5. THE SYSTEM NS OF CSL. The s-formulas of CSL are defined also in the usual way i.e. as formed from atomic formulas by the binary connectives $\wedge \vee \searrow \nwarrow \supset \not\subset \supsetneq \subsetneq$ and the zero-ary ones (or constants) $\bot \top$.

In order to anticipate multiple rules, and consequently multiple deductions, yet persisting in singular ones, we shall use the following multiple rules as abbreviations for singular ones:

$$\frac{\Gamma \qquad D_q \ \dots \ D_1}{B_1 \ \dots \ B_n \qquad \Delta} \quad \text{for} \quad \frac{\Gamma \quad E \ \dots \ E \quad E[D_1] \dots E[D_q]}{E \qquad\qquad \Delta}$$

and

$$\frac{\Gamma \qquad\qquad E}{[B_n]E \ \dots \ [B_1]E \quad E \ \dots \ E \quad [D_q] \quad [D_1]}$$

and

$$\frac{\Gamma}{\Delta} \quad \text{for} \quad \frac{\Gamma}{B \qquad \Delta} \quad \text{and} \quad \frac{\Gamma \qquad D}{\Delta}$$

The particular s-rules of NS are divided into several groups and subgroups (st-,sf-,I-,E-; junctions $\wedge \vee \searrow \nwarrow$, plications $\supset \not\subset \supsetneq \subsetneq$, absurds $\bot$ $\top$; intuitionist J 1-4, contraintuitionist CJ 1-4) according to the following table:

s-rules of NS

	st-rules: I-rules	st-rules: E-rules		sf-rules: E-rules	sf-rules: I-rules	
J1	$\frac{A \quad B}{A \wedge B}$	$\frac{A_1 \wedge A_2}{A_i}$	S1	$\frac{A \quad B}{A \wedge B}$	$\frac{A_1 \wedge A_2}{A_i}$	CJ2
J2	$\frac{A_i}{A_1 \vee A_2}$	$\frac{A \vee B}{A \quad B}$	S2	$\frac{A_i}{A_1 \vee A_2}$	$\frac{A \vee B}{A \quad B}$	CJ1
	$\frac{A}{A \searrow B \quad B}$	$\frac{A \searrow B \quad A}{A}$ $\frac{A \searrow B \quad B}{A}$	S3	$\frac{A}{B \quad A \searrow B}$	$\frac{B \quad A \searrow B}{A}$ $\frac{A \searrow B}{A}$	
	$\frac{A}{B \nwarrow A}$ $\frac{B \nwarrow A \quad B}{A}$		S4	$\frac{E}{B \nwarrow A}$ $\frac{A}{B \nwarrow A}$	$\frac{B \quad B \nwarrow A}{A}$	
J3	$\frac{[A]}{B}$ $\frac{A \quad A \supset B}{B}$		S5	$\frac{A \quad A \supset B}{A}$ $\frac{B}{A \supset B}$	$\frac{A \quad A \supset B}{B}$	
	$\frac{B}{B \not\subset A \quad A}$ $\frac{B \not\subset A}{B}$ $\frac{B \not\subset A}{A}$		S6	$\frac{B}{B \not\subset A \quad A}$	$\frac{B \not\subset A}{B}$ $\frac{}{[A]}$	CJ3
	$\frac{B \quad [A]}{A \supsetneq B}$ $\frac{A \supsetneq B}{B \quad A}$		S7	$\frac{A_i}{A_1 \supsetneq A_2}$	$\frac{A \supsetneq B}{A \quad B}$	
	$\frac{B \quad A}{B \subsetneq A}$ $\frac{A_2 \subsetneq A_1}{A_i}$		S8	$\frac{A \quad B}{B \subsetneq A}$	$\frac{B \subsetneq A}{[A] \quad B}$	
	$\frac{A}{\bot \quad A}$	J4 $\frac{\bot}{B}$	S9		$\frac{\bot}{}$	
	$\frac{}{\top}$		S10	$\frac{B}{\top}$	CJ4 $\frac{A \quad \top}{A}$	

The role of $\bot$ as a t-constant is that of a st-absurd having no st-construction. In JL, its role is that of an intuitionist absurd having no intuitionist construction; J4 is traditionally called "ex falso quodlibet", efq, and it can be abbreviated by the multiple "antiaxiomatic"

$$efq_m \quad \frac{\bot}{}$$

For this reason $\leftarrow$S9E is called st-efq.

The role of $\bot$ as a f-constant is that of a sf-theorem having a sf-construction.

Similar remarks apply to $\top$ as a f- as well as a t-constant. Therefore S10$\rightarrow$E is called sf-"ex vero quodlibet", sf-evq.

$\leftarrow$S9I is called st-"non-contradiction", st-ncd; under st-efq it can be replaced by

$$\frac{A}{B \mid A}$$

S10$\rightarrow$I is called sf-ncd; under sf-evq, it can be replaced by

$$\frac{A \mid B}{A}$$

Hence, under st-efq and sf-evq, both st- and sf-cnd together can be abbreviated by the multiple "s-antiaxiomatic"

$$s_m\text{-cnd} \quad \frac{A \mid A}{}$$

Remark 1. If the table contained the following rules instead

$$\frac{A \mid A}{\bot} \qquad \text{S9} \qquad \frac{A \mid A}{\bot} \qquad \frac{\bot}{\mid A}$$

$$\frac{}{\top} \qquad \frac{\top \mid A}{A} \qquad \text{S10} \qquad \frac{A \mid \top}{A}$$

then one would obtain the symmetric D-system, DSL.

$\leftarrow$S10E can be called st-"tertium non datur", st-tnd; under $\leftarrow$S10I; it can be replaced by the multiple "axiomatic"

$$\frac{A}{A \mid A}$$

S9$\rightarrow$E can be called sf-tnd; under S9$\rightarrow$I, it can be replaced by

$$\frac{A}{A \mid A}$$

being the same as above. Hence, under $\leftarrow$S10I and S9$\rightarrow$I, the multiple "s-axiomatic"

$$s_m\text{-tnd} \quad \frac{A \mid A}{A}$$

can abbreviate both st- and sf-tnd.

Remark 2. If the table contained besides the cnd-rules also the tnd-ones, one would obtain the symmetric classical system, KSL.

Remark 3. Especially with respect to S9 and S10 some other combination of rules might be of interest, e.g., that for the symmetric minimal system, MSL, containing neither the cnd-rules nor the tnd-ones.

Remark 4. In this paper we do not consider the class of s-absurds, $\bot_2$, neither we iterate the process to obtain CSL of second order, CSL_2, and so forth.

Remark 5. One obviously extends the presented propositional logic to the full predicate one.

Remark 6. One also obviously transforms the presented natural s-deduction formulation, NS, of CSL into its coextensive s-sequent calculus reformulation, LS.

Remark 7. To be sure that the system CSL extends the systems of JL and CJL conservatively, one has to prove the following theorem.

THEOREM. For any (intuitionist) $\wedge\vee\supset\bot$-formulas Γ and B,

$$\Gamma \vdash B \quad \text{(in NS)} \iff \Gamma \vdash B \quad \text{(in NJ)}$$

holds good. For any (contraintuitionist) $\wedge\vee\not\subset\top$-formulas Δ and B,

$$\Delta \vdash D \quad \text{(in NS)} \iff D \dashv \Delta \quad \text{(in NCJ)}$$

holds good.

Remark 8. If one wished to transform the presented singular system, NS, of CSL into its coextensive multiple reformulation, N_mS, one should prove the following theorem.

THEOREM. For any s-formulas Γ, Γ_o, $\Delta \equiv B_1, \ldots, B_m$, and $\Delta_o \equiv D_q, \ldots, D_1$,

$$\Gamma \vdash \Gamma_o \vdash \Delta \vdash \Delta_o \ (\text{in } N_mS) \iff \Gamma \vdash \Gamma_o \vdash \Delta^\wedge \vdash \Delta_o^\vee \ (\text{in NS})$$
$$\iff \Gamma \vdash \Gamma_o \vdash \Delta^\wedge \vdash \Delta_o^\vee \ (\text{in NS})$$

hold good. Here $\Delta^\wedge$ stands for B_j's conjunction, if $m \geq 2$, or for B_1 itself, if $m = 1$, or for $\top$, if $m = 0$; similarly, $\Delta_o^\vee$ stands for D_1's adjunction, or D_1 itself, or $\bot$, respectively.

Remark 9. The restricted CSL containing only $\wedge\vee\supset\not\subset\bot\top$ and S1,2,5,6,9,10 is a minimal unification of both JL and CJL. (It was but mentioned in [3] under the name of "simple".) The whole CSL extends it conservatively as well.

6. s-EXPRESSIBILITY. In sec.1 we have indicated some types of expressibility of connectives. The expressibility is now precisely defined by s-interdeducibility.

DEFINITION. For given s-formulas A and B, one defines the following types of s-expressibility relation:

tf-, or ft-, expressibility by

$$A \rightleftharpoons B: \Leftrightarrow B \leftrightharpoons A: \Leftrightarrow A\,[\vdash [B \;\&\; [B \vdash A\,[$$

t-expressibility by

$$A \rightleftharpoons B: \Leftrightarrow A[\vdash B[\;\&\; B[\vdash A[$$

f-expressibility by

$$A \doteqdot B: \Leftrightarrow [A \vdash [B \;\&\; [B \vdash [A$$

cross-expressibility by

$$A \times B: \Leftrightarrow A \rightleftharpoons B \;\&\; A \leftrightharpoons B$$

parallel-expressibility by

$$A = B: \Leftrightarrow A \doteqdot B \;\&\; A \doteqdot B$$

The first three relations are called partial, and the last two total.

COROLLARY. a) The relations $\rightleftharpoons$, $\doteqdot$, and $=$ are reflexive, symmetric, and transitive. b) The relation $\times$ is symmetric and parallel-transitive: $A \times B \;\&\; B \times C \Rightarrow A = C$. c) The following expressibility relations hold good:

$$A \searrow B \rightleftharpoons A \supset B$$
$$B \not\subset A \rightleftharpoons B \nwarrow A$$
$$A \supset B \doteqdot A \vee B$$
$$B \wedge A \rightleftharpoons B \not\subset A$$
$$A \searrow B \times A \nwarrow B$$

The last relation shows that each of $\searrow$ or $\nwarrow$ is cross-expressible by the other. In such a case we say that each of them is cross-quasi-definable by the other, and so, under that view, superfluous. If we had chosen only one of them as primitive, the relation, as we say, cros-quasi-defines the other by the chosen one, and the relation is called its cross-quasi-definition. However, for the sake of symmetricity of presentation, we have chosen both.

Similarly, a connective may happen to be parallel-expressible by another one, in case of which we say it is parallel-quasi-definable by the other.

E.g., the injunction $A \downarrow B$ and the equivalence $A \supset\subset B$ are defined by such quasi-definitions:

$$A \downarrow B: \times A \vee B$$
$$A \supset\subset B: = (A \supset B) \wedge (B \supset A)$$

Next we list the most interesting quasi-definitions.

DEFINITION. The "weak" negations are defined as reductions to absurd:

negation by $\neg A: = A \supset \bot$
contranegation (or affirmation) by $A^{\perp}: = \top \not\subset A$
t-affirmation by $\downarrow A: = A \supset \!\!\!\cdot\, \bot$
f-negation by $A^{\not\perp}: = \top \not\supset A$

and the "strong" plications as two-sided combinations:

in-ex-plication (or t-biplication) by $A \sqsupset B: = (A \supset B) \searrow (A \not\subset B)$
ex-in-plication (f- or contra-biplication) by $B \not\sqsubset A: = (B \supset A) \nwarrow (B \not\subset A)$
t-cross-plication by $A \rightleftarrows B: = (A \supset \!\!\!\cdot\, B) \wedge (B \supset \!\!\!\cdot\, A)$
f-cross-plication by $B \not\rightleftarrows A: = (A \not\supset B) \;\; (B \not\supset A)$

Remark 10. For the chosen connectives, problems of their independence, completeness etc. arise. If deeper insights into CSL are needed, its tetralogical foundational study is to be developed (in the sense of Lorenzen's dialogical foundation of logic).

7. STRONG NEGATIONS. As mentioned in the abstract, a number of systems of logic with strong negation appeared by several authors. However, all those systems are presentationally asymmetric, and indeed t-presented.

The logically dual "strong" connectives, strong negation, $-\cdot A$, and strong contranegation (or strong affirmation), $A \cdot -$, are introduced as new connectives in CSL by the following rules which characterize them as t- as well as f-connectives explicitely:

$$\frac{-\cdot A \;|\; A}{-\cdot A \;|\; A} \qquad \frac{A \;|\; -\cdot A}{A \;|\; -\cdot A} \qquad \text{S11}$$

$$\frac{A\cdot - \;|\; A}{A\cdot - \;|\; A} \qquad \frac{A \;|\; A\cdot -}{A \;|\; A\cdot -} \qquad \text{S12}$$

Thus one obtains the system of a quasi-t-presentation of CSL, call it CSL:$\cdot$-$\cdot$ containing $-\cdot$ $\cdot-$ and S11, 12, in addition.

Obviously, $-\bullet A \dashv\vdash A$ and $A \bullet - \dashv\vdash A$ hold, and hence $-\bullet A = A \bullet -$ holds, too. So, $-\bullet$ and $\bullet -$ are totally parallel-interexpressible. If $-\bullet$ is the only primitive connective, it is denoted simply by $-$, and the system itself by CSL:-.

The relations $-A \dashv\vdash A\bot$ and $-A \dashv\vdash \neg A$ show that $-$ is a combination of $\neg$ as a f-connective and $\bot$ as a t-connective.

The system CSL:- can be simplified in various ways. E.g., the relations

$$A \searrow B = A \wedge -B$$
$$B \nwarrow A = -B \vee A$$
$$B \nLeftrightarrow A = -(-A \supset -B)$$
$$A \nRightarrow B = -A \supset B$$
$$B \nLeftarrow A = -(A \supset -B)$$
$$\top = -\bot$$

enable to reduce it to the system of a restricted quasi-t-presentation of CSL:-, call it $\wedge\vee\supset\bot$ -restricted CSL:-, with only $-$ $\wedge \vee \supset \bot$, S11, and S1, 2,5,9 replaced by the transforms $S^*1,2,5,9$, respectively:

$\leftarrow S^*1 \equiv \leftarrow S1$ $\qquad S^*1$ $\qquad \dfrac{-(A \wedge B)}{-A \mid -B} \qquad \dfrac{-A_i}{-(A_1 \wedge A_2)}$

$\leftarrow S^*2 \equiv \leftarrow S2$ $\qquad S^*2$ $\qquad \dfrac{-(A_1 \vee A_2)}{-A_i} \qquad \dfrac{-A \quad -B}{-(A \vee B)}$

$\leftarrow S^*5 \equiv \leftarrow S5$ $\qquad S^*5$ $\qquad \dfrac{-(A \supset B)}{A} \mid \dfrac{-(A \supset B)}{-B} \mid \dfrac{A \quad -B}{-(A \supset B)}$

$\leftarrow S^*9 \equiv \leftarrow S9$ $\qquad S^*9$ $\qquad \dfrac{}{-\bot}$

Remark 11. If, in addition, S11 is replaced by

$$\frac{A}{--A} \qquad \frac{--A}{A} \qquad S^*11$$

containing $\leftarrow S^*11$ solely, one obtains the system of a pseudo-presentation of $\wedge\vee\supset\bot$-restricted CSL:-, call it CSL^*:- $\wedge\vee\supset\bot$, having no explicite characterization of $-$. This property is a remarkable disadvantage of the system (and similar systems with strong negation).

Remark 12. More drastical modifications of CSL:- (restricted or not) are possible, and some of them actually appeared in the literature. E.g., the system of a deformed presentation of restricted CSL:-, call it

CSL:-$\sqsupset$, is obtained by replacing $\supset$ by $\sqsupset$ and S^*5 by the corresponding transform $S^{**}5$ for $\sqsupset$. If, in addition, S11 is replaced by S^*11, one obtains the system of a deformed pseudo-presentation of CSL:-, call it CSL^{**}:- $\wedge\vee\sqsupset\bot$.

Remark 13. Disregarding minor differences, the system CSL^* is essentially that of Vorob'ev, and the systems CSL:-$\supset$ and CSL^{**} are those of Zaslavskiĭ.

REFERENCES

1. Th.Skolem, Untersuchungen über die Axiome des Klassenkalküls und über Produktations- und Summationsprobleme, welche gewisse Klassen von Aussagen betreffen, Videnskapsselskapets Skrifter, I. Mat.-Nat. Klasse 3 (1919), pp.37.
2. I.D. Zaslavskiĭ, Simmetričeskaja konstruktivnaja logika, Erevan 1978.
3. K.Šeper, Contraintuitionist logic and symmetric Skolem algebras, pp. 155-163 in: Proc. of the 4th Conf. "Algebra and Logic", Zagreb 1984.

Institute and Faculty of Mechanical Engineering
University of Osijek at Slavonski Brod
Trg maršala Tita 18
55000 Slavonski Brod

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

MAPPINGS OF ORDERED SETS

by Milan R. Tasković

Abstract

In this paper we present some new characterizations of inductiveness, completeness, conditionally completeness and chain completeness of posets in terms of fixed apexes, fixed edges and fixed points.

1. INTRODUCTION AND MAIN RESULTS. An order-preserving (isotone or increasing) map f of a partially ordered set (:=poset) P to itself has a *fixed point* if there exists an element ξ in P such that $f(\xi) = \xi$. P is said to have the *fixed point property* if every isotone map f of P into itself has a fixed point. The first of the fixed point theorems for partially ordered sets goes back to Tarski and Knaster (c.f.[TA]), who proved that the lattice of all subsets of a set has the fixed point property. In the mid - 1950's Tarski [TA] published a generalization: *Every complete lattice has the fixed point property* . Tarski [TA] raised the question whether the converse of this result also holds. Davis [DA] proved the converse: *Every lattice, with the fixed point property is complete.*

In [RI] , Rival published a far-reaching extension: Every isotone map of finite, connected poset P into itself has a fixpoint.

Let a poset P be called INDUCTIVE (CHAIN COMPLETE) when every non-empty chain in P has an upper bound (supremum) in P. Many authors have investigated properties of posets satisfying some sort of chain-completess condition and used them in a variety of applications. Tarski's fixpoint theorem generalizes to chain-complete posets, i.e. if $f: P \to P$ is an isotone map and P is a chain-complete poset, then the set of fixpoints is a chain-complete poset under the induced order. This sharpens the results of Abian and Brown [AB] , that every isotone, self-map of chain-complete poset has a fixpoint. Conversely, Markowski [MG] show that if every isotone map $f: P \to P$ has a least fixpoint, P is chain-complete.

*) This paper is in final form and no version of it will be submited for publication elsewhere.

Also, Klimeš [KJ] characterized chain complete posets in terms of the least fixed points of relatively isotone selfmappings.

In this paper we consider a concept of FIXED APEXES for the mapping f of a poset into itself. A map f of a poset P to itself has a *fixed apex* $u \in P$ if for $u \in P$ there is $v \in P$ such that $f(u) = v$ and $f(v) = u$. The point u, v P are called fixed apexes of f if $f(u) = v$ and $f(v) = u$.

In this paper we present a new characterization of inductiveness (chain-completeness) of posets in terms of the fixed apexes.

The analogous problem for *conditionally complete* (that is, every nonempty subset of P with upper bound has its supremum) partially ordered sets has remained largely unexplored.

It should be pointed out that the result of Davis [DA] cannot be transferred to the completely ordered sets that are not lattices. That is seen from the following example.

EXAMPLE 1. Let the set P ={a,b,c} be ordered by $\leq$ so that $a \leq b$, $a \leq c$ and assume the elements b, c are ancomparable; as shown on the diagram (Fig. 1):

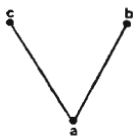


Fig. 1


Fig. 2

Every isotone mapping $f: P \to P$ has the fixed point, but yet P is still not completelly ordered set. However, P is conditionally complete.

We begin with a statement for conditionally complete sets.

FIXED POINT LEMMA: *Let* (P,$\leq$) *be a partially ordered set and* f *a mapping from* P *into* P *such that:*

(A) f *is an isotone mapping,*

(B) f has a *fork* i.e. $a \leq f(a) \leq f(b) \leq b$ *for some* $a,b \in P$, *and*

(C) *The set* $]a,b[$ or P *is a conditionally complete.*

Then

(1.1.) *The set* $I(P,f) := \{x \in P: f(x) = x\}$ *is nonempty ,*

and

(1.2.) *Neither of the conditions* (A), (B), (C) *can be deleted if* (1.1.) *is to be valid.*

A brief proof of this statement may be found in our paper of conditionally complete posets i.e.see Tasković [MI].

In connection with the preceding, analogous to the Fixed Point Lemma we have an immediate consequence:

LEMMA 0. *Let* (P,$\leq$) *be a chain complete poset and* f *an isotone mapping from* P *into* P *such that*
(LF) f has a *left fork* i.e. $a \leq f(a)$ for some $a \in P$.
Then there exists a fixed point of f .

Let P be a partially ordered set and f a mapping from P into P. For any $f: P \to P$ it is natural to consider the following set

$$\mathrm{Sub}\, f(P) := f(P) \cup \{a \in P \mid a = \mathrm{ub}\, C, \text{ for some chain } C \text{ in } f(P)\},$$

where ub C is an upper bound of C.

We begin with the following Lemma which is essential.

LEMMA 1. (Eixed Apexes Lemma). *Let* L *be an inductive lattice and* f *a mapping from* P *into itself such that*
(M) $x \leq f^2(x)$, *for all* $x \in \mathrm{Sub}\, f(L)$.
Then there exists a fixed apex of f .

We notice that the map f *has a fixed apex if and only if* $f^2 := f(f)$ *has a fixed point.*

Namely, if f has fixed apexes $u, v \in L$, then $u = f(v)$ and $v = f(u)$, i.e. we can see that $u = f^2(u)$ and $v = f^2(v)$. Hence, the equation $x = f^2(x)$ has a solution. On the other hand, if the equation $x = f^2(x)$ has a solution $\xi = f^2(\xi)$ for some $\xi \in L$, then f has fixed apexes $\xi, f(\xi) \in L$, because $\xi = f^2(\xi)$ and $f(\xi) = f(\xi)$. This completes the proof of preceding remark.

PROOF OF LEMMA 1. Since L is a inductive lattice, then L is with majorant i.e. every non-empty chain in L has an upper bound in L. By Zorn's lemma (or Bourbaki's lemma) there exists a maximal element $z \in \mathrm{Sub}\, f(L)$ i.e. Sub f(L) has a maximal element. From the condition (M) we have $z \leq f^2(z)$ and because z is a maximal element of the set Sub f(L) it will be also $f^2(z) \leq z$. Hence, we obtain the relation $f^2(z) = z$, i.e. the equation $x = f^2(x)$ has a solution $z \in L$. Hence, from the preceding remark, f has a fixed apex. This completes the proof of this statement.

THEOREM 1. *For a lattice* L *to be inductive it is necessary and sufficient that every mapping* f *on* L *to* L *with the condition* (M) *has a fixed apex.*

Proof. Since the condition of this theorem is known to be necessary for the inductiveness of a lattice, from Lemma 1, we have only to show that it is sufficient. In other words, we have to show that, under the assumption that the lattice L is not inductive, there exists mapping f on L to L without fixed apexes and with the condition (M).

Suppose that the lattice L is not inductive. We first notice that there exists at least one subset of L without a majorant, upper bound (for otherwise the lattice would be inductive). Hence we can find a chain A of L with the following property :an upper bound i.e. *majorant* of A, does not exists in L.
Let U be a chain cofinal with A such that

$$U:=\{x\in A\ x_0\leq x\},\ x_0=\text{a fixed element of } A=\min U.$$

Thus all the elements of U can be arranged in a sequence i.e.one can show that there exist increasing sequence $\{x_\alpha\}$ in U such that:$\{x_\alpha\}$ is strictly increasing and, for each $t\in U$, there exists $\alpha(t)$ such that $\alpha(t)<\alpha$ implies $t\leq x_\alpha$, and an upper bound of $\{x_\alpha\}$ does not exist.

We define a mapping f from L into itself according to the following presciption

$$(1)\qquad f(x)=\begin{cases} x_\beta, & \text{if } x=x_\alpha\in U \\ x_0:=\min U, & \text{if } x\notin U \end{cases}$$

where $x_\alpha\leq x_\beta$ $(x_\alpha\neq x_\beta)$ for any $\alpha<\beta<w$, and where w is any (finite or transfinite) ordinal. Thus we have defined a function f on L to L. Now, for any $x\in U(\supset \text{Sub } f(L))$ we have $x\leq f^2(x)$ i.e. $x=x_\alpha\leq x_\gamma=f(x_\beta)=f(f(x_\alpha)=f^2(x_\alpha)=f^2(x)$, for $\alpha<\beta<\gamma<w$; so f satisfies the condition (M), and does not has a fixed apex.

Thus the function $f:L\to L$ satisfies the condition (M) and does not have fixed apexes. This completes the proof of this main statement.

The following result of Bourbaki [BO] , allows us to prove the basic fixpoint for complete lattice without using the Axiom of Choice (see [MT]). We extensions this statement of Bourbaki [BO], in our paper [MT] .

LEMA 2. (Fixed Point Lemma). *Let* L *be an inductive lattice and* f *a mapping from* L *into itself such that*

(T) $x\leq f(x)$, *for all* $x\in\text{Sub } f(L)$.

Then there exists a fixed point of f.

PROOF is analogous to the proof of the preceding Lemma 1 (see, Tasković [MT]).

In connection with the preceding, L is said to have the *general fixed point property* if every map f of L into itself with the condition (T) has a fixed point. Analogously, L is said to have the *fixed apex property* if every map f of L into itself with the condition (M), has a fixed apex.

We are now in a position to formulate our the following general main statement.

THEOREM 2. Let L be a lattice, then the following statements are equivalent:

(a) L is an inductive lattice,

(b) L has the fixed apex property,

(c) L has the general fixed point property.

PROOF. From Theorem 1, (a) is equivalent to the condition (b). Lemma 2 implies that (c) is a consequence of (a). Thus, we need only show that (c) implies (a).

Suppose that the lattice L is not inductive. Then there exists a sequence (chain) A in L, that does not have an upper bound. We define a mapping f from L into itself with (1). Then f is well defined and for any $x\in\text{Sub } f(L)$ we have $x\leq f(x)$, i.e. i.e. $x=x_\alpha\leq x_\beta=f(x_\alpha)=f(x)$. Thus, f satisfies the condition (T), and does not have a fixed point. Thus, the proof is complete.

2. SOME COROLLARIES. In this section we give applications of the preceding statements.

We notice, in [KJ] Klimeš, [KĐ] Kurepa and [BB] Baclawski-Björner considered the concept of a *fixed edge* for the order-reversing (antitone or decreasing) mapping of a lattice into itself. Let f be an antitone mapping of a lattice L into itself and let $a\leq b$ be elements of L. An ordered pair (a,b) is called a *fixed edge* of f if f(a)=b and f(b)=a. We notice that fixed edges are evidently fixed apexes, and the set of all fixed edges can be a proper subset of the set of fixed apexes. Also, fixed point is evidently fixed apex.

In connection with this, we are now in a position to formulate the following statement.

THEOREM K. (Klimeš [KJ]). *Let* L *be a complete lattice and* f *an antitone mapping of* L *into itself. Then there exists a fixed edge of* f.

PROOF. L is a complete lattice, and applying Lemma 1 to the set $S:=\{x\in L \mid x\leq f^2(x)\}$, we obtain that f has fixed apexes $u,v\in S$, where $v=\sup I(f^2,L)$ for $I(f^2,L):=\{x\in L \mid x=f^2(x)\}$ and $u\leq v$, i.e. f has a fixed edge.

In connection with the preceding, we notice that the terms of fixed edges are not best sufficiency for characterization of inductiveness of lattices.

Namely let $L:=\mathbb{N}=\{0,1,2,\ldots\}$ be the chain of the natural numbers. L *is obviously not inductive* . Let f be an antitone mapping on L, then the set $\{0,1,\ldots f(0)\}$ is closed under f, because $0<k$ implies $f(k)\leq f(0)$. But this is a finite inductive lattice, i.e. from Theorem K, f has a fixed edge, which is a fixed edge of L too.

This example proof the preceding remark.

Ih this section, we present a new characterization of chain-completeness and completeness of posets i.e. lattices.

Let P be a partially ordered set and f a mapping from P into P. For any $f:P\to P$ it is natural to consider the following set

$$\overline{f(P)}:=f(P)\cup\{a\in P \mid a=\sup C, \text{ for some chain } C \text{ in } f(P)\}.$$

In connection with the preceding, analogous to the Lemmas 1,2 we have an immediate consequence:

LEMMA 3. *Let* L *be a complete lattice and* f *a mapping from* L *into itself such that*

(LM) $x\leq f^2(x)$, *for all* $x\in\overline{f(L)}$

Then there exist a fixed apex of f.

LEMMA 4. *Let* L *be a complete lattice and* f *a maping from* L *into itself such that*

(LT) $x\leq f(x)$, *for all* $x\in\overline{f(L)}$.

Then there exists a fixed point of f.

PROOFS. L is complete lattice, and hence $\overline{f(L)}$ is an inductive lattice, also. Applying the Lemmas 1,2 to the set $\overline{f(L)}$, we obtain that f has a fixed apex or a fixed point.

LEMMA 5. *Let* P *be a totally ordered set by the order relation* $\leq$. *If the nonempty part A of* P *does not have a supremum, then there is, by relation* $\leq$, *well ordered subset* A_0 *of the set* A *which does not have an upper bound in* A.

PROOF. According to Zermelo's theorem there is a well order $\trianglelefteq$ of set A. Based on the theorem of transfinite definition, there is the function $f:A\to\{0,1\}$ with the characteristics:

1^o $f(a)=1$, where $a=\min A$ in the system $(A,\trianglelefteq)$,

2^o $f(x)=1$ or $f(x)=0$, for every $x\trianglelefteq a$, $x\in A$, according whether it is or whether it is not $t<x$, for every $t\trianglelefteq x$ for which $f(t)=1$.

Due to $f(a)=1$ the set $A_0=f^{-1}(\{1\})\subset A$ is nonempty. On the other hand,

(Δ) $x\trianglelefteq y\Rightarrow x<y$, for all $x,y\in A_0$.

Indeed, let A_1 be the set of all elements $t\in A_0$ with characteristic that (Δ) is valid for all $x,y\in\{u\in A_0: u\trianglelefteq t\}$. It is evident that $a\in A_1$.

If $v\in A_1$ for every $v\in\{u\in A_0: u\trianglelefteq t\}$, where $t\in A_0$, then the condition (Δ) is valid and $y\trianglelefteq t$ (because this condition and hypothesis $x\trianglelefteq y$ lead to $y\in A_1$ and $x,y\in\{u\in A_0: u\trianglelefteq y\}$); in the case when, $y=t$ and $x\in A_0$, relation $x\trianglelefteq y$, i.e. $x\trianglelefteq t$ lead to, $x<t=y$, having in view the way in which the set A_0 is defined and the characteristic 2^o of the function f. Hence according to the theorem of the transfinite induction the equality $A_1=A_0$ is proved, that is, the condition (Δ) is valid for every $x,y\in A_0$. Having in view the well order by the relation $\trianglelefteq$ of the set A_0, from that it follows immediately

$$x\trianglelefteq y\iff x<y, \text{ for all } x,y\in A_0$$

and it means that the set A_0 is well ordered by the relation $\leq$.

At last, let $x\in A$. This element cannot be the upper bound of the set A, because we would have $x=\max A=\sup A$. Because of that the set $X:=\{t\in A \mid x<t\}$ is nonempty; there is $y=\min X$ in the system $(A,\trianglelefteq)$. Then $x<y$ and $t\trianglelefteq y$ implies $t\leq x<y$, for every $t\in A_0$, and this latter, considering the way in which the set A_0 is defined, gives $y\in A_0$. That is, the set A_0 has also the upper bound in A.

In connection with the preceding, L is said to have the *locally*

general fixed point property if every map f of L into itself with the condition (LT), has a fixed point. Analogously, L is said to have the *locally fixed apex property* if every map f of L into itself with the condition (LM), has a fixed apex.

From the preceding statements and Lemma 5, we are now in a position to formulate our the following general main statement:

THEOREM 3. Let L be a lattice, then the following statements are equivalent:

(a) L *is a chain-complete lattice,*
(b) L has the locally general fixed point property
(c) L has the locally fixed apex property.

PROOF. From Theorem 2, and Lemma 4, (b) is a consequence of the condition (a). Lemma 3 implies that (c) is a consequence of (a), i.e. (b). Thus, we need only show that (c) implies (a).

Suppose that the lattice L is not complete (chain-incomplete). Then there exists a sequence (chain) A in L, that does not have a least upper bound. We define a mapping f from L into itself with (1). Then f is well defined and for any $x \in U(\supset \overline{f(L)})$ we have $x \leq f^2(x)$, i.e. $x=x_\alpha \leq x_\gamma = f(x_\beta)=f(f(x_\alpha))=f^2(x)$, for $\alpha<\beta<\gamma<w$. Thus, the condition (LT) holds, for $x \in \overline{f(L)}$. Thus, f satisfies the condition (LT), and does not have a fixed point. Thus, the proof is complete.

Let P and Q be posets and f:P→Q a map (posets are nonempty by definition). Map f is *inf-preserving* if for all X⊂P such that infX exists in P and $f(\inf_P X)=\inf_Q f(X)$.

We are now in a position to formulate the following statement, from the preceding statements.

THEOREM 4. *Let* L *be a lattice. If* L *has minimum, then the following statements are equivalent:*

(a) L *is a complete lattice,*
(b) L *has the locally fixed apex property,*
(c) L *has the locally general fixed point property,*
(d) (Tarski [TA], Davis [DA]). L *has the fixed point property,*
(e) (Markowski [MG]). *Every inf-preserving map* f:L→L *has a least fixpoint.*

THEOREM 5. (Tasković [TI] ,[MI]). *Let* (P,≤) *be a poset and suppose if* x, y *are upper bounds of a bounded subsets* X *of* P, *then there is an upper bound* z *for* X *such that* z≤x *and* z≤y. *For set* P *to be conditionally complete it is necessary and sufficient that every increasing function* f : P→P *with fork has a fixed point.*

We note, that the partially ordered set P on Fig.2. is not conditionally complete, however, every isotone mapping f:P→P has the fixed point. This prove that the condition:
(DD) if x,y are upper bounds of a bounded subsets X of P, then there is an upper bound z for X such that z≤x and z≤y;
cannot be removed in preceding statement.

In connection with the preceding, analogous to this statement and Lemma 1 we have an immediate consequence:

THEOREM 6. *Let* (P,≤) *be a partially ordered set with the condition* (DD). *For set* P *to be chain complete it is necessary and sufficient that every increasing function* f:P→P *with left fork has a fixed point.*

PROOF . The necessity follows from Lemma. It remains to prove the sufficiency. In other words, we have to show that, *under the assumption that the set* P *is not conditionally complete, there exists an increasing function* f *on* P *to* P *such that (B), without fixed points.*

Suppose that the set P is not conditionally complete. Then there exists a nonempty part U of P which is bounded from above and has not its supremum. Let us denote by V the set of all upper bounds of U. The sets U and V are nonempty, U has no supremum, and V has no infimum. Clearly infV does not exists, for if it did, it would coincide with supU, what contradicts the supposition that U has no supremum. One can show that there exist sequences (generalized) $\{x_\alpha\}$ in U and $\{x_\beta\}$ in V such that:

(1) $\{x_\alpha\}$ is increasing and, for each t∈U, there exist α(t) such α(t)<α implies $t \leq x_\alpha$, and

(2) $\{x_\beta\}$ is decreasing and, for each t∈V, there exists β(t)<β such that β(t)<β implies $x_\beta \leq t$.

To define f:P→P for any element x∈P, we distinguish two cases depedent upon whether x is a lower bound of $\{x_\beta\}$ or not . In the first case, by (1) and (2), if x is not an upper bound of $\{x_\alpha\}$ then

(3) $f(x) = \min\{x_\alpha : x_\alpha \not\leq x\}$.

where, $a \not\leq b$ will be used to express the fact that $a \leq b$ does not hold. In the second case, we let

(4) $f(x) = \max\{x_\alpha : x \not\leq x_\beta\}$.

Thus we have defined a function f on P to P. From (1) - (4) if follows clearly that either $f(x) \not\leq x$ of $x \not\leq f(x)$ for every $x \in P$; thus f has no fixpoints, and also then (B) holds.

Let x and y be any elements of P with $x \leq y$. If x is a lower bound of $\{x_\beta\}$ but y is not, then, by (1)-(4), $f(x) \leq f(y)$. If bouth x and y are lower bounds of $\{x_\beta\}$ we see from (2) and (4) that $f(x) \leq f(y)$. Finally, if x is not a lower bound of $\{x_\beta\}$, then y is not either, and by an argument analogous to that just outlined (using (3) and (4) we again obtain $f(x) \leq f(y)$. Thus the function f is increasing, and the proof of the theorem is complete.

Special cases of Theorem have been discussed by Davis [DA], Tarski [TA] and some others.

Let L be a lattice. In this part we consider the following functional equation

(FE) $f^2(x) := f(f(x)) = g(x), \qquad x \in L,$

where $g: L \to L$ is a given increasing function and $f: L \to L$ is the unknown function.

We notice, the equation (FE) has a solution if the equation

(E) $FgF: = F(g(F(x)) = x, \qquad x \in L,$

has a solution where g is a given increasing function and $F: L \to L$ is the unknown function.

LEMMA 6. *Let L be an incomplete lattice. If there exists an antitone function* $\Pi: L \to L$ *such that*

(Π) $g(a) = b\,(a, b \in L) \Rightarrow (\exists x \in L)\,(\Pi(b) = x \wedge \Pi(x) = a)$,

then the equation (FE) *has a solution of the form* $f(x) = g(\Theta(x))$, *where* $\Theta(x)$ *is an arbitrary solution of the equation* (E).

PROOF. The equation (E) has a solution if the condition (Π) holds. In that case its solution is $\Theta(x)$, i.e.

$\Theta g \Theta = x$, $x \in L$. Then, for $f(x) = g(\Theta(x))$, we have

$$f^2(x) = f(g(\Theta(x)) = g(\Theta(g(\Theta(x))) = g(x),$$

which means that $f(x) = g(\Theta)$ is a solution of (FE). This proves the preceding statement.

IN PARTICULAR, if $\Theta(x)$ is a decreasing mapping, then $f(x) = g(\Theta)$ is a decreasing function, because $g: L \to L$ is a given increasing function.

2. *Further results.* With the help of Lemmas we now obtain the main result of this section.

THEOREM 7. *For a lattice L to be complete it is necessary that every antitone mapping on L to L have a fixed edge,* and sufficient that L with the condition (Π) has the fixed edge property.

We note that the condition (Π) can be replace with the condition that the functional equation (FE) has a solution an antitone function $f: L \to L$, where $g: L \to L$ is a given increasing function and $g(x) \neq x$, $x \in L$.

We are now in a position to formulate the following statement

THEOREM 8. *Let L be an incomplete lattice. If the functional relation (equation)*

(F) $\phi^2(x) = g(x) \neq x$ or $\phi^2(x) \neq x, \qquad x \in L$

where $g: L \to L$ *is a given increasing function and* $\phi: L \to L$ *is the unknown antitone function, has a solution; then there exists an antitone mapping f on L to L without fixed edges.*

We note, on the other hand, that it is easy to construct an incomplete lattice which the condition that (F) has a solution, but the condition (Π) is not satisfied.

EXAMPLE 1. Let $L := \{\ldots, -3, -2, -1, 1, 2, 3, \ldots\}$ be the chain of the integer numbers. L is obviously not complete. Then, the condition (Π) is not satisfied, i.e. the equation (FE) does not have solution in the class of desreasing functions, where $g: L \to L$ is an increasing map with $g(x) \neq x$, $x \in L$. But, the equation, relation, (F) has a solution in the class of decreasing functions. We give an example. For $g(n) = 4n$, $n \in L$, we have the function $f(n) = -2n$, $n \in L$ such that f is a solution of the equation (F).

Proofs. Since the condition of the theorem is known to be necessary for the completeness of a lattice, from Lemma 6, we have only to show that it is sufficient. In other words, we have to show that, under the assumption that the lattice L is incomplete, there exists an antitone mapping f on L to L without fixed edges.

Suppose that the lattice L is not complete. We first notice that there exists a least one subset of L without a least upper bound (for othervise the lattice would be complete). Hence we can find a subset A of L with the following properties: $\forall A$ does not exists and if X is any subset of L with smaller power than A, then $\forall A$ exists. Thus all the elements of A can be arranged in a sequence i.e. one can show that there exist increasing sequence i.e. one can show that there exist increasing sequence $\{x_\alpha\}$ in A such that: (1).

Let us denote by B the set of all upper bounds of $\{x_\alpha\}$. Clearly $\wedge B$ does not exist, for it did, it would coincide with $\forall\{x_\alpha\}$; this result would contradict (1). Now B, like A, is either empty or infinite. Since B is partly ordered by the relation $\leq$, there is a strictly decreasing sequence $\{x_\beta\}$ such that $\{x_\beta\}$ is a subset of B with which: (2).

To define $g: L \to L$ for any element $x \in L$, we distingush_two cases depedent upon whether x is a lower bound of $\{x_\beta\}$ or not. In the first case, by (1)-(2), if x is not an upper bound of $\{x_\alpha\}$ then (3) and (4).

Thus we have defined a dunction g on L to L. From (1)-(4) it follows clearly that either $g(x) \nleq x$ or $x \nleq g(x)$ for every $x \in L$, thus g has no fixpoints.

Let x and y be any elements of L with $x \leq y$. If x is a lower bound of $\{x_\beta\}$ but y is not, then, by (1)-(4), $g(g) \leq g(y)$. If both x and y are lower bounds of $\{x_\beta\}$ we see from (2) and (4) that $g(x) \leq g(y)$. Finally, if x is not a lower bound of $\{x_\beta\}$, then y is not either, and by an argument analogous to that just outlined (usign (3) and (4)) we again obtain $g(x) \leq g(y)$. Thus the function is increasing, and $g(x) \neq x$ for all $x \in L$.

From Lemma 6, define an antitone mapping $f: L \to L$ such that $f^2(x) := f(f(x)) = g(x)$. Let us prove that so defined mapping $f: L \to L$ does not have fixed edge.

If f would have an edge (u, v), then it would be also $f(u) = v$, $f(v) = u$, and hence $f^2(u) = f(v) = u$, $f^2(v) = v$. However, by construction it follows $f^2(x) = g(x) \neq x$ for all $x \in L$, we have a contradiction.

Thus the function $f: L \to L$ is an antitone and does not have fixed

edge. This completes the proof of the statements 7 and 8.

We notice that the following example will show that the condition (Π) cannot be omited in the Theorem 8.

Example 2. Let $L := \mathbb{N} = \{0, 1, 2, \ldots\}$ be the chain of the natural numbers. L *is obviously not complete*. Let f be an antitone mapping on L, then the set $\{0, 1, \ldots, f(0)\}$ is closed under f, because $0 < k$ implies $f(k) \leq f(0)$. But this is a finite complete lattice, i.e. from Lemma 5 f has a fixed edge, which is a fixed edge of L too.

However, the condition (Π) is not satisfied, i.e. the equation (FE) does not have solution in the class of decreasing functions, where $g: L \to L$ is an increasing map with $g(x) \neq x$, $x \in L$. Now, every antitone mapping $f: \mathbb{N} \to \mathbb{N}$ has a fixed edge, but yet lattice $\mathbb{N}$ is still not completelly ordered.

Also, the condition that the functional equation (F) has a solution in the class of decreasing function is not satisfied.

At the end of this paper we notice, in the our paper [TI] was considered the preceding problems (see Theorem 1,2 of [TI]). But the establishment of this problems was not good, and therefore was are turning again on this in Theorem 5 and 7.

REFERENCES

[AB] S.Abian, A.Brown, A theorem on partially oredered sets with application to fixed point theorems, Canadian J.of Math., 13(1961), 78-83

[BB] K.Baclawski, A.Björner, Fixed points in partially ordered sets, Advances in Math., 31(1979), 263-287

[BG] G.Birkhoff, Lattice theory, Amer. Math. Soc.Coloq.Publ. vol.25, New York, 1948

[BO] N. Bourbaki, Sur le theoreme de Zorn, Archiv der Math., 2(1950), 434-437

[DA] A. Davis, A characterization of complete lattices, Pacific J.Math. 5(1955), 311-319

[HH] H.Höft, M.Höft, Some fixed point theorems for partially ordered sets, Canad. J.Math., vol.28(5),1976, 992-997

[KJ] J.Klimeš, Fixed edge theorems for complete lattices, Arch.Math. 4. scripta, 17(1981), 227-234

[KL] J.Klimeš, Fixed points characterization of completeness of lattice for relatively isotone mappings, Arch.Math.,3, scripta, 20(1984),125-132

[KĐ] Đ.Kurepa, Fixpoints of decreasing mappings of ordered sets, Publ.Inst.Math. 32(1975), 111-116

[MG] G.Markovski, Chain-complete posets and directed sets with applications, Algebra Univ., 6(1976), 53-68

[MS] B.Muenzenberger, E.Smithson, Characterizations of compactness of the interval topology in semilattices, Proc. Amer.Math.Soc.46(1974), 133-136

[KO] S.Kogalovskij, On a theorem of Frink, Uspehi Math. Nauk, 19(1964), 143-145

[RI] I.Rival, A fixed point theorem for finite partially ordered sets, J.Combin.Th., A21(1976), 309-318

[SR] E.R.Smithson, Fixed points in partially ordered sets, Pacific Jour.Math. 45(1973), 363-367

[TA] A. Tarski, A lattice theoretical fixed point theorem and its applications, Pacific J.Math. 5(1955), 285-309

[TM] M.Tasković, Banach's mappings of fixed points on spaces and ordered sets, These, Math. Balkanica, 9(1979),p.150

[MT] M.Tasković, A monotone principle of fixed points, Proc.Amer.Math. Soc. 94(1985), 427-432

[TAS] M.Tasković, On an equivalent of the axiom of choice and its applications, Math.Japonica, 31, 6(1986), 979-991

[MT] M.Tasković, Characterization of conditionally complete posets, Facta Universitatis, 1(1986), 1-5

[TI] M.Tasković, Monotone mappings of ordered sets, Third Algebraic Conference, 1982, 153-154

[WA] E.Ward, Completeness in semi-lattices, Canad.J.Math. 9(1957), 578-582

[WO] S.Wolk, Dedekind completeness and a fixed point theorem, Canad. J.Math., 9(1957), 400-405

[ZE] E.Zermelo, Neuer Beweis für die Möglichkeit einer Wohlordnung, Math. Ann., 15(1908), 107-128

Prirodno-matematički fakultet
11000 Beograd, P. O. Box 550
Yugoslavia

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

A NOTE ON NON-EXISTENCE FOR SOME CLASSES OF CONTINUOUS (3,2) GROUPS

Kostadin Trenčevski

Abstract. In this paper it is proved that if M is n-cube ($n \geq 1$), or M is n-dimensional sphere, or M is a connected subset of R which contains more than one point, then there does not exist a continuous function $[\,]: M\times M\times M \to M\times M$ which defines a (3,2) group on M.

The definition of (n,m) groups (n > m) is given in [1]. We give here only the definition of (3,2) groups.

DEFINITION 1. The pair $(M,[\,])$ is (3,2) group if $[\,]: M^3 \to M^2$ and the next conditions are satisfied

(i) $(\forall_{a,b,c,d\in M})$ $\quad [[abc]d] = [a[bcd]]$

(ii) For arbitrary $a,b,c \in M$ the equations $[axy]=(b,c)$ and $[xya]=(b,c)$ have solutions for x and y.

It can be proved that the equations in (ii) have unique solutions if $(M,[\,])$ is (3,2) group.

Dimovski [3] has shown the existence of non-trivial (3,2) group by constructing the free (3,2) group. In this paper we shall give some results of non-existence for some classes of continuous (3,2) groups.

The mapping $\Psi: M^2\times M^2 \to M^2$ defined by $\Psi((a,b),(c,d)) = [[abc]d]$ induces a group structure (M^2,Ψ). If (e_1,e_2) is the identity in (M^2,Ψ) then it is proved in [2] that $e_1=e_2$. Suppose that (e,e) is the identity in the group (M^2,Ψ) and let

$$\alpha(x) = \alpha_x = g(e,e,x), \quad \beta(x) = \beta_x = h(e,e,x) \qquad (1)$$

This paper is in final form and no version of it will be submitted for publication elsewhere.

where g and h are the first and the second components for the mapping $[\,]$. Then it will hold also that

$$g(x,e,e)=\alpha_x\,, \qquad h(x,e,e)=\beta_x \tag{2}$$

It is easy to verify that α_x and β_x also satisfy

$$g(a,\alpha_x,\beta_x)=a, \qquad h(a,\alpha_x,\beta_x)=x, \tag{3}$$

$$g(\alpha_x,\beta_x,b)=x, \qquad h(\alpha_x,\beta_x,b)=b, \tag{4}$$

for arbitrary $a,b\in M$.

Dimovski [3] has proved the following lemma.

LEMMA 1. If $(M,[\,])$ is nontrivial (3,2) group, i.e. $|M|\geqslant 2$, then for arbitrary $x,y\in M$ it is satisfied

$$\alpha_x\neq x, \qquad \beta_x\neq x \quad \text{and} \quad \alpha_x\neq\beta_y\,.$$

If $[\,]$ is continuous function it follows that g and h are also continuous functions and from (1) it also follows that α and β are continuous functions.

THEOREM 1. There does not exist continuous function $[\,]:D^n\times D^n\times D^n\longrightarrow D^n\times D^n$ where D^n is n-cube $(n\geqslant 1)$ which defines a (3,2) group on D^n.

Proof. Assume that there exists a (3,2) group with the required properties. Then α is continuous function on D^n and Brower fixed-point theorem implies that there exists a point y such that $\alpha_y=y$. This contradicts the lemma.∎

THEOREM 2. There does not exist continuous function $[\,]:S^n\times S^n\times S^n\longrightarrow S^n\times S^n$ $(n\geqslant 1)$ which defines a (3,2) group on S^n.

Proof. Assume that there exists a continuous function $[\,]:S^n\times S^n\times S^n\longrightarrow S^n\times S^n$ which defines a (3,2) group. Since α is continuous function on S^n, it maps S^n on a compact subset of S^n. It follows from the lemma above that α is not a bijection, and since $\alpha(S^n)$ is closed subset of S^n, there exists a point $y\in S^n$ and $\varepsilon>0$ such that $B(y,\varepsilon)\cap\alpha(S^n)=\emptyset$ where $B(y,\varepsilon)=\{z\in S^n \mid d(z,y)<\varepsilon\}$. The set $S^n\setminus B(y,\varepsilon)$ is homeomorphic to n-cube and $\alpha(S^n\setminus B(y,\varepsilon))\subseteq S^n\setminus B(y,\varepsilon)$. Brower fixed-point theorem implies that there exists a point $z\in S^n\setminus B(y,\varepsilon)$ such that $\alpha_z=z$ and this contradicts the lemma.∎

THEOREM 3. There does not exist continuous function $[\,]:M^3\longrightarrow M^2$ where M is a connected subset of R, such that

$[\,]$ defines a nontrivial (3,2) group on M.

Proof. Assume that there exists a continuous function with the required properties. We should consider three possibilities a) $M=[0,1]$, b) $M=[0,1)$ and c) $M=(0,1)$ because each connected subset of R such that $|M|>1$ is homeomorphic to one of these three sets.

a) In this case the proof follows from the theorem 1.

b) From the above lemma it follows that if the inequality $\alpha_x>x$ holds for $x=x_0$ then it holds for each $x\in M$. It also holds for the inequalities $\alpha_x<x$, $\beta_x>x$ and $\beta_x<x$. Since $\alpha_0>0$ and $\beta_0>0$ we obtain that for each $x\in M$ $\alpha_x>x$ and $\beta_x>x$. The mappings α and β are continuous and $\lim_{x\to 1}\alpha_x=\lim_{x\to 1}\beta_x=1$ and so we obtain that there exist $x,y\in M$ such that $\alpha_x=\beta_y$. This contradicts the lemma above.

c) Analogously as in the previous case we see that

(i) $(\forall_{x\in M})\quad \alpha_x<x<\beta_x$, or (ii) $(\forall_{x\in M})\quad \beta_x<x<\alpha_x$.

Now we will prove that the equation $h(e,y,z)=z$ has solution for $y,z\in M$.

Assume that $\alpha_x<x<\beta_x$ for each $x\in(0,1)$. Then $h(e,\alpha_x,\beta_x)=x<\beta_x$. On the other hand it follows from (1) that $h(e,e,\beta_x)=\beta_{\beta_x}>\beta_x$. The function $\theta(t)=h(e,t,\beta_x)-\beta_x$ is positive for $t=e$ and negative for $t=\alpha_x$. Since θ is continuous, there exists $y\in(0,1)$ such that $\theta(y)=0$, i.e. $h(e,y,\beta_x)=\beta_x$.

Assume that $\alpha_x>x>\beta_x$ for each $x\in(0,1)$. Then the function $\theta(t)=h(e,t,\beta_x)-\beta_x$ is positive for $t=\alpha_x$ and negative for $t=e$. Since θ is continuous, there exists $y\in(0,1)$ such that $h(e,y,\beta_x)=\beta_x$.

Now we will prove that the equation $g(z,x,e)=z$ has solution for $x,z\in M$.

Assume that $\alpha_x<x<\beta_x$. Then the function $\theta(t)=g(\alpha_x,t,e)-\alpha_x$ is positive for $t=\beta_x$ and negative for $t=e$, and θ is continuous. So there exists $y\in(0,1)$ such that $g(\alpha_x,y,e)=\alpha_x$.

Assume that $\beta_x<x<\alpha_x$. Then the function $\theta(t)=g(\alpha_x,t,e)-\alpha_x$ is positive for $t=e$ and negative for $t=\beta_x$ and θ is continuous. So there exists $y\in(0,1)$ such that

$g(\alpha_x, y, e) = \alpha_x$.

Since the equation $h(e,y,z)=z$ has solution, it follows that $[eyz]=(p,z)$ where $p=g(e,y,z)$. On the other hand, from (4) it follows that $[\alpha_p \beta_p z]=(p,z)$, and since the equation $[xyz]=(p,z)$ has unique solution for x and y, we obtain $\alpha_p=e$. Similarly, since the equation $g(z,x,e)=z$ has solution it follows that $[z\ x\ e]=(z,q)$ where $q=h(z,x,e)$. On the other hand, from (3) it follows that $[z\ \alpha_q\ \beta_q]=(z,q)$, and since the equation $[zxy]=(z,q)$ has unique solution for x and y, we obtain $\beta_q=e$. Hence $\alpha_p=\beta_q$ and this contradicts the lemma. ∎

REFERENCES

1. G.Čupona, Vector valued semigroups, Semigroup Forum Vol. 26 (1983) 65-74
2. D.Dimovski, Some existence conditions for vector valued groups, Год. збор. Матем. фак. 33-34 (1982-1983), 99-103
3. D.Dimovski, On (3,2)-groups, Proceedings of the Conference "Algebra and Logic", Cetinje 1986.

Institut za matematika
Prirodno-matematički fakultet
p.f. 162, Skopje

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

A_t-GROUPOIDS

Janez Ušan

Abstract

In this article A_t-groupoids are induced, as one generalization of A_t-quasigroups [4], i.e. of A_t^m-quasigroups [2] , i.e. of A_t^3-and A_t^4-algebras (-quasigroups)[1]. By means of A_t^m-quasigroups one can coordinatise the finite regular planes whose lines ℓ satisfy the condition $|\ell| \geqslant 3$[3], and by A_t-quasigroups finite TCL-geometries (2H-geometries) whose lines ℓ satisfy the condition $|\ell| \geqslant 3$[4]. Among other things, it is proved in the paper that by means of A_t-groupoids one can coordinatise the finite 2H-geometries whose lines ℓ satisfy the condition $|\ell| \geqslant 2$. It is proved, in fact, that to every A_t-groupoid there corresponds one finite 2H-geometry, and that to every finite 2H-geometry there corresponds a class of disjoint generomorphic A_t-groupoids. Here every A_t-groupoid with $|[a,b]| \geqslant 3$, $a \neq b$, is generomorphic with some A_t-quasigroup.

This paper is in final form and no version of it will be submitted for publication elsewhere.

AMS mathematics subject classification (1980): 20N05.

Key words and phrases: A_t^m-quasigroups, A_t-quasigroups, A_t-groupoids, 2H-geometry.

Let (T,A), $|T|=t\in N\setminus\{1\}$, be a groupoid. A subgroupoid generated by $a,b\in T$ will be denoted by $([a,b],A)$[1] .

DEFINITION 1. A groupoid (T,A), $|T|=t\in N\setminus\{1\}$[1], is said to be an A_t-groupoid iff:

G0 $(\forall a\in T)A(a,a)=a$; and

G1 $a\neq b\wedge c\neq d\wedge[a,b]\neq[c,d]\Rightarrow|[a,b]\cap[c,d]|\leqslant 1$

for all $a,b,c,d\in T$.

PROPOSITION 1. If a groupoid (T,A), $|T|=t\in N\setminus\{1\}$, satisfies G1 and

G0̄ $(\forall a\in T)(\exists b\in T)(\exists c\in T)(a\neq b\wedge a\neq c\wedge[a,b]\neq[a,c])$, then (T,A) satisfies G0 as well.

Proof

From

$[a,b]\neq[a,c]\wedge a\neq b\wedge a\neq c$,

and by G1, it follows that

(a) $|[a,b]\cap[a,c]|=1$.

The assumption

$A(a,b)=d\neq a$

implies that

$d\in[a,b]\wedge d\in[a,c]$,

i.e. that

$|[a,b]\cap[a,c]|\geqslant 2$.

This contradicts to (a), proving the proposition.

Tab. 0 represents a groupoid $(\{1,2,3\},A)$ in which $[1,2]=[1,3]=[2,3]$, i.e. which fails to satisfy the proposition

1) $a\neq b\Rightarrow|[a,b]|\geqslant 2$.

A	1	2	3
1	2	1	3
2	1	3	2
3	3	2	1

Tab. 0

$[a,b]\neq[c,d]\wedge a\neq b\wedge c\neq d$

for all $a,b,c,d\in\{1,2,3\}$. Thus, $(\{1,2,3\},A)$ satisfies G1[1]. Thereby, since $(\{1,2,3\},A)$ is not an idempotent groupoid, we get the following proposition:

PROPOSITION 2. There is a groupoid (T,A), $|T|=t\in N\setminus\{1\}$, satisfying G1, and fails on G0.

PROPOSITION 3. Let (T,A), $|T|=t\in N\setminus\{1\}$, satisfies G1. Then it also satisfies:

G2 every subgroupoid $([a,b],A)$, $a\neq b$, of (T,A) is generated by any two different elements of the set $[a,b]$.

Proof

Let $a,b,c,d\in T$ be four arbitrary elements, such that

(1) $a\neq b$,

(2) $c\neq d$ and

(3) $c,d\in[a,b]$.

By (2) and (3) it follows that

(4) $|[a,b]\cap[c,d]|\geqslant 2$.

Now, considering (1),(2) and the contraposition of G1, we get

(5) $|[a,b]\cap[c,d]|>1\Rightarrow[c,d]=[a,b]$.

Finaly , by (4) and (5) we conclude that the proposition holds.

PROPOSITION 4. If a groupoid (T,A), $|T|=t\in N\setminus\{1\}$,

1) $v(\bot\Rightarrow p)=\top$.

satisfies G2, then (T,A) satisfies G1 as well.

Proof

Let $a,b,c,d \in T$ be such that

(a) $[a,b] \neq [c,d] \wedge a \neq b \wedge c \neq d$.

Suppose that the proposition is not valid, i.e. that (a) implies

(b) $|[a,b] \cap [c,d]| > 1$.

Hence, it follows that there are $p,q \in T$ such that

(c) $p \neq q \wedge p,q \in [a,b] \wedge p,q \in [c,d]$.

Finally, (c) implies (by G2) that

$$[a,b]=[p,q]=[c,d],$$

i.e.

$$[a,b]=[c,d],$$

which contradicts to (a), proving the proposition.

By Definition 1, Proposition 3 and Proposition 4, we conclude immediately that the following proposition also holds:

THEOREM 5. An idempotent groupoid (T,A), $|T| = t \in \mathbb{N} \setminus \{1\}$, is an A_t-groupoid iff (T,A) satisfies G2[1].

DEFINITION 2. We say that an indempotent groupoid (T,A), $|T| = t \in \mathbb{N} \setminus \{1\}$, is an A_t^m - groupoid iff:

G3 $a \neq b \Rightarrow |[a,b]| = m \in \mathbb{N} \setminus \{1\}$
for all $a,b \in T$.

PROPOSITION 6. If a groupoid (T,A) is and A_t^m - groupoid, then it is an A_t-groupoid[2].

1) G1 <=> G2.

2) The converse does not hold: Proposition 11.

Proof

Let $a,b,c,d \in T$ be any four elements such that

$a \neq b \wedge c \neq d \wedge c,d \in [a,b]$.

Since $c \neq d$ and $c,d \in [a,b]$, it follows that:

$$[c,d] \subsetneq [a,b].$$

Hence, using G3, we get that:

$$[c,d]=[a,b].$$

Thus, we have proved the implication: G3 $\Rightarrow$ G2. Hence, by Theorem 5, we conclude that (T,A) is an A_t-groupoids.

Idempotent quasigroups satisfying G3 are said to be A_t^m-quasigroups. They are introduced in [2] as a generalization of A_t^3- and A_t^4-algebras (-quasigroups) [1]. Idempotent quasigroups satisfying G1 are said to be A_t-quasigroups. They are introduced in [4] as a generalization of A_t^m-quasigroups.

There is no A_t^m-groupoid on a twoelement set. An A_2^2-groupoid is given on Tab. 1. On any (finite) T with at least three elements, there is an A_m^m-quasigroup [3]. An A_3^3-groupoid which is not quasigroup is shoun on Tab. 2

A	1	2
1	1	2
2	1	2

Tab. 1

A	1	2	3
1	1	3	2
2	1	2	1
3	1	1	3

Tab. 2

The following proposition is an immediate consequence of Proposition 3 and of Definition 2:

COROLLARY 7. If (T,A) is an A_t-groupoid, then $([a,b],A)$ is an A_m^m-groupoid for all $a,b \in T, a \neq b$; $m=|[a,b]|$.

**

Let T be an unempty set, and let L be an nonvoid collection of some unempty subsets of T. Then we say that L is a partition of Hartmanis of type 2 on the set T [1] iff the following two conditions are satisfied:

H1 $(\forall A\in T)(\forall B\in T)(A\neq B\Rightarrow(\exists!\ell\in L)(A\in\ell\wedge B\in\ell))$; and

H2 $(\forall\ell\in L)|\ell|\geqslant 2$ [6] [2].

We shall say that the ordered pair (T,L) is an 2H-geometry, the elements of the set T will be the points, and the elements of L - the lines [3].

An immediate consequence of H1 is the following condition:

H3 $(\forall\ell\in L)(\forall\ell'\in L)(\ell\neq\ell'\Rightarrow|\ell\cap\ell'|\leqslant 1)$.

Let (T,A) be an A_t-groupoid. Let also

$L \overset{\text{def}}{=\!=} \{[a,b]\,|\,a,b\in T\wedge a\neq b\}$.

Then, by Proposition 3 and by the fact that H1$\Leftrightarrow$H3 $\wedge$ H1', where

H1' $(\forall A\in T)(\forall B\in T)(A\neq B\Rightarrow(\exists\ell\in L)(A\in\ell\wedge B\in\ell))$ [4]

and since $|[a,b]|\geqslant 2$, we conclude that the following proposition holds:

1) Shortly: 2H-partition of T.
2) To every 2H-partition of the set T there corresponds a ternary equivalence relation on T, and conversly [7].
3) 2H-geometries are TCL-geometries satisfying H2 [4-5]. For example, there are k-seminets $(T,\{L_1^k\})$, $k\in N\setminus\{1,2\}$ [8], whose underlying sets (T,L), $L=\bigcup_{i=1}^{k}L_i$, are TCL-geometries violating H2. Regular planes [1-3] are 2H-geometries satisfying the condition: $(\forall\ell\in L)(\forall\ell'\in L)|\ell|=|\ell'|$.

4) There are finite idempotent quasigroups violating C1 [4]

PROPOSITION 8. If (T,A), $|T|=t\in N\setminus\{1\}$, is an A_t-groupoid, and

(ℓ) $L \overset{\text{def}}{=\!=} \{[a,b]\,|\,a,b\in T\wedge a\neq b\}$,

then (T,L) is a 2H-geometry.

Hence, by the definition of a regular plane, we get the following proposition:

COROLLARY 8'. If (T,A), $|T|=t\in N\setminus\{1\}$, is an A_t^m-groupoids, and L is given by (ℓ), then (T,L) is a regular plane.

The following lemma also holds:

LEMMA 9. (J.Šiftar, [3]) For every $m\in N\setminus\{1,2\}$, there is an A_m^m-quasigroup [1].

Hence, using the fact that an A_2^2-groupoid exists (Tab. 1) we conclude:

LEMMA 9'. For every $m\in N\setminus\{1\}$ there is an A_m^m-groupoid.

PROPOSITION 10. To every 2H-geometry (T,L), where $|T|=t\in N\setminus\{1\}$, there corresponds an A_t-groupoid (T,A).

Proof

Let (T,L) be a finite 2H-geometry; $|T|=t\in N\setminus\{1\}$ [2]. Using lemma 9', we get the following:

1^o On every line $\ell_i\in L, i\in I$, there is A binary operation $A^{(i)}$, $i\in I$, such that $(\ell_i,A^{(i)})$ is an A_m^m-groupoid; $m=|\ell_i|$.

H1 and 1^o imply:

2^o For any two $a,b\in T, a\neq b$, there is one and only one (from those choosen in 1^o) $A^{(i)}, i\in I$, such that $A^{(i)}(a,b)\in T$.

Because of H1, every $a\in T$ is in at least one of the

1) The proof is given by the construction of one class of A_m^m-quasigroups ; $m\in N\setminus\{1,2\}$.
2) H2.

sets ℓ_i, $i\in I$. Hence, by 1^o, and by Corollary 7, we get:

3^o For every $a\in T$ there is at least one (from those choosen in 1^o) $A^{(i)}$, $i\in I$, such that where the equality holds for every $i\in I$ such that $a\in\ell_i$.

Now, by 2^o and 3^o, we conclude:

4^o (T,A) is a groupoid, where $A \overset{def}{=\!=} \bigcup_{i\in I} A^{(i)}$.

3^o Implies

5^o (T,A) is an idempotent groupoid.

Now, by H1, H2, 1^o, 2^o and 3^o, we get:

6^o (T,A) satisfies G1.

The proposition is proved.

Remark 1.

By Lemma 9, to each 2H-geometry (T,L) satisfying $|\ell|\in N\setminus\{1,2\}$ for every $\ell\in L$, one can associate an A_t-quasigroup [4].

Fig. 1 represents a 2H-geometry, with: $|\{1,4\}|=|\{2,4\}|=|\{3,4\}|=2$ and $|\{1,2,3\}|=3$. Thus, by Proposition 10, we get:

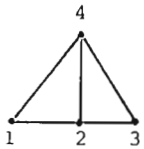


Fig. 1

PROPOSITION 11. There is an A_t-groupoid which is not an A_t^m-groupoid [1].

*

* *

We say that a groupoid (T,A) is generomorphic with a groupoid (T,B) iff

(ℊ) $[a,b]_A = [a,b]_B$ for all $a,b\in T$.

1) An analogous proposition holds for A_t-quasigroups [4].

The following proposition is obvious:

PROPOSITION 12. To be generomorphic is an RST-relation on the set $G(T)$ of all groupoids on T.

PROPOSITION 13. If a groupoid (T,A) is generomorphic with an A_t-groupoid (T,B), then (T,A) is also an A_t-groupoid.

Proof

Consider G1 for (T,B), i.e.:

$$(\forall a\in T)(\forall b\in T)\forall c\in T)(\forall d\in T)([a,b]_B\neq[c,d]_B\wedge$$
$$\wedge\ a\neq b\wedge c\neq d\Rightarrow|[a,b]_B\cap[c,d]_B|\leqslant 1).$$

Hence, since (T,A) and (T,B) are generomorphic, i.e.

$$(\forall x\in T)(\forall y\in T)[x,y]_A=[x,y]_B\ ,$$

we get:

$$(\forall a\in T)(\forall b\in T)(\forall c\in T)(\forall d\in T)([a,b]_A\neq[c,d]_A\wedge$$
$$\wedge\ a\neq b\wedge c\neq d\Rightarrow|[a,b]_A\cap[c,d]_A|\leqslant 1).$$

Thereby, since $[a,a]_A=[a,a]_B=\{a\}$ for every $a\in T$, we conclude that the proposition holds.

By Proposition 8 and by the definition of generomorphism, we conclude immediately:

THEOREM 14_1. If A_t-groupoids (T,A) and (T,B), are generomorphic, then the corresponding 2H-geometries (T,L_A) and (T,L_B) are equal;

$$L_A=\{[a,b]_A\,|\,a,b\in T\wedge a\neq b\},\ L_B=\{[a,b]_B\,|\,a,b\in T\wedge a\neq b\}.$$

The proof of Proposition 10 and the definition of generomorphism imply the following proposition:

THEOREM 14_2. Let (T,L) be a finite 2H-geometry, and let (T,A) and (T,B) be the corresponding A_t-groupoids [1].

1) In the sence of Proposition 10.

Then, (T,A) is generomorphic with (T,B).

Remark 2.

By Lemma 9, one can associate an A_7^3-quasigroup[1] to Figure Fano (i.e. to a projective plane of order 3). However, by means of the A_3^3-groupoid from Tab. 2, one can associate an A_7^3-groupoid which is not a quasigroup to the same plane. The influence of the medial law in $A_{m\,m}^{m\,n}$-quasigroup to the desargues-property of the corresponding regular planes was considered in [9].

Using Proposition 10, Remark 1 (Lemma 9) and Theorem 14_2, we get that the following proposition holds:

THEOREM 15. Every A_t-groupoid (T,A) satisfying

$$(\forall a \in T)(\forall b \in T)(a \neq b \Rightarrow |[a,b]| \geq 3)$$

is generomorphic with some A_t-quasigroup.

Immediately by Definition 1, we get

PROPOSITION 16. If the groupoid $(\hat{T},A)$, $|\hat{T}| = \hat{t} > 1$, is a subgroupoid of an A_t-groupoid (T,A), then $(\hat{T},A)$ is an $A_{\hat{t}}$-groupoid.

[1]) Considered already in [1].

REFERENCES

1 Szamkolowicz L., On the problem of existence of finite regular planes, Colloq. Math., 9(1962), 245-250.

2 Пухарев Н.К., Об A_n^k-алгебрах и регулярных конечных плоскостях, Сибирский Мат.ж., том VI ,No4(1965), 892-899.

3 Šiftar J., On the existence of A_n^k-quasigroups, Glasnik Mat., Vol. 18(38), 1983, 217-219.

4 Ушан Я ., A_t-квазигруппы, Review of Research Faculty of Science-University of Novi Sad, Vol. 15-2 (1985) .

5 Ушан Я ., LN -и RN - k - Полусети, Review of Research Faculty Science-University of Novi Sad, Vol. 16-1 (1986), to appear.

6 Hartmanis J., Generalized Partitions and Lattice Embedding Theorems, Proc. of Symposium in Pure Math., Vol. II, Lattice Theory, Amer. Math.Soc. (1961),22-30.

7 Pickett H.E., A note Generalized Equivalence Relations, Amer. Math. Manthly, 1966, 73, N^{o}8, 860-861.

8 Ušan J., k-Seminets, Mat. Bilten, Skopje, 1(XXVII), 1977. 41-46.

9 Пухарев Н.К., Геометрические вопросы некоторых медиальных квазигрупп, Сибирскии Мат. ж., Том IX, N^{o}4 (1968), 891-897.

Janez Ušan,
21000 NOVI SAD
Balzakova 25
Yugoslavia

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

ON CEP AND CIP IN THE LATTICE OF WEAK CONGRUENCES

Gradimir Vojvodić, Branimir Šešelja

Abstract. The aim of this paper is to give some lattice characterizations of the congruence extension peoperty (CEP) as well as of the congruence intersection property (CIP, see below) of an algebra A, the lattice being the one of all weak congruences (all congruences on all subalgebras) on A.

(CEP and CIP appear together among the conditions for the modularity of that lattice).

We show that A satisfies:

- CEP, if and only if D (diagonal) obeys the lattice cancellation law;
- CIP, if and only if D is distributive element;
- both CEP and CIP if and only if D is neutral element;

(all in the lattice of weak congruences).

We also characterize CEP and CIP by means of an embedding and an isomorphism of the above lattice into the Cartezian product $(S(A) \times C(A), \leqslant)$ (subalgebras and ordinary congruences).

This paper is in final form and no version of it will be submitted for publication elsewhere.

0. Let $A = (A,F)$ be an algebra and $K \subseteq A$ the set of its constants. Then ([8]), a weak congruence relation ρ on A is a symmetric, transitive and compatible relation on A, satisfying a weak reflexivity: If $c \in K$, then $c\rho c$.

We shall denote by

$S(A)$ the set of all subalgebras of A;
$C(A)$ the set of all congruences on A;
$C_w(A)$ the set of all weak congruences on A;
$C(B)$ the set of all congruences on $B \in S(A)$.

$C_w(A)$ is obviously a set of all congruences on all subalgebras of A, i.e.

$$C_w(A) = \bigcup (C(B) \mid B \in S(A)) .$$

Also, it is clear that $(C_w(A), \leqslant)$ is a lattice.

A is said to have the congruence extension property (CEP) ([1],[3],[7]) if every congruence on an arbitrary subalgebra of A is a restriction of a congruence on A.

A is said to have the congruence intersection property (CIP), if for all $\rho,\theta \in C_w(A)$

$$(\rho \wedge \theta)_A = \rho_A \wedge \theta_A ,$$

where

$$\rho_A \overset{\text{def}}{=\!=} \bigcap (\sigma \in C(A) \mid \rho \subset \sigma) .$$

If d_ρ is a diagonal of ρ, i.e.

$$d_\rho = \rho \wedge D , \quad \text{where} \quad D = \{(x,x) \mid x \in A\} ,$$

then $\rho_A = \rho \vee D$.

It was proved in [8] that:

I $(C_w(A), \leqslant)$ is an algebraic lattice, $(C(A), \leqslant)$ is its sublattice (as a filter generated by D) and $(S(A), \leqslant)$ is (up to the isomorphism) a retract of $(C_w(A), \leqslant)$ (as an ideal generated by D). The subalgebras are represented in $C_w(A)$ by diagonal relations.

II $(C_w(A), \leqslant)$ is a modular lattice iff

(i) $(S(A), \leqslant)$ is a modular lattice;
(ii) $(C(A), \leqslant)$ is a modular lattice;
(iii) A satisfies CEP;
(iv) A satisfies CIP.

A finite group has CIP iff it is Hamiltonian ([9]).

In [10], CEP, and CIP are given among the conditions for the complementness of the lattice $(C_w(A), \leqslant)$.

In the following we shall need some special elements of a lattice [4].

Let L be a lattice and $a \in L$. Then,

(1) a is distributive element if for all $x,y \in L$

$$a \vee (x \wedge y) = (a \vee x) \wedge (a \vee y) .$$

(2) Dually, a is codistributive if

$$a \wedge (x \vee y) = (a \wedge x) \vee (a \wedge y) .$$

(3) a is neutral element if for all $x,y \in L$

$$(a \wedge x) \vee (x \wedge y) \vee (y \wedge a) = (a \vee x) \wedge (x \vee y) \wedge (y \vee a) .$$

(This notion is obviously selfdual).

PROPOSITION 1. An algebra satisfies CEP if and only of for all $\rho,\theta \in C_w(A)$, $\rho \wedge D = \theta \wedge D$, and $\rho \vee D = \theta \vee D$ imply $\rho = \theta$. (i.e. iff D_A obeys the concellation law).

Proof. Note that $\rho \wedge D = \theta \wedge D$ and $\rho \vee D = \theta \vee D$ is equivalent with $d_\rho = d_\theta$ and $\rho_A = \theta_A$.

Suppose first that A satisfies CEP. Then, (see [8]) the mapping $\rho \to \rho_A$, from $C(B)$ to $C(A)$ ($B \in S(A)$, $\rho \in C(B)$) is an injection. Thus, if $d_\rho = d_\theta$, then $\rho,\theta \in C(B)$, and since $\rho_A = \theta_A$ it follows that $\rho = \theta$.

Let now A violates the CEP, i.e. suppose that there is $\rho \in C(B)$, $B \in S(A)$, such that for every $\theta \in C(A)$, $\rho \neq B^2 \wedge \theta$. Since $\rho \leqslant B^2$ and $\rho \leqslant \rho_A$, it follows that

$\sigma \overset{\text{def}}{=\!=} B^2 \wedge \rho_A \geq \rho$, and $\sigma_A = \rho_A$ ($\rho \leq \sigma$ implies $\rho_A \leq \sigma_A$, and $\sigma \leq \rho_A$ gives $\sigma_A \leq \rho_A$).

Since $\rho, \sigma \in C(B)$, $d_\rho = d_\theta$, but $\rho \neq \sigma$ and the cancellation is not satisfied. □

The following characterization of CIP is obvious:

PROPOSITION 2. *A satisfies CIP if and only if* D *is a distributive element in* $(C_w(A), \leq)$.

Proof. Straightforward, since $\rho_A = \rho_A \vee D$. □

COROLLARY 3. *A satisfies CIP if and only if the mapping* $h: C_w(A) \to C(A)$ *such that* $h(\rho) = \rho_A$, *is a homomorphism.*

Proof. The equality

$$(\rho \vee \theta)_A = \rho_A \vee \theta_A$$

is satisfied for all $\rho, \theta \in C_w(A)$ (since $\rho_A = \rho \vee D$). Thus, CIP (i.e. $(\rho \wedge \theta)_A = \rho_A \wedge \theta_A$) holds iff h is a homomorphism. □

(The proof follows from Proposition 2 as well, since by Ore's theorem (see for example Theorem 2.2. III in [4]) D is distributive in $(C_w(A), \leq)$ iff $\rho \to \rho \vee D$ is a homomorphism of that lattice into it's filter $[D) = C(A)$.)

Remark. Note that the dual mapping for h in Corollary 3 is always a homomorphism [8]:

(3′) *The mapping* $k: C_w(A) \to \overline{S(A)}$ *such that* $k(\rho) = d_\rho$ *is a homomorphism.*

($(\overline{S(A)}, \leq)$ is a sublattice of diagonals, isomorphic with $(S(A), \leq)$. In the following we identify those two structures).

The duality becomes obvious if we put

$$C(A) = [D) \qquad \overline{S(A)} = (D]$$

$$\rho_A = \rho \vee D \qquad d_\rho = \rho \wedge D \ .$$

Remark 2. Let $[\rho_A] = \{\theta \in C_w(A) \mid \rho_A = \theta_A\}$ be a class in $C_w(A)/\ker h$ to which ρ belongs. It is clear that $([\rho_A], \leq)$ is a sublattice of $(C_w(A), \leq)$ if *A* satisfies CIP. In that case, $(F_{\rho_A}, \leq)$ where $F_{\rho_A} = \{d_\theta \mid \theta \in [\rho_A]\}$ is (up to the isomorphism) a sublattice of $(S(A), \leq)$ (the proof is straightforward.) Thus, if algebra *A* satisfies CIP, then every congruence ρ on *A* determines a lattice of associated subalgebras $(F_\rho, \leq)$.

Consider now an algebra *A* satisfying both CEP and CIP.

PROPOSITION 4. *An algebra A satisfies CEP and CIP if and only if* D *is a neutral element in the lattice* $(C_w(A), \leq)$.

Proof. It is one result of Grätzer and Schmidt (1961, see Theorem 4.2. III in [4]) that an element of a lattice is neutral iff it is distributive, codistributive and obeys the concellation low. Consider D . Since for $\rho, \theta \in C_w(A)$, $d_{\rho \vee \theta} = d_\rho \vee d_\theta$ (see [8]) it follows that

$$D \wedge (\rho \vee \theta) = (D \wedge \rho) \vee (D \wedge \theta) \ .$$

i.e. D is codistributive element in $C_w(A)$.

The proof now follows by Propositions 1. and 2. □

PROPOSITION 5. *An algebra A satisfies CEP and CIP if and only if the mapping* $f: C_w(A) \to S(A) \times C(A)$, *given by* $f(\rho) = (d_\rho, \rho_A)$ *is an embedding.*

Proof. Let *A* satisfies CEP and CIP. Then by Proposition 4 D is neutral element in $(C_w(A), \leq)$. Now, the mapping $f: C_w(A) \to S(A) \times C(A)$ such that $f(\rho) = (d_\rho, \rho_A)$ is a homomorphism by Corollary 3 and its dual (3′). f is a bijection since D satisfies the cancellation low.

On the other hand, if f is an embedding, then by Theorem 4.2. III in [4] D is neutral if this embedding is such that

$$f(D) = (D, D)$$

which is obviously satisfied.

Thus, D is neutral and by Proposition 4 A satisfies CEP and CIP. □

Now we shall give the necessary and sufficient condition under which the mapping f from Proposition 5 is an isomorphism. (This condition is implicit in [10]).

PROPOSITION 6. For an algebra A, the mapping $f:C_w(A) \to S(A) \times C(A)$ where $f(\rho) = (d_\rho, \rho_A)$, is an isomorphism if and only if the lattice of congruences on any subalgebra of A is isomorphic with the lattice of congruences on the whole algebra A, under the mapping $\rho \to \rho_A$.

Proof. If f is an isomorphism, then by Proposition 5 A satisfies CEP and CIP. By CEP, $\rho \to \rho_A$ ($\rho \in C(B)$, $B \in S(A)$) is an injection. By CIP, this is a homomorphism. It is "onto" since every pair (d_{B2}, θ) has an inverse image (under f) $\rho \in C(B)$. But then $\theta = \rho_A$. Thus $\rho \to \rho_A$ is an isomorphism.

On the other hand, if $\rho \to \rho_A$ ($\rho \in C(B)$) is an isomorphism from $C(B)$ to $C(A)$, then f (defined in Proposition 5) is also an isomorphism, since

i) f is a bijection;

ii) f and f^{-1} preserve the order (see [10]). □

REFERENCES

[1] B.Biro, E.W.Kiss, P.P.Palfy, On the congruences extension property, Colloquia Mathematica Societatis Janos Bolyai, 29. Universal Algebra, Esztergom, 1977., 129-151.

[2] I.Chaida, Characterizations of relational blocks, Algebra Universalis, 10(1980), 65-69.

[3] A.Day, A Note on the congruence extension property, Algebra Universalis 1, (1971), 234-235.

[4] G.Grätzer, General lattice theory, Akademie-Verlag, Berlin, 1978.

[6] A.A.Iskander, The lattices of correspondences of universal Algebras, Izv. Akad. Nauk SSSR Ser. Math. 29(1965), 1357-1372.

[7] E.W.Kiss, L.Márki, P.Pröhle, W.Tholen, Categorical Algebraic properties, A compondium on amalgamation, congruence extension, epimorphisms residual smallness, and injectivity, Studia Sci. Math. Hung. 18(1983), 70-141.

[8] G.Vojvodić, B.Šešelja, On the lattice of weak congruence relations (to appear in Algebra Universalis).

[9] G.Vojvodić, B.Šešelja, A Note on the Modularity of the Lattice of Weak Congruences on a Finite group., (to appear in Contributions to General Algebra 5, Wien, 1986).

[10] B.Šešelja, G.Vojvodić, On the Complementness of the Lattice of Weak Congruences, to appear in Studia Sci.Math. Hung.).

Gradimir Vojvodić
Institute of Mathematics
University of Novi Sad
21000 Novi Sad
Dr Ilije Djuričića 4
Yugoslavia

Branimir Šešelja
Institute of Mathematics
University of Novi Sad
21000 Novi Sad
Dr Ilije Djuričića 4
Yugoslavia

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", CETINJE 1986.

ON LOCAL (NONASSOCIATIVE) NEAR-RING

Veljko Vuković

ABSTRACT. We make an extension of a part of the theory of local associative near-rings which is analogous to the corresponding part of nonassociative near-rings theory.

In fect, we initiate a study of local nonassociative near-rings in this paper. The necessary back ground material from the theory of nonassociative near-ring is given in Section 1. The definitions and basic properties of local (nonassociative) near-ring are given in Section 2.

1. PRELIMINARIES

DEFINITIONS 1. A unitary right nonassociative near-ring is a nonempty set S with two binary operations addition (+) and multiplication (•), such that :

1. The elements of S form a group (S,+) under addition ,

2. The elements of S form a groupoid (S, +) under multiplication ,

3. $\forall x \in S$, $x \cdot o = o$, where o is the additive identity of S ,

4. There exists an element $1 \in S$ such that $1 \cdot s = s \cdot 1 = s$, for all $s \in S$,

5. $\forall x,y,z \in S$, $(x + y) \cdot z = x \cdot z + y \cdot z$.

DEFINITION 2. A normal subgroup N of (S,+) is called the left ideal of a near-ring S if

$$s(s_1 + n) - ss_1 \in N$$

and two sided ideal if $ns \in N$ and $s(s_1 + n) - ss_1 \in N$, for all $n \in N$

and all $s, s_1 \in S$.

A subgroup $(H,+)$ of S is called an S-subgroup if $SH \subseteq H$. Near-ring homomorphisms and S-homomorphisms are defined in the usual manner. The kernels of (nonassociative) near-ring homomorphisms are ideals of S and every ideal I of S gives rise to a near-ring homomorphism with kernel I.

Beidleman [2] calls a left ideal strictly maximal if it is maximal as an S-subgroup and proves that an ideal I is strictly maximal if and only if S/I is a near-field.

A left radical J(S) of a (nonassociative) near-ring S is defined by $J(S) = \{\bigcap M/M$ is strictly maximal left ideal of $S\}$ (see Df. 3 [3]).

The element $a = (sr)t - s(rt)$, $s,r,t \in S$ is said to be an associator of the ordered triple (s,r,t). The ideal $\overline{A}(S)$ generated by the subset $A(S) = \{a = (sr)t - s(rt);\ s,r,t \in S\}$ is called an associator-ideal and the set A(S) an associator of S.

2. BASIC PROPERTIES OF LOCAL (NONASSOCIATIVE) NEAR-RING

DEFINITION 3. Let L be a subset of S of elements without left inverses, i.e. $L = \{\ell \in S / S \neq S\ell\}$. S is said to be a local near-ring if L is a left S-subgroup (Df. 2.1. [1]).

THEOREM 1. Let S be a near-ring, $A(S) \subseteq L$ and $(L,+)$ be a subgroup of $(S,+)$. Then S is a local near-ring if and only if $(U = S \setminus L, \cdot)$ is a groupoid.

PROOF. 1° If S is a local near-ring, then $(U,\cdot)$ is a groupoid. Assume that $xy = \ell \in L$, for some $x,y \in S \setminus L$. Then, $x^{-1}(xy) = x^{-1}\ell$. From here, $y+a = x^{-1}\ell \Rightarrow y = x^{-1}\ell - a$, where a is the associator of the ordered triple (x^{-1}, x, y) and x^{-1} is a left inverse of x. Since $x^{-1}\ell \in L$ and $a \in L$ then $y = (x^{-1}\ell - a) \in L$ is a contradiction. So, $x \cdot y \in S \setminus L$.

2° If A(S) is contained in L and $(L,+)$ is a subgroup of $(S,+)$, then L is an S-subgroup and from here S is a local near-ring. Supose that for some $\ell \in L$ and some $s \in S$, $s\ell \notin L$. Then for some $x \in S \setminus L$, $x(s\ell) = 1$. Hence $(xs)\ell + a = 1$ and $(xs)\ell = 1 - a$. Hence since there exists a left inverse of xs, say $(xs)^{-1}$, it follows $(xs)^{-1}((xs)\ell) = (xs)^{-1}(1-a)$ and $\ell + a_1 = (xs)^{-1}(1-a)$, where a, a_1 are the associators of ordered triples (x, s, ℓ) and $((xs)^{-1}, xs, \ell)$ respectively. Since $a \in L$, $(xs)^{-1}$, $(1-a)$, $(xs)^{-1}(1-a) \in U$ then $\ell + a_1 \in S \setminus L$ is a contradiction to $\ell + a_1 \in L$. Thus, $s\ell \in L$ and the proof is finished.

THEOREM 2. Let S be a local (nonassociative) near-ring. Then, $(L,+)$ is the unique maximal S-subgroup.

PROOF. If N is an arbitrary proper S-subgroup of S then $N \subseteq L$, because no element of N has a left inverse. Conversely, if $N \supset L$, i.e. if for some $x \in N$, $x \notin L$, then there exists some y such that $yx = 1 \in N$ and N would not be a proper S-subgroup. This theorem is given by Maxson for a local associative near-ring (T.2.2. [1]).

LEMMA 1. If S is, in general a nonassociative, local near-ring and L contains the associator A(S) of S, then the elements of L do not have right inverses.

PROOF. Suppose that there exists some ℓ of L with a right inverse ℓ' in L then $\ell\ell' = 1 \in U$ contradicts to $\ell\ell' \in L$. Hence the elements of L do not have right inverse in L. Let some element $\ell \in L$ has a right inverse $s \in U$, i. e. $\ell s = 1$. As $s\ell \in L$, then $1 - s\ell \notin L$ and there exists $x \in U$ such that $x(1-s\ell) = 1$. As $(1-s\ell)s = s - (s\ell)s = a$ then $s = (x(1-s\ell))s$ and $x((1-s\ell)s) + a_1 = x(s - s(\ell s) + a) + a_1 = xa + a_1 \in L$, where a, a_1 are the associators of the ordered triples (s,ℓ,s) and $(s,(1-s\ell),s)$ respectively. This contradiction establishes the lemma.

A nonzero element a of S is called a unit if $st = ts = 1$, for some $t \in S$.

Denote by A the subset of all nonunits of S.

COROLLARY. If S is, in general, a nonassociative, local near-ring and if every element of U has a right inverse, then $L_d \supseteq A = L$, where L_d is the subset of all elements of S without right inverses.

THEOREM 3. Let every element of U has a right inverse, then S is a local (nonassociative) near-ring if and only if the subset A is a left S-subgroup.

PROOF. It is clear that $A = L$, if every element of U has a right inverse. If A is the S-subgroup then it contains L. If there exists $\ell \notin L$ such that $\ell \in A$, then for some k, $k\ell = 1 \in A$. But this is imposible. Therefore, $A = L$.

The left associator ideal A of S is the minimal left ideal of S generated by associator A(S) of S.

A near-ring $(S,+,\cdot)$ is called a skew near-field if and only if $(S\setminus\{0\}, \cdot)$ is a group.

THEOREM 4. Let S be a local near-ring, A_ℓ the left associator ideal of S and $A(S)S = \{as / a \in A(S); s \in S\} \subseteq A(S)$. If $A_\ell \neq S$ then L is the maximal right S-subgroup. Moreover, if the distributor ideal D of S is not equal to S then L is an ideal of S and S/L is a skew near-fild.

PROOF. Let S be a local (nonassociative) near-ring and A_ℓ left associator ideal of it. Since $as \in A(S)$, $(a \in A(S), s \in S)$, then $\left[s(-\bar{s}+a+\bar{s})\right]s_1 - s\left[(-\bar{s}+a+\bar{s})s_1\right] = \bar{a}$ and from here $\left[s(-\bar{s}+a+\bar{s})\right]s_1 = \bar{a} + s\left[(-\bar{s}+a+\bar{s})s_1\right] = \bar{a} + s\left[-as_1+\bar{s}s_1\right] \in A(S)$, for all $a \in A(S)$ and all $s, s_1 \in S$. So, A_ℓ is a two-sided ideal of S. If $A_\ell \neq S$ theh A_ℓ is the left proper S-subgroup and by the Th. 2. $A_\ell \subseteq L$. Let $h : A_\ell \longrightarrow L$ be the inclusion map. Then h induces an S-epimorphism $h : S/A_\ell \longrightarrow S/L$ and hence $S/A_\ell/\ker h \cong S/L$. However, S/A_ℓ is associative. Since $(S/L\setminus\{\bar{0}\}, \cdot) \cong (U,\cdot)$ is associative. Since $(U,\cdot)$ is by Th. 1. a groupoid, then $(S/L\setminus\{\bar{0}\}, \cdot)$ is a groupoid. Since $L \supseteq A_\ell$ then the elements of L do not have right inverses (L. 1.).

Suppose now $s \notin L$ and let s' be a left inverse of s. Since we have proved that $s' \notin L$, then there exists $s'' \in U$ such that $s''s' = 1$. Then $s'' = s$ and consequently $s's = s''s' = 1 = ss'$ which implies s is an unit in S. From here it follows that $L_d = L = A$. Hence $\ell s \in L$, for all $\ell \in L$ and all $s \in S$; otherwise if $\ell s \notin L$ then $(\ell s)s'' - (ss'') = a$ and $(\ell s)s'' - \ell = a \Longrightarrow (\ell s)s'' = a + \ell$, where s'' is a right inverse of s. Since $(\ell s)s'' \in U$ and $a + \ell \in L$ is

a contradiction, this establishes the first part of the theorem. Because, if H is any proper right S-subgroup then $H \subseteq L$.

Since $(U,\cdot)$ is the group, $(S/L\setminus\{0\}, \cdot) \cong (U,\cdot)$, $(L,+)$ is the normal subgroup and a proper ideal of S, then S/L is a skew near-field. Really, since C, D, G an ascending central series of the group (S,+) then (S,+) is a nilpotent group and by Th.6.4.1o. [4] (L,+) is a normal subgroup of S. So, (L,+) is a member of some normal central series of (S,+) and there exist a normal subgroup K of (S,+) such that $K \supseteq L$. If $K \subset S$ and if we denote by $\overline{L}$ the normal subgroup generated by L, then $K \supseteq \overline{L}$. It follows $\overline{L} \neq S$. If K=S, then $\overline{L} = L \neq S$. Otherwise, if there exists $\ell \in \overline{L}$ and $\ell \notin L$, then $s = 1 \in \overline{L}$, for some $s \in S$. This contradiction establishes the second part of the theorem (where C the commutor of (S,+)).

THEOREM 5. Let S be a local near-ring in which each element of U has a right inverse element, then L is the maximal right S-subgroup if and only if L contains the associator A(S).

PROOF. 1° If each element of U has a right inverse and the right relative associator A_r of L in S is contained in L, then ks belongs to L, for all $k \in L$ and all $s \in U$. Otherwise, $ks \in L$, i.e. $(ks)x = 1$, for some $x \in U$. Hence, $k(sx) - a = 1$ and $k(sx) = 1 + a$, where a is the associator of the ordered triple (k,s,x). As there exists a right inverse of sx, say $(sx)^{-1}$, then $(k(sx))(sx)^{-1} = (1-a)(sx)^{-1}$ and from here $k - a_1 = (1-a)\cdot(sx)^{-1}$, where a_1 is the associator of ordered triple $(k, sx, (sx)^{-1})$. Since $k - a_1 \in L$ then $(1-a)(sx)^{-1} \in L$. But, by Th.1., $(1-a)(sx)^{-1} \in U$. This contradiction proves the first part of the Theorem. Really, if K any proper right S-subgroup then $K \subseteq L$. Otherwise, if there exists $k \notin L$ such that $k \in K$ then $ky = 1$, for some $y \in U$. It means that $1 \in K$ and $K = S$ is a contradiction.

2° Conversely, suppose that L is a proper maximal right S-subgroup, i.e. $ks \in L$, for all $k \in L$ and all $s \in S$. Then, $(ks)x - k(sx) = a \in L$, for all $k \in L$ and all $s, x \in S$.

LEMMA 2. Every proper S-subgroup of a unitary near-ring S is contained in a maximal S-subgroup (See [3]).

THEOREM 6. Let S be a (nohassociative) near-ring in which A(S) is contained in L. Then, S is local if and only if S contains a unique left maximal S-subgroup (See Th. 2.8.[1]).

PROOF. 1° If S is local, then S containes a unique maximal S-subgroup (Th.2.).

2° Conversely, if $A(S) \subseteq L$, then S is local, i.e. L = M. Really, $Sk, k \in L$, is a proper S-subgroup. But, $x(sk) - (xs)k = a \in A(S)$, for all $x, s \in S$. Hence $x(sk) = a + (xs)k \in M$. So, L = M, where M is a unique maximal S-subgroup (See the proof of Th. 2.8.[1]).

An element x of a (nonassociative) near-ring S is called right quasiregular if and only if $y(1-x) = 1$, for some $y \in S$. A left S-subgroup N is quasiregular if and only if each

LEMMA 3. If S is, in general a nonassociative, local near-

-ring, then L is quasiregular (See L.2.9.[1]).

The proof is the same as one of L.2.9.[1].

THEOREM 7. If the radical of S is J(S) and $J(S) \neq S$ then S is local (nonassociative) near-ring if and only if $L = J(S)$ (See Th.2.1o.[1]).

The proof is the same as one of Th. 2.1o.[1].

If S is a local associative near-ring, then it is completely primary. If S is a ring, then the converse is true 1 . That this is not the case for a near-ring, in general, is shown by the next examples.

EXAMPLE 1. Let S be the left nonassociative near-ring given by the following operation tables:

Table 1.

+	o	a	b	c	d	e
o	o	a	b	c	d	e
a	o	a	b	c	d	e
b	b	d	o	e	a	c
c	c	e	d	o	b	a
d	d	b	c	a	e	o
e	e	c	a	b	o	d

Table 2.

•	o	a	b	c	d	e
o	o	o	o	o	o	o
a	o	a	b	c	d	e
b	o	c	a	b	d	e
c	o	b	c	a	e	d
d	o	o	o	o	o	o
e	o	o	o	o	o	o

The radical J(S) of S is $\{o, d, e\}$, $L = \{o, d, e\}$, $A = \{o, d, e\}$. So, S is a local nonassociative near-ring.

EXAMPLE 2. $(S, +, \cdot_1)$, where the operations + and $\cdot_1$ are defined by tables 1. and 3. respectively.

Table 3.

$\cdot_1$	o	a	b	c	d	e
o	o	o	o	o	o	o
a	o	a	b	c	d	e
b	o	a	b	c	d	e

Table 3.(continuation)

$\cdot_1$	o	a	b	c	d	e
c	o	b	a	c	e	d
d	o	o	o	o	o	o
e	o	o	o	o	o	o

The radical of S is $\{o, d, e\}$, but $L = \{o, c, d, e\}$. So, $L \neq J(S)$. S is not a local near-ring.

EXAMPLE 3. Let $(I_p, +_p, \cdot_p)$ be the ring of integes modulo p , where p is prime. Then $S = (I_p \times I_p, +, \otimes)$ is an affine near-ring , where $+, \otimes$ are the operations : componet-wise addition and affine multiplication : $(x,y) \otimes (x_1, y_1) = (x \cdot x_1 , xy_1 + y)$, $(x,y), (x_1, y_1) \in I_p \times I_p$ respectively. Also, the radical $J(S) = L = \{o\} \times I_p$. Hence, S is a local near-ring. Since $J(S) \neq S$ and $J(S) = L$ then Th. 7. holds. However, in non-associative near-ring $T = (I_p \times I_p, +, \otimes_1)$, (where $\otimes_1$: $(x,y) \otimes_1 (x_1, y_1) = (x \cdot x_1 , (x \cdot y_1) \cdot y)$, $(x,y), (x_1, y_1) \in I_p \times I_p$, $L = \{o\} \times I_p$, $J(T) = \{(o,o)\}$ and $J(T) \neq L$. Hence, Th.7. can not be applied to this example, because T has not right identity. If T-subgroups $I_p \times \{o\}$ and $\{o\} \times I_p$ of $(T,+)$ do not considered as proper maximal T-subgroups then $J(T) = \{o\} \times I_p$ and this case can be included in above conception.

R E F E R E N C E S

1. C. J. Maxson : On Local Near-Ring , Math. Zeitscher. 1o6, 197-2o5(1968).

2. J. Beidleman: Quasi-regularity in Near-Rings, Math. Z. 89, 224-229(1965).

3. " A Radical for Near-Ring Modules, Mich.Math. J.12, 377-383(1965).

4. Scott William R. Group Theory, New Jersey Prentice-Hall, 1964.

5. V. Vuković : (Nonassociative) Near-Rings, Glasnik Matematički, Vol. 2o(4o)(1985), 279-287.