INSTITUTE OF MATHEMATICS

UNIVERSITY OF NOVI SAD

PROCEEDINGS OF THE CONFERENCE "ALGEBRA AND LOGIC"

SARAJEVO

1987.

NOVI SAD

1989

PROCEEDINGS OF THE CONFERENCE
"ALGEBRA AND LOGIC", SARAJEVO 1987
published by
INSTITUTE OF MATHEMATICS
FACULTY OF SCIENCE
UNIVERSITY OF NOVI SAD
dr ILIJE ĐURIČIĆA 4
21000 NOVI SAD, YUGOSLAVIA

Editor:
Siniša Crvenković

Editorial Board:
Koriolan Gilezan
Milan Grulović
Svetozar Milić
Đura Paunić
Zoran Stojaković
Branimir Šešelja
Janez Usan
Gradimir Vojvodić

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

PREFACE

The Sixth Yugoslav Algebraic Coference "Algebra and Logic" organized by the Faculty of Science, Sarajevo, was held in Sarajevo, June 18-20, 1987.

The Conference was dedicated to Professor Đuro Kurepa on the occasion of his eightieth anniversary.

This book containes most of the papers presented during the Conference.

CONTENTS

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

CONGRUENCES OVER COMPLETELY SEMISIMPLE SEMIGROUPS

Branka P. Alimpić

Abstract. In this paper congruences of a regular semigroup over completely semisimple semigroups are considered. For any interval $[\rho_T, \rho^T]$ the set of all congruences over completely semisimple semigroups of $[\rho_T, \rho^T]$ is either empty or is an ideal of $[\rho_T, \rho^T]$. For any interval $[\rho_K, \rho^K]$ a dual statement holds.

Let $\mathcal{K}$ be a class of semigroups. A congruence ρ on a regular semigroup S is over $\mathcal{K}$ if all idempotent ρ-classes of S belong to $\mathcal{K}$ [6].

A congruence ρ on a semigroup S is a band congruence if S/ρ is a band. A semigroup S is a band of semigroups belonging to a class $\mathcal{K}$ of semigroups if S has a band congruence all of whose classes belong to $\mathcal{K}$.

If S is a rectangular band $I \times \Lambda$ of semigroups $S_{i\mu}$, $i \in I$, $\mu \in \Lambda$, then $S_{i\lambda} S_{j\mu} \subseteq S_{i\mu}$, for all $i, j \in I$, $\lambda, \mu \in \Lambda$.

A semigroup all of whose principal factors are completely 0-simple or completely simple is completely semisimple [4].

For undefined notations or terminology see [2], [9].

If S is a semigroup, and $X \subseteq S$, let E(X) denote the set of all idempotents of X. The relation $\leq$ defined on a regular semigroup S by

$$a \leq b \Leftrightarrow (\exists\, e, f \in E(S))\, a = be = fb$$

is the natural partial order of S [5]. For any $e, f \in E(S)$, $e \leq f \iff e = fe = ef$.

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

LEMMA 5. Let S be a band B of completely semisimple semigroups S_α, $\alpha \in B$. Then S is completely semisimple.

Proof. By Result 1, semigroups S_α are regular, so S is a regular semigroup.

Let ρ be a band congruence on S over completely semisimple semigroups, such that $S/\rho = B$. The band B is a semilattice Y of rectangular bands B_β, $\beta \in Y$. Let η be a semilattice congruence on B such that $B/\eta = Y$. For any $e,f \in E(S)$ we have $e \mathcal{D} f \Rightarrow (e\rho)\mathcal{D}(f\rho) \Rightarrow (e\rho)\eta(f\rho)$.

Hence e and f belong to the same rectangular band B of completely semisimple semigroups. According to Lemma 3, we obtain $e \mathcal{D} f \wedge e \leq f \Rightarrow e = f$, and by Result 1 it follows that S is a completely semisimple semigroup.

Let S be a regular semigroup. 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, $\mathrm{tr}\rho = \rho|_{E(S)}$ [1]. Let Con S be the congruence lattice of S, K and T equivalences on Con S defined by

$$\rho K \xi \Leftrightarrow \ker\rho = \ker\xi \qquad \text{and} \qquad \rho T \xi \Leftrightarrow \mathrm{tr}\rho = \mathrm{tr}\xi .$$

It is known that K-classes $[\rho_K, \rho^K]$ and T-classes $[\rho_T, \rho^T]$ are intervals on Con S ([7], [10]).

Let CS(S) denote the set of all congruences on a regular semigroup S over completely semisimple semigroups. Using the Result 1, we have immediately the following characterization of the set CS(S).

LEMMA 6. For a regular semigroup S and $\rho \in$ Con S, $\rho \in$ CS(S) if and only if for any $e,f \in E(S)$, $e\rho$ is a regular subsemigroup of S and $e(\rho \wedge \mathcal{D}^{e\rho} \wedge \leq)f \Rightarrow e = f$.

THEOREM 1. Let ρ and ρ' be congruences on a regular semigroup S. If $\rho' \leq \rho$ and $\rho' T \rho$, then $\rho \in CS(S) \Rightarrow \rho' \in CS(S)$.

Proof. For any idempotent $e \in E(S)$, $T = e\rho$ is a completely semisimple subsemigroup of S. Since $\mathrm{tr}\rho = \mathrm{tr}\rho'$, the relation $\rho' \wedge (T \times T)$ is a group congruence on T, so $e\rho'$ is a regular subsemigroup of T. Now by Lemma 1, the semigroup $e\rho'$ is completely semisimple. Hence, the congruence ρ' is over completely semisimple semigroups.

COROLLARY 2. For any interval $[\rho_T, \rho^T]$ the set $CS(S) \cap [\rho_T, \rho^T]$ is either empty or is an ideal of $[\rho_T, \rho^T]$.

COROLLARY 3. If S is a completely semisimple semigroup, every group congruence ρ on S is over completely semisimple semigroups.

The following statement is a dual of Theorem 1.

THEOREM 2. Let ρ and ρ' be congruences on a regular semigroup S. If $\rho \subseteq \rho'$ and $\rho \mathcal{K} \rho'$, then $\rho \in CS(S) \Rightarrow \rho' \in CS(S)$.
Proof. For any idempotent $e \in E(S)$, $T = e\rho'$ is a subsemigroup of S. Since $\ker\rho = \ker\rho'$, the relation $\rho \cap (T \times T)$ is a band congruence on T, so by hypothesis T is a band of completely semisimple semigroups. Now by Lemma 5 the semigroup $e\rho'$ is completely semisimple.
Hence, the congruence ρ' is over completely semigroups.

COROLLARY 4. For any interval $[\rho_K, \rho^K]$ the set $CS(S) \cap [\rho_K, \rho^K]$ is either empty or is an dual ideal of $[\rho_K, \rho^K]$.

Next we consider completely semisimple semigroups satisfying $\mathcal{D}$-majorization. A regular semigroup S satisfies $\mathcal{D}$-majorization if for any $\mathcal{J}$-class D and any idempotent $e \in E(S)$ the set $D \cap \{f \in E(S) \mid f \leq e\}$ is either empty or has a greatest element [8].

RESULT 3. [8] The following conditions on a regular semigroup S are equivalent:
(i) For any $e, f, g \in E(S)$, $e \geq f, e \geq g$ and $f \mathcal{D} g$ imply $f = g$.
(ii) The semigroup S is completely semisimple and satisfy $\mathcal{D}$-majorization.

The following two statements are corresponding to Lemma 1 and Lemma 3, respectively.

LEMMA 7. Let S be a completely semisimple semigroup satisfying $\mathcal{D}$-majorization and T a regular subsemigroup of S. Then T is a completely semisimple semigroup satisfying $\mathcal{D}$-majorization.

LEMMA 8. Let S be a rectangular band of completely semisimple semigroups $S_{i\mu}$ satisfying $\mathcal{J}$-majorization. Then S is a completely semisimple semigroup satisfying $\mathcal{J}$-majorization.

Proof. Since the semigroups $S_{i\mu}$ are regular, the semigroup S is regular. For any $e,f,g \in E(S)$ we have

$e \geq f, e \geq g, f \mathcal{J} g \Rightarrow (\exists S_{i\mu})(e \geq f, e \geq g, f \mathcal{J}^{i\mu} g)$ (by Lemma 2)

$\Rightarrow e=f$ (by hypothesis and Result 3).

Hence, again by Result 3, S is a completely semisimple semigroup satisfying $\mathcal{J}$-majorization.

Let CSD(S) denote the set of all congruences on a regular semigroup S over completely semisimple semigroups satisfying $\mathcal{D}$-majorization. Using the Result 3, we have immediately the following characterization of the set CSD(S):

LEMMA 9. For a regular semigroup S and $\rho \in \mathrm{Con}\, S$, $\rho \in \mathrm{CSD}(S)$ if and only if for any $e,f,g \in E(S)$ $e\rho$ is a regular subsemigroup of S, and $(e(\geq \cap \rho)f, e(\geq \cap \rho)g, f \mathcal{J}^{e\rho} g) \Rightarrow f=g$.

Using the Lemma 7 we obtain the following result for CSD(S) corresponding to the result for CS(S) given in Theorem 1.

THEOREM 3. Let ρ and ρ' be congruences on a regular semigroup S. If $\rho' \subseteq \rho$ and $\rho' \mathrm{T} \rho$, then $\rho \in \mathrm{CSD}(S) \Rightarrow \rho' \in \mathrm{CSD}(S)$.

Remark. The following example shows that the analogue of the Lemma 5 for completely semisimple semigroups satisfying $\mathcal{J}$-majorization does not hold in general.

Example. Let $S=\{e,a,b\}$ be a semigroup with Cayley table:

·	e	a	b
e	e	a	b
a	a	a	b
b	b	a	b

S is a semilattice of $\{e\}$ and the right-zero semigroup $\{a,b\}$, but $e \geq a$, $e \geq b$, $a \mathcal{J} b$ and $a \neq b$.

REFERENCES

1. R.Feigenbaum, Regular semigroup congruences, Semigroup Forum 17(1979),373-377.

2. J.M.Howie, An Introduction to Semigroup Theory, Academic Press, London 1976.

3. J.E.Mills, Matrices of bisimple regular semigroups, Semigroup Forum 26(1983), 117-123.

4. W.D.Munn, Semigroups satisfying minimal conditions, Proc. Glasgow Math.Assoc. 3(1957), 145-152.

5. K.S.S.Nambooripad, The natural partial order on a regular semigroup, Proc. Edinburgh Math. Soc. 23(1980),249-260.

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. 119(1985), 191-214.

8. M.Petrich, Regular semigroups satisfying certain conditions on idempotents and ideals, Trans.Amer.Math.Soc. 170(1972), 245-267.

9. M.Petrich, Structure of regular semigroups, Montpellier, 1977.

10. N.R.Reilly and K.E.Scheiblich, Congruences on regular semigroups, Pac.J.Math. 23(1967),349-360.

Branka P.Alimpić
Prirodno matematički fakultet
Studentski trg 16
YU-11000 Beograd

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

NIL-EXTENSIONS OF A COMPLETELY REGULAR SEMIGROUP

Stojan Bogdanović

Abstract. In this paper we describe a nil-extension of a completely regular semigroup (Theorem 1.). By Theorem 2. we characterized a retract extension of a completely regular semigroup by a nil-semigroup . At the end, by Theorem 3. a characterization of an n-inflation of a completely 0-simple semigroup is given.

A semigroup S is Π-regular if for every $a \in S$ there exists $m \in Z^+$ such that $a^m \in a^m S a^m$. Let us denote by $Reg(S)$ ($Gr(S)$, $E(S)$) the set of all regular (completely regular, idempotent) elements of a semigroup S . S is a GV-semigroup (semigroup of Galbiati-Veronesi) if S is Π-regular and $Reg(S) = Gr(S)$, [1,6] . A semigroup S is a retract extension of a semigroup T if S is an ideal extension of T and there exists a homomorphism φ of S onto T such that $\varphi(t) = t$ for all $t \in T$.

For undefined notions and notations we refer to [1] and [3] .

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

PROPOSITION 1. *The following conditions are equivalent on a semigroup* S:

(i) $\langle E\rangle$ *is a regular subsemigroup of* S;

(ii) $\mathrm{Reg}(S)$ *is a subsemigroup of* S;

(iii) $V(E) = E^2$;

(iv) $(\forall n \in Z^+)\ V(E^n) = E^{n+1}$.

Proof. (i)$\Rightarrow$(ii). Let $a,b \in \mathrm{Reg}(S)$. Then $a = axa$ and $b = byb$ for some $x,y \in S$. By the hypothesis there is a $z \in \langle E\rangle$ such that

$$(xa)(by) = (xa)(by)z(xa)(by) \ .$$

Thus

$$ab = axabyb = a(xabyzxaby)b = (axa)(byzxa)(byb)$$
$$= abyzxab \in \mathrm{Reg}(S) \ .$$

(ii)$\Rightarrow$(iii) and (ii)$\Rightarrow$(iv) follows by Theorem [7], (iv)$\Rightarrow$(ii) follows immediately, (iii)$\Rightarrow$(ii) this is as (i)$\Rightarrow$(ii), at the end (ii)$\Rightarrow$(i) follows by Corollary of Theorem [7] . □

COROLLARY 1. *The following conditions are equivalent on a semigroup* S:

(i) S *is* $\mathcal{J}$*-regular and* $\mathrm{Reg}^2(S) = \mathrm{Reg}(S)$;

(ii) S *is* $\mathcal{J}$*-regular and* $\langle E(S)\rangle$ *is a regular semigroup*;

(iii) $(\forall a,b \in S)(\exists m,n \in Z^+)\ a^m b^n \in a^m b^n S a^m b^n$.

Proof. By Proposition 1. □

THEOREM 1. *A semigroup* S *is a nil-extension of a completely regular semigroup if and only if for every* $a,b \in S$ *and* $x,y \in S^1$ *there exists* $m \in Z^+$ *such that*

(1) $$x(ab)^m y \in x(ab)^m yb S x(ab)^m y \ .$$

Proof. Let S be a nil-extension of a completely regular semigroup T . Then S is $\mathcal{J}$-regular . Assume $a \in \mathrm{Reg}(S)$. Then there exists $z \in S$ such that $a = a(za) \in T = \mathrm{Gr}(S)$. So

$\mathrm{Reg}(S) = \mathrm{Gr}(S)$. Therefore, S is a GV-semigroup . Now by Theorem X 1.1. [1] we have that S is a semilattice Y of completely archimedean semigroups S_α , $\alpha \in Y$. Assume that S_α is a nil-extension of a completely simple semigroup K_α , $\alpha \in Y$. For any $a \in S_\alpha$, $b \in S_\beta$, $x \in S_\mu$, $y \in S_\delta$ we have that $(ab)^m, (ba)^m \in K_{\alpha\beta}$ for some $m \in Z^+$. Since T is an ideal of S we obtain that $x(ab)^m y, (ba)^m yx \in K_{\alpha\beta\gamma\delta}$. Since $K_{\alpha\beta\gamma\delta}$ is a completely simple semigroup we have that

$$x(ab)^m y \in x(ab)^m y(ba)^m yx K_{\alpha\beta\gamma\delta} x(ab)^m y \subseteq x(ab)^m ybSx(ab)^m y .$$

If $x = y = 1$, then by Theorem VI 2.2.1. 1 we have that

$$(ab)^m \in (ab)^m (ba)^m K_{\alpha\beta} (ab)^m \subseteq (ab)^m bS(ab)^m .$$

If $x = 1$ or $y = 1$ the proof is similar to the above.

Conversely, from (1) we have that for every $a, b \in S$ there exists $m \in Z^+$ such that

$$(ab)^{m+1} \in (ab)^m abbS(ab)^m ab = (ab)^{m+1} bS(ab)^{m+1} .$$

Assume $a \in \mathrm{Reg}(S)$. Then there exists $u \in S$ such that $a = aua$. So

$$a = aua = a(ua)^{m+1} \in a(ua)^{m+1} aS(ua)^{m+1} = a^2 Sa .$$

Hence, $\mathrm{Reg}(S) = \mathrm{Gr}(S)$.

Let $a \in \mathrm{Reg}(S)$ and $y \in S$. Then by (1) we have that

$$\begin{aligned} ay &= auay \text{ , for some } u \in S \\ &= a(ua)^m y \text{ , for every } m \in Z^+ \\ &\quad a(ua)^m yaS(ua)^m y \text{ , for some } m \in Z^+ \\ &= auayaSuay = ayaSuay \in aySay . \end{aligned}$$

From this it follows that $\mathrm{Reg}^2(S) = \mathrm{Reg}(S)$, and also that $\mathrm{Reg}(S)$ is a right ideal of S . Similarly it can be proved that $ya \in yaSya$. Hence $\mathrm{Reg}(S) = \mathrm{Gr}(S)$ is an ideal of S , and since S is $\mathcal{J}$-regular we have that S is a nil-extension

of a completely regular semigroup . □

THEOREM 2. *A semigroup S is a retract extension of a completely regular semigroup by a nil-semigroup if and only if for every* $a,b,c \in S$ *there exists* $m \in Z^+$ *such that*

(2) $(ab)^m c \in e(ab)^m cbS(ab)^m cf$ *and* $c(ab)^m \in c(ab)^m Sc(ab)^m$

where $a^k \in G_e$ *and* $c^r \in G_f$ *for some* $k,r \in Z^+$.

Proof. Let S be a retract extension of a union of groups by a nil-semigroup , and let $a,b,c \in S$. Then by Theorem 1. we have that the second condition (6) holds, and that there exists $m \in Z^+$ and $x \in S$ such that

(3) $(ab)^m c = (ab)^m cbx(ab)^m c$.

Also there is a retraction $\varphi : S \to T = Reg(S) = Gr(S)$. So by (3) we have

(4) $(ab)^m c = \varphi(a)\varphi(b)\varphi((ab)^{m-1}cbx(ab)^m)\varphi(c)$.

Now, since $\varphi(a) \in G_h$ and $\varphi(c) \in G_g$, and $a^k \in G_e$, $c^r \in G_f$ for some $h,g,e,f \in E$ and $k,r \in Z^+$, we then have that $a^k = \varphi(a^k) \in G_h$ and $c^r = \varphi(c^r) \in G_g$. So $h = e$ and $g = f$, i.e.

$$\varphi(a) = e\varphi(a) \quad \text{and} \quad \varphi(c) = \varphi(c)f .$$

From this and by (4) it follows that

$$\begin{aligned}(ab)^m c &= e\varphi(a)\varphi(b)\varphi((ab)^{m-1}cbx(ab)^m)\varphi(c)f \\ &= \varphi(e(ab)^m cbx(ab)^m cf) \\ &= e(ab)^m cbx(ab)^m cf \in e(ab)^m cbS(ab)^m cf .\end{aligned}$$

Hence, the first condition (2) also holds .

Conversely, by the first condition (2) we have

(5) $(ab)^m c = e(ab)^m c = (ab)^m cf$

and so

$$(ab)^m c \in e(ab)^m cbS(ab)^m cf = (ab)^m cbS(ab)^m c .$$

Now by Theorem 1. we have that S is a nil-extension of a union of groups T. Since S is a $\mathcal{V}$-regular semigroup and $Gr(S) = Reg(S) = T$ we have that S is a GV-semigroup. From this and from Theorem X 1.1. [1] it follows that S is a semilattice Y of semigroups S_α, which are nil-extensions of completely simple semigroups P_α, $\alpha \in Y$. Define a mapping

$$\varphi: S \longrightarrow T = \bigcup_{\alpha \in Y} P_\alpha$$

by:

$$\varphi|_{S_\alpha} = \varphi_\alpha: S_\alpha \longrightarrow P_\alpha$$

$$\varphi_\alpha(x_\alpha) = x_\alpha e_\alpha \quad \text{if} \quad x^m \in G_e \quad \text{for some} \quad m \in Z^+ .$$

Then φ_α maps S_α onto P_α and $\varphi_\alpha(x_\alpha) = x_\alpha$ for every $x_\alpha \in P_\alpha$. For $x_\alpha \in S_\alpha$ and $x_\beta \in S_\beta$ there exists $k \in Z^+$ such that $(x_\alpha x_\beta)^k \in G_{e_{\alpha\beta}}$. So

$$\begin{aligned}
\varphi_\alpha(x_\alpha)\varphi_\beta(x_\beta) &= x_\alpha e_\alpha x_\beta e_\beta = e_\alpha x_\alpha x_\beta e_\beta \quad (\text{Theorem I 4.3. [1]}) \\
&= e_\alpha^m x_\alpha x_\beta e_{\alpha\beta} e_\beta, \quad ((5)) \\
&= e_\alpha x_\alpha x_\beta e_{\alpha\beta} e_\beta \\
&= e_\alpha (x_\alpha x_\beta e_{\alpha\beta})^2 (x_\alpha x_\beta e_{\alpha\beta})^{-1} e_\beta, \quad x_\alpha x_\beta e_{\alpha\beta} \in G_{e_{\alpha\beta}} \\
&= (x_\alpha x_\beta e_{\alpha\beta})^2 (x_\alpha x_\beta e_{\alpha\beta})^{-1} e_\beta, \quad ((5)) \\
&= x_\alpha x_\beta e_{\alpha\beta} e_\beta \\
&= e_{\alpha\beta} x_\alpha x_\beta e_\beta, \quad (\text{Theorem I 4.3. [1]}) \\
&= (e_{\alpha\beta} x_\alpha)^{-1} (e_{\alpha\beta} x_\alpha)(e_{\alpha\beta} x_\alpha) x_\beta e_\beta \\
&= (e_{\alpha\beta} x_\alpha)^{-1} e_{\alpha\beta} x_\alpha e_{\alpha\beta} x_\alpha x_\beta, \quad ((5)) \\
&= e_{\alpha\beta} x_\alpha x_\beta = x_\alpha x_\beta e_{\alpha\beta}, \quad (\text{Theorem I 4.3. [1]}) \\
&= \varphi_{\alpha\beta}(x_\alpha x_\beta) .
\end{aligned}$$

Hence, φ is a homomorphism of S onto T and $\varphi(x) = x$ for all $x \in T$. Therefore, φ is a retraction of S onto T. □

A semigroup S is an n-<u>inflation</u> of a semigroup T if $S^{n+1} \subseteq T$, where T is an ideal of S and there exist a retraction φ of S onto T, [2]. For 1- and 2-inflation see [3] and [5].

THEOREM 3. A semigroup S is an n-inflation of a completely 0-simple semigroup if and only if the following conditions hold:

(a) S^{n+1} is a completely 0-simple semigroup;

(b) $a_1a_2\dots a_{n+1} \neq 0$, ua_1, $a_{n+1}v \in E(S)$

$$a_1a_2\dots a_{n+1} = a_1(ua_1)a_2\dots a_{n+1} = a_1a_2\dots a_n(a_{n+1}v)a_{n+1}.$$

Proof. Let S be an n-inflation of a completely 0-simple semigroup. Then by the definition of n-inflation we have that S^{n+1} is a completely 0-simple semigroup. Let φ be a retraction from S onto S^{n+1}.

Let $a_1a_2\dots a_{n+1} \neq 0$ and $ua_1 \in E^*(S)$. Then

$$ua_1 = \varphi(ua_1) = \varphi(u)\varphi(a_1) \in E^*(S^2) \tag{6}$$

and

$$\begin{aligned}\varphi(a_1)\varphi(u)\varphi(a_1) &= \varphi(a_1)[\varphi(u)\varphi(a_1)]^k \quad \text{for every } k \in Z^+\\ &= \varphi(a_1(ua_1)^n) = a_1(ua_1)^n\\ &= a_1(ua_1) \neq 0\end{aligned}$$

since $0 \neq ua_1 = u(a_1ua_1)$. Since S^{n+1} is a completely 0-simple semigroup we then have that $\varphi(a_1) \in G_e$ for some $e \in E(S)$ and $\varphi(a_1) \neq 0$, whence by Lemma [4] we have that $\varphi(a_1)\varphi(u)\varphi(a_1) \in G_e$ (Lemma [4]). Now

$$\begin{aligned}[e\varphi(u)\varphi(a_1)]^2 &= e\varphi(u)\varphi(a_1)e\varphi(u)\varphi(a_1)\\ &= e\varphi(u)\varphi(a_1)\varphi(u)\varphi(a_1), \quad \text{since } \varphi(a_1) \in G_e\\ &= e\varphi(u)\varphi(a_1), \quad \text{by (6)}.\end{aligned}$$

Thus, $e\varphi(u)\varphi(a_1) = e$, so

$$\varphi(a_1)\varphi(u)\varphi(a_1) = \varphi(a_1). \tag{7}$$

Furthermore,

$$a_1a_2\dots a_{n+1} = \varphi(a_1a_2\dots a_{n+1}) = \varphi(a_1)\varphi(a_2)\dots\varphi(a_{n+1})$$

$$= \varphi(a_1)\varphi(u)\varphi(a_1)\varphi(a_2)\dots\varphi(a_{n+1}) \text{ , by (7)}$$
$$= \varphi(a_1 u a_1 a_2 \dots a_{n+1})$$
$$= a_1(ua_1)a_2\dots a_{n+1} .$$

The second identity from (b) it can be proved in a similar way .

Conversely, let a be nonzero element of S . Assume that $ax_2\dots x_{n+1} \neq 0$. Then there exists $y \in S^{n+1}$ such that

(8) $$ax_2\dots x_{n+1} = ax_2\dots x_{n+1} y a x_2 \dots x_{n+1} .$$

Let $z = x_2\dots x_{n+1} y$. Then

$$(az)^2 = azaz = ax_2\dots x_{n+1} y a x_2 \dots x_{n+1} y$$
$$= ax_2\dots x_{n+1} y = az .$$

If $aza = 0$, then $(aza)z = 0$, i.e. $az = 0$, and by (8) we have that $ax_2\dots x_{n+1} = 0$, which is not possible . Hence, $aza \neq 0$. Now $aza = (aza)w(aza)$ for some $w \in S^{n+1}$, $w \neq 0$.

Let us put that $u = waz$. Then

$$au = awaz = (aw)(az)az = a(waza)z = aw(azawaza)z$$
$$= (awaz)^2 az$$
$$= (awaz)^2 \text{ , since } az = (az)^2$$
$$= (au)^2 .$$

Similarly, $(ua)^2 = ua$. If $au = 0$, then $awaz = 0$, so $aza = 0$ which is not possible . Thus $au \in E^*(S)$, and similarly $ua \in E^*(S)$.

For an arbitrary $a \in S$ we define

$$\varphi(a) = \begin{cases} aua & \text{if } aS \neq 0, \text{ where } au, ua \in E^*(S) \\ 0 & \text{if } aS = 0 . \end{cases}$$

Fix $a \in S$ and assume that $au, ua, av, va \in E^*(S)$. Then by (b) , $av \neq 0$, $ua \in E^*(S)$ implies

$$av = av\dots av = a(ua)v\dots av = auav$$

and similarly $ua = u(ava)$. Now $ava = (aua)va = aua$. Hence ,

is a well defined function . From the preceding it is clear that with $ua, au \in E^*(S)$ it can be chose u from S^{n+1} . Hence, if $a \in S^{n+1}$, then $au, ua \in E^*(S)$, $u \in S^{n+1}$ implies $a = aua$ (see the proof of (7)). Therefore, φ maps S onto S^{n+1} , and $\varphi(t) = t$ for every $t \in S^{n+1}$. It remains to prove that φ is a homomorphism .

Let $a, b \in S$. If $aS \neq 0$, let $au, ua \in E^*(S)$, and if $bS \neq 0$, let $bv, vb \in E^*(S)$. Now we have the following cases

1) $aS = 0$, then

$$(ab) = \varphi(0) = 0 = 0\,\varphi(b) = \varphi(a)\,\varphi(b) .$$

2) $aS \neq 0$, $ab = 0$, then

$$\varphi(a)\varphi(b) = \begin{cases} (aua)(bvb), & bS \neq 0 \\ (aua)0 , & bS = 0 \end{cases} = \begin{cases} 0 \\ 0 \end{cases} = 0 = \varphi(0)$$

$$= \varphi(ab) .$$

3) $ab \neq 0$, $abS = 0$. Then $\varphi(ab) = 0$. If $\varphi(a)\varphi(b) \neq 0$, then $\varphi(a)\varphi(b) = (aua)(bvb) \neq 0$, which is not possible , since $abS = 0$. Thus $\varphi(a)\varphi(b) = 0 = \varphi(ab)$.

4) $abS \neq 0$, then $bS \neq 0$, and we have

$\varphi(ab) = abwab$, $abw, wab \in E^*(S)$, since $abS \neq 0$

$= abwabw...abwab$

$= abwabw...abwabvb$ (by the hypothesis)

$= (abwab)vb$

$= (abwab)vbvb...vb$

$= abvbvb...vb$ (by the hypothesis)

$= abvb$

$= a(bvbvb...vbvb)$

$= (aua)bvbvb...vbvb$ (by the hypothesis)

$= (aua)(bvb)$

$= \varphi(a)\varphi(b) .$

Therefore, φ is a homomorphism from S onto S^{n+1} .□

REFERENCES

1. S. Bogdanović , Semigroups with a system of subsemigroups , Inst. of Math. N. Sad 1985.

2. S. Bogdanović and S. Milić , Inflations of semigroups , Publ. Inst. Math. 41(55), 1987.

3. A.H. Clifford and G.B. Preston , The algebraic theory of semigroups , Vol. I , Amer. Math. Soc. 1977.

4. W.D. Munn , Pseudoinverses in semigroups , Proc. Camb. Phil.Soc. 57 (1961) , 247-250.

5. M. Petrich , Sur certaines classes de demi-groupes III , Acad. Roy. Belg. Cl. Sci. 53 (1967) , 60-73.

6. M.L. Veronesi , Sui semigruppi quasi fortemente regolari , Rivisita di Matematica dell' Universita di Parma (4) 10 (1984), 319-329.

7. D.G. Fitz-Gerald , On inverses of products of idempotents in regular semigroups , J. Australian Math. Soc. 13 (1972) , 335-337.

Faculty of Economics
18000 Niš
Trg JNA 11.
YUGOSLAVIA

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

ON SEMIGROUP-RELATION ALGEBRAS

S. Crvenković and R. Madarasz

Abstract. *In this paper we are presenting one of the possible semigroup approaches to relation algebras. To each semigroup S we correlate a relation algebra $\mathfrak{A}(S)$ so that S can be embedded into the semigroup reduct of $\mathfrak{A}(S)$. We examine some properties of this "construction $\mathfrak{A}$".*

1° Relation algebras

The fundamentals of the arithmetic of binary relations were made by C. S. Peirce, between 1870. and 1882. Peirce's work was continued and extended in a very thorough and systematic way by E. Schröder in the book "Algebra und Logic der Relative" (1895.). The first beginnings of the contemporary axiomatic development of the theory of binary relations were made by A. Tarski ([7]). Tarski gave, in [7], his system of axioms of the arithmetic of relations and proposed some, metatheoretical questions which determined the direction of further investigation. The original axioms of Tarski were not in the form of identities. The axiomatic system we use now (in which all the axioms are identities) was presented for the first time by L. Chin and A. Tarski [1].

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

DEFINITION 1.

Let $\mathfrak{A}=(A,+,\cdot,-,0,1,\circ,1',^{-1})$ be an algebra of type $(2,2,1,0,0,2,0,1)$. We call it *relation algebra* (RA) if it satisfies the following axioms :

(i) $(A,+,\cdot,-,0,1)$ is a Boolean algebra ;

(ii) $(A,\circ,1')$ is a monoid ;

(iii) $^{-1}$ is an involution of the semigroup $(A,\circ)$ i.e.

$(\forall x)(\forall y)(x\circ y)^{-1}=y^{-1}\circ x^{-1}$,

$(\forall x)(x^{-1})^{-1}=x$;

(iv) $^{-1}$ and $\circ$ are distributive over $+$ i.e.

$(\forall x)(\forall y)(x+y)^{-1}=x^{-1}+y^{-1}$,

$(\forall x)(\forall y)(\forall z)\ x\circ(y+z)=(x\circ y)+(x\circ z)$;

(v) $(\forall x)(\forall y)\ (x^{-1}\circ(\overline{x\circ y}))\cdot y=0$.

Example 1.

Let X be a set , and

$$\mathcal{R}(X)=(\mathcal{P}(X^2),\cup,\cap,^{-},\emptyset,X^2,\circ,\Delta_x,^{-1}),$$

where $\circ$ is the relative multiplication of binary relations (some authors use $R|S$ instead of $R\circ S$) :

$$R\circ S=\{(x,y):(\exists z\in X)((x,z)\in R \ \&\ (z,y)\in S)\} ,$$

$$\Delta_x=\{(x,x):\ x\in X\}\ (\text{called the diagonal of } X)$$

$$R^{-1}=\{(y,x):(x,y)\in R\}.$$

Then, it is easy to see that $\mathcal{R}(X)$ is a relation algebra. Algebras of the form $\mathcal{R}(X)$ are called *full relation algebras*. Obviously, every subalgebra of a full relation algebra is a relation algebra too. It is called *proper ralation algebra*.

Example 2.

We can generalize the previous example. Let ρ be an equivalence relation on the set X. Then every subalgebra of the algebra

$$E(\rho)=(\mathcal{P}(\rho),\cup,\cap,-,\emptyset,\rho,\circ,\Delta_x,^{-1})$$

satisfies the axioms of relation algebras. These algebras are called *algebras of relations*.

Note , that there are RA which are not isomorphic to any algebra of relations.

Relation algebra is in fact an "enriched" Boolean algebra. Since the additional operations are distributive (i.e additive) in each of their arguments, we can use, in our studies of relation algebras, the results of the theory of Boolean algebras with operators ([1],[3]).

On the other hand, every relation algebra $\mathcal{A}=(A,+,\cdot,-,0,1,\bullet,1',^{-1})$ contains the structure of a semigroup. The semigroup $(A,\bullet)$ is called the *semigroup reduct* of the algebra $\mathcal{A}$ and is denoted by $Rd_s(\mathcal{A})$.

How do the properties of the semigroup reduct reflect on relation algebra ? Can we learn something about the variety of relation algebras from the variety of semigroups ? In this paper we will present one of the possible semigroup-approaches to relation algebras. To each semigroup $\mathcal{S}$ we correlate a relation algebra $\Phi(\mathcal{S})$ so that $\mathcal{S}$ can be embedded into the semigroup reduct of $\Phi(\mathcal{S})$. This "construction Φ" enables, among other things, to show the unsolvability of the word problem for relation algebras and some other undecidability results. Here, we will present some other properties of this construction Φ.

2° SEMIGROUP - RELATION ALGEBRAS

It is well known that every Boolean algebra can be "enriched" to be a relation algebra. The analogous problem for semigroups has a negative answer : there are semigroups which are not semigroup reduct of any relation algebra. Namely, for any natural number k, there is a semigroup of cardinality k, but all finite relation algebras have 2^n elements for some n. The situation is similar for infinite semigroups too. For every relation algebra $\mathcal{A}$ the semigroup reduct $Rd_s(\mathcal{A})$ is a semigroup with identity element 1' and zero element 0. Hence, if a semigroup $\mathcal{S}$ has no identity element or no zero element, then it can not be the semigroup with such elements which can be enriched to be RA :

PROPOSITION 1.

For every cardinal number $\lambda \geq 3$ there is a semigroup $\mathcal{S}$ of cardinality λ, with identity and zero, such that $\mathcal{S}$ is not a semigroup reduct of any relation algebra.

Proof.

Let C be a set of cardinality λ, $\lambda \geq \omega$. Let $C=(C,*)$ be a constant semigroup (i.e. for all $x,y \in C$, $x*y=c$ for some $c \in C$). Denote by $\mathcal{S}$ the semigroup obtained from C by adding an identity 1' and a zero element 0. Suppose there is a relation algebra $\mathcal{A}$ such that $\mathcal{S} \cong Rd_s(\mathcal{A})$. Then 0 is a Boolean zero of $\mathcal{A}$ and 1' is the identity element of $Rd_s(\mathcal{A})$, and we know that $0^{-1}=0$ and $(1')^{-1} = 1'$. Hence for all $x \in C$ we have $x^{-1} \in C$. For the element $\bar{c}$ there are two possibilities :

(1) $\bar{c} \in C \cup (1')$ or

(2) $\bar{c} = 0$

We will prove that both (1) and (2) lead to a contradiction.

(1) Suppose $\bar{c} \in C \cup (1')$. First of all, it is a simple fact that $c^{-1}=c$ ($c^{-1}=(c \circ c)^{-1}=c^{-1} \circ c^{-1}=c$). Consider tha axiom (v) of RA and put $x=y=c$. We have $(c^{-1} \circ (\overline{c \circ \bar{c}}))\ c = (c \circ \bar{c})\ c = c\ c = c = \emptyset$, a contradiction.

(2) Suppose $\bar{c}=0$. Let $x_o \in C \setminus (\overline{1'}, c)$. Then $\overline{x_o} \in C$. Consider the axiom (v) and put $x=x_o$, $y=1'$. Then, we have :

$(x_o^{-1} \circ (\overline{x_o \circ 1'}))\ 1' = (x_o^{-1} \circ \overline{x_o})\ 1' = c\ 1' = 0 \Rightarrow 1' \leq \bar{c} \Rightarrow 1' \leq 0 \Rightarrow 1'=0$ a contradiction.

If $2<\lambda<\omega$, then the only difference is that for the set C we should take a set of cardinality $\lambda-2$.

Hence, we are forced to pose a weaker question : Is every semigroup embeddable into the semigroup reduct of some RA ?

The following assertion is well known in semigroup theory.

PROPOSITION 2.

Every semigroup is embeddable into the semigroup reduct of some relation algebra.

Proof.

Denote by $\mathcal{S}_1$ the monoid constructed from a semigroup by adding an identity. If $\mathcal{S}$ already has an identity, then put $\mathcal{S}_1=\mathcal{S}$. Since $\mathcal{S}<\mathcal{S}_1$, it is sufficient to prove the assertion for $\mathcal{S}_1$.

Define a mapping $\varphi: S_1 \to \mathcal{P}(S_1 \times S_1)$ in the following way :

$$\varphi(s)=\rho_s=\{(x, x\cdot s): x \in S_1\}.$$

Denote by $R=\{\rho_s: s \in S_1\}$. Then, φ is an isomorphism of semigroups $(S_1, \cdot)$ and $(R, \circ)$, where $\circ$ is the relative multiplication of relations.

Now, in the full relation algebra $\mathcal{R}(S_1)$ we distinguish the algebra generated by R,

$$\mathcal{A} = \langle R \rangle = \langle \{\rho_s: s \in S_1\} \rangle.$$

Then $\mathcal{S}_1 \cong (R, \circ) < Rd_s(\mathcal{A})$.

This correspondence, from the assertion above, which to every semigroup $\mathcal{S}$ assigns a proper relation algebra $\mathcal{A}$, we denote by Φ. All relation algebras $\mathcal{A}$ of the form $\Phi(\mathcal{S})$ will be called *semigroup relation algebras*.

Is it possible to obtain every proper relation algebra from a semigroup by the construction Φ ? It is easy to see that the one-element relation algebra can not be obtained in this way. But it is not the only one.

PROPOSITION 3.

For any cardinal number $\lambda \geq 3$ there is a proper relation algebra $\mathcal{A}$, over the set of λ elements, such that $\mathcal{A}$ is not a semigroup relation algebra.

Proof

Let X be a set of cardinality $\lambda \geq 3$, and $\mathcal{A}$ the minimal subalgebra of a full relation algebra $\mathcal{R}(X)$. Then $A=\{\Delta_x, \bar{\Delta}_x, \emptyset, X^2\}$. It is not difficult to see that there is no semigroup $\mathcal{S}$ such that $\Phi(\mathcal{S})=\mathcal{A}$.

It is interesting to note that all (non-trivial) finite full relation algebras are semigroup-relation algebras, but no infinite ful relation algebra is a semigroup-relation algebra.

THEOREM 1

The full relation algebras $\mathcal{R}(n)$, with n finite and $n \geq 1$, are semigroup-relation algebras.

Proof

For n=1 the proof is obvious.

Let $n \geq 2$, and let $\mathcal{S}_o$ be a right-zero semigroup over $S_o=\{0,1, \ldots ,n-2\}$. Denote by $\mathcal{S}$ the monoid constructed from $\mathcal{S}_o$ by adding an identity element e. Then

$S=\{0,1,2, \ldots ,n-2,e\}$,

$\rho_k=\{(x,x\cdot k): x \in S\}=\{(x,k): x \in S\}$, for $k \in S_o$,

$\rho_s^{-1} \circ \rho_k=\{(s,k)\}$ for $s,k \in S_o$.

Let $k \in S_o$, and

$\sigma_k=\cup\{\rho_s^{-1} \circ \rho_k: s \in S_o\}$.

Then

$\rho_k \cap \overline{\sigma_k} = \{(e,k)\}$ and

$(\rho_k \cap \overline{\sigma_k}) \circ (\rho_k \cap \overline{\sigma_k}) = \{(e,e)\}$

Thus, we obtain all the atoms in $\mathcal{R}(n)$. Therefore $\mathfrak{A}(\mathcal{S})=\mathcal{R}(n)$.

3° A CHARACTERIZATION OF SEMIGROUP-RELATION ALGEBRAS

Since there are proper relation algebras which are semigroup-relation algebras and there are some which are not, it is natural to ask what is a necessary and sufficient condition for a proper relation algebra to e a semigroup-relation algebra ?

By the construction, a necessary condition is that it is generated by some functional elements. An element f of relation algebra is *functional* if $f^{-1} \circ f \leq 1'$ ($\leq$ is the sign of the partial order in the Boolean part of relation algebra). However, from the proof of Proposition 3 we see that this condition is not sufficient. We need a new notion.

DEFINITION 2.

For an element $a \in A$ of a relation algebra $\mathcal{A}$ we say that it is a *proper functional element* if the following holds:

(i) $a^{-1} \circ a \leq 1'$

(ii) $a \circ a^{-1} \geq 1'$

Every proper functional element is functional but the converse is not true. If $\mathscr{A} < \mathscr{R}(X)$, then an element $f \in \mathscr{A}$ is a proper functional element of $\mathscr{A}$ iff f is the graph of a total function from X into X. If $\mathscr{A} < \mathscr{R}(X)$ and $f \in \mathscr{A}$ is a functional element, then f is the graph of some partial function from X. In these cases we can write $f(x)=y$ instead of $(x,y) \in f$.

THEOREM 2.

Let $\mathscr{A} < \mathscr{R}(B)$, $B \neq \emptyset$. The following conditions are equivalent.

(i) $\mathscr{A}$ is a semigroup-relation algebra ;

(ii) There is a set of proper functional elements $\langle f_b : b \in B\rangle$ which generates $\mathscr{A}$ so that

$$(\exists e \in B)(\forall x \in B)\ \ f_e(x) = f_x(e) = x \ \text{ and if}$$
$$f_k(j) = t \ \text{ then } \ f_j \circ f_k = f_t \qquad (j,k \in B)$$

Proof

(ii) $\rightarrow$ (i)

Define on the set B an operation $*$ in the following way

$$x * y = f_y(x).$$

Then $(B,*)$ is a monoid with the identity e, because

$$(i*j)*k = f_k(i*j) = f_k(f_j(i)) = (f_j \circ f_k)(i) = f_{f_k(j)}(i) = f_{j*k}(i) =$$
$$= i*(j*k)$$

and

$$x*e = f_e(x) = f_x(e) = e*x = x.$$

Further on, for all $b \in B$ we have

$$\rho_b = \{(x,x*b) : x \in B\} = \{(x,f_b(x)) : x \in B\}$$

i.e. $\rho_b = f_b$. Hence,

$$\mathscr{A} = \langle\{f_b : b \in B\}\rangle = \langle\{\rho_b : b \in B\}\rangle \text{ and}$$
$$\mathfrak{P}(\mathscr{B}) = \mathscr{A}.$$

(i) $\rightarrow$ (ii) ,

If $\mathfrak{P}(\mathscr{B}) = \mathscr{A}$, then we can take that $\mathscr{B}$ is a monoid. If we define elements f_b $(b \in B)$ by

$$f_b = \{(x,x\cdot b) : b \in B\},$$

then all f_b will be proper functional elements satysfying the condition (ii). Namely, if e is the identity of $\mathscr{B}$, then

$$f_e(x) = x\cdot e = e\cdot x = f_x(e) = x .$$

$$(f_j\circ f_k)(i) = f_k(f_j(i)) = f_k(i\cdot j) = (i\cdot j)\cdot k = i\cdot(j\cdot k) = i\cdot f_k(j) =$$

$$= f_{f_k(j)}(i).$$

Remark

We can prove that the class of all RA, which are isomorphic to a semigroup-relation algebra, is not an elementary class. ([2])

Using the characterization of semigroup-relation algebras given in Theorem 2. we can prove the following :

COROLLARY 1.

Let X be an infinite set. The full relation algebra $\mathcal{R}(X)$ is not a semigroup-relation algebra.

Proof

If $\mathcal{R}(X)$ is a semigroup-relation algebra, then according to Theorem 2. it has a generating set of cardinality $|X|$. However, if X is infinite, then $|X|$ elements generate a set of $|X|$ elements but $|X|<|\mathcal{R}(X)|$. So, $\mathcal{R}(X)$ is not a semigroup-relation algebra.

4° REGULARITY

Which smigroup-properties are preserved by the mapping $\mathfrak{P}$? For example, if $\mathcal{S}$ is a commutative semigroup, is then $Rd_s(\mathfrak{P}(S))$ comutative too ? Not necessarily.

Example 3.

Let $\mathcal{S}=(\{a,b\},\cdot)$ be a (commutative) semigroup with the identity a, and $b\cdot b=b$. Then

$$\rho_a = \{(a,a),(b,b)\}$$

$$\rho_b = \{(a,b),(b,b)\}$$

$$\rho_b \cap \rho_b^{-1} = \{(b,b)\}$$

$$\{(b,b)\}\circ\overline{\rho_a} = \{(b,a)\} \text{ and}$$

$$\{(b,a)\} \circ \{(b,b)\} \neq \{(b,b)\} \circ \{(b,a)\} ,$$

i.e. $Rd_s(\mathfrak{P}(S))$ is not commutative.

Here, we are going to examine the regularity of relation algebras. A semigroup S is *regular* if $(\forall x \in S)(\exists y \in S)\ x\,y\,x = x$. Zareckiĭ (1962) was the first to give a characterization of regular elements in the semigroup $\mathcal{B}_X = (\mathcal{P}(X^2), \circ)$, but his criterion is not very suitable for practical applications. B. Schein gave in [5] a new, much simpler criterion for determination of regularity of a given binary relation.

THEOREM 3. (Schein, 1976.)

A binary relation $\rho \subseteq X^2$ is regular in the semigroup $\mathcal{B}_X$ iff $\rho \subseteq \rho \circ (\rho^{-1} \circ \overline{\rho} \circ \rho^{-1}) \circ \rho$.

Why are we interested in regular elements ? Among other things, regular relations are connected with very important binary relations - relations of partial order. The theorem, which says something about that, was proved by Wolk in 1969 (Sinkevič simplified this proof in 1974 [6]).

THEOREM 4. (Wolk, 1969.)

A reflexive and antisymmetric relation is transitive iff it is regular.

We are going to use these two theorems later.

DEFINITION 3.

For a relation algebra $\mathcal{A}$ we say that it is *regular* if $\mathrm{Rd}_s(\mathcal{A})$ is a regular semigroup.

The following example shows that the mapping Φ does not preserve regularity:

Example 4.

Let $\mathcal{G}$ be the cyclic group of order 3, $G=\{e, a, a^2\}$. Since $\mathcal{G}$ is a group, it is a regular semigroup. Then $\rho_a = \{(e,a),(a,a^2),(a^2,e)\}$. The relation $\rho = \rho_a \cup \Delta_G$ is reflexive and antisymmetric, but not transitive. Because of Wolk's theorem, this relation is not regular element of the semigroup $\mathrm{Rd}_s(\Phi(\mathcal{G}))$.

We can generalize this example.

PROPOSITION 4.

Let $\mathcal{S}$ be a semigroup. If $\mathfrak{P}(\mathcal{S})$ is regular, then

$$\mathcal{S} = (\forall y)(\exists x)\ x\,y^2 = x.$$

Proof

Suppose $\mathcal{S} \neq (\forall y)(\exists x)\ x\,y^2 = x$. Then $\mathcal{S} = (\exists y)(\forall x)\ x\,y^2 \neq x$, and denote that element y by c hence, $(\forall x \in S)\ x\,a^2 \neq x$). Then the relation $\rho = \rho_a \cup \Delta_s$ is not a regular element of the semigroup $Rd_s(\mathfrak{P}(S))$. Namely, ρ is reflexive and antisymmetric but it is not transitive : for all elements $x \in G$ it holds that

$$(x, xa) \in \rho_a\ ,\ (x\,a, x\,a^2) \in \rho_a \quad \text{but} \quad (x, x\,a^2) \notin \rho.$$

COROLLARY 2.

Let $\mathcal{G}$ be a group. If $\mathfrak{P}(\mathcal{G})$ is regular, then $\mathcal{G}$ is a Boolean group.

Proof

In a Boolean group, for all elements x it holds that $x^2=e$, where e is the identity of the group. If $\mathcal{G}$ is not a Boolean group, then there is an element a such that $a^2 \neq e$. Hence

$$\mathcal{G} = (\forall x)\ x\,a^2 \neq x.$$

The conclusion follows now, immediately, from the previous assertion.

Therefore, out of groups, only Boolean groups can give a regular relation algebra. However, the converse is not true. There is a Boolean group $\mathcal{G}$ such that $\mathfrak{P}(\mathcal{G})$ is not regular.

Example 5.

Let $\mathcal{G}$ be the Klein's four-element group, $G = (e,a,b,c)$. Then, the element $\rho = \rho_a \cup \rho_b \cup \Delta_G$ is not regular in $Rd_s(\mathfrak{P}(\mathcal{G}))$. Namely,

$$\rho^{-1} \circ \bar{\rho} \circ \rho^{-1} = \rho_c \cup \Delta \cup \rho_b \cup \rho_a\ ,$$

$$\rho^{-1} \circ \bar{\rho} \circ \rho^{-1} = \emptyset \quad \text{and} \quad \rho \subseteq \rho \circ \emptyset \circ \rho = \emptyset\ .$$

Because of Schein's criterion, ρ is not regular element in $Rd_s(\mathfrak{S}(\mathcal{G}))$.

THEOREM 5.

Let $\mathcal{G}$ be a Boolean group having order greater than 2. Then $\mathfrak{S}(\mathcal{G})$ is not regular.

Proof

1. If $\mathcal{G}$ is a group, then for all $a,b \in G$ we have

$$a \neq b \to \rho_a \cap \rho_b = \emptyset \quad \text{and} \quad \cup(\rho_a : a \in G) = G^2.$$

Really, $(x,y) \in \rho_a \cap \rho_b \to (y = x\,a \;\&\; y = x\,b) \to a = b$ and

$$(x,y) \in G^2 \to (\exists a)(y = x\,a) \to (\exists a)(x,y) \in \rho_a.$$

2. If $\mathcal{G}$ is a Boolean group, then all the relations

$$\sigma_X = \cup(\rho_a : a \in X), \quad X \subseteq G,$$

are symetric. Namely,

$$(x,y) \in \rho_a \to y = x\,a \to y\,a = x\,a\,a \to x = y\,a \to (y,ya) \in \rho_a$$

i.e $(y,x) \in \rho_a$,

and

$$(\cup(\rho_a : a \in X))^{-1} = \cup(\rho_a^{-1} : a \in X) = \cup(\rho_a : a \in X).$$

3. Let $\mathcal{G}$ be a Boolean group, $a \in G$ ($a \neq e$). Then the relation $\rho = \overline{\rho_a}$ is not a regular element of $Rd_s(\mathfrak{S}(\mathcal{G}))$. Namely, we can prove that $\rho^{-1} \circ \overline{\rho} \circ \rho^{-1} = G^2$:

$$\sigma = \rho^{-1} \circ \overline{\rho} \circ \rho^{-1} = (\overline{\rho}_a)^{-1} \circ \overline{\rho}_a \circ (\overline{\rho}_a)^{-1} =$$

$$= (\cup(\rho_b : b \neq a, b \in G))^{-1} \circ \rho_a \circ (\cup(\rho_c : c \neq a, c \in G))^{-1} =$$

$$= (\cup(\rho_b : b \neq a, b \in G)) \circ \rho_a \circ (\cup((\rho_c : c \neq a, c \in G)).$$

Let $d \neq a$, $d \neq e$. Then

$$\rho_d = \Delta \circ \rho_a \circ \rho_{ad} \subseteq \sigma.$$

If $b \neq e$ and $b \neq a$ then $a\,b \neq a$ and we have

$$\Delta = \rho_e \subseteq \rho_b \circ \rho_a \circ \rho_{ab} \subseteq \sigma.$$

Finally,

$\rho_a = \Delta \circ \rho_a \circ \Delta \subseteq \sigma$, so we have that

$\cup(\rho_d : d \in G) \subseteq \sigma$ i.e. $\sigma = G^2$. Hence, because of Schein's criterion, ρ is not a regular element.

COROLLARY 3.

Let $\mathcal{G}$ be a group. Then $\mathfrak{S}(\mathcal{G})$ is regular iff $|G| \leq 2$.

Proof

($\Leftarrow$) One-element group gives a regular relation algebra. If $|G|=2$, then the carrier of $\mathfrak{P}(\mathfrak{G})$ is $B=(\Delta_\sigma, \bar{\Delta}_\sigma, \emptyset, G^2)$ and $(B,\circ)$ is a regular semigroup.

($\Rightarrow$) Let $\mathfrak{P}(\mathfrak{G})$ be a regular RA. Because of Corrolary 2. and Theorem 5. it follows that $|G| \leq 2$.

Note, that the propertie of Boolean groups given in the proof of Theorem 5. was the first step in the proof of non-axiomatizability of the class $I\mathfrak{P}^*(SEM)$ of all relation algebras isomorphic to a semigroup-relation algebra (see [2]).

REFERENCES

[1] L.H.Chin, A.Tarski, Distributive and modular laws in the arithmetic of relation algebras, Univ. Calif. Publ. Math., New Series, 1 (1951), 341-384.

[2] S.Crvenković, R.Madarasz, A non-axiomatizability result, to appear ,

[3] B.Jonsson, The Theory of binary relations, A first draft.

[4] R.Madarasz, Relacione algebre, M.Sc.Theses, Novi Sad, 1986.

[5] B.Schein, Regular elements of the semigroup of all binary relations, Semigroup Forum , 13 (1976) , 95-102.

[6] В.Н.Синкевич, Элементарное доказательство одной теоремы Е.С. Волка, Теория полугрупп и ее приложения, Межвузовски научны сборник, Б.3. (1974), 107-108.

[7] A.Tarski, On the calculus of relations, The Journal of Sumbolic Logic, 6 (1941) , 73-89.

Institute of Mathematics
University of Novi Sad
21000 Novi Sad
Yugoslavia

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

FULLY COMMUTATIVE VECTOR VALUED GROUPOIDS

Ǵ.Čupona, A.Samardžiski, N.Celakoski

Abstract. The notion of "commutative vector valued operation" is modified in this paper such that the range of the operation is factorized under commutativity. Namely, if Q is a nonempty set and r is a positive integer, then $Q^{(r)}=Q^r/\simeq$, *where*

$a,b\in Q^r \Longrightarrow (a \simeq b \Longleftrightarrow b$ *is a permutation of* $a)$.

Every mapping $f: Q^{(n)}\longrightarrow Q^{(m)}$ *is called a fully commutative (n,m)-operation and* $\underline{Q}=(Q;f)$ *is called a fully commutative (n,m)-groupoid (shortly: f.c.g.).*

A description of the free generated f.c.g. is given and a result different from the usual algebras is obtained here. Namely, if $\underline{Q}$ *is a free f.c. (n,m)-groupoid* ($m \geq 2$) *with a basis B, then the identity mapping on B can be extended to infinitely many automorphisms on* $\underline{Q}$. *We discuss the notion of fully commutative (n,m)-quasigroups (shortly: f.c.q.) and we give a description of the free f.c.q. by using the notion of partial f.c.q. Finally, finite f.c.q. are considered and some examples of finite f.c.q. are given.*

1. FULLY COMMUTATIVE (n,m)-OPERATIONS

If Q is a nonempty set and n,m are positive integers, then any mapping $f: Q^n\longrightarrow Q^m$ is called an (n,m)-operation or a vector valued operation. (Here, Q^r is the r-th Cartesian power, i.e.

$$Q^r = \{(a_1,a_2,\ldots,a_r) \mid a_\nu\in Q\};$$

the elements of Q^r will be denoted also by $a_{\alpha+1}^{\alpha+r}$, where $a_\nu\in Q$, $\alpha \geq 0$ and sometimes by a single letter a.)

An (n,m)-operation f is said to be commutative ([4], §2) iff for every permutation σ of the set $\mathbb{N}_n = \{1,2,\ldots,n\}$ the following identity holds:

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

$f(a_1^n) = f(\sigma(a_1^n))$, where $\sigma(a_1^n) = a_{\sigma(1)}a_{\sigma(2)}\cdots a_{\sigma(n)}$.

More generally, f is said to be weakly commutative iff for every $a_1^n \in Q^n$ and a permutation b_1^n of a_1^n, the following implication is true:

$f(a_1^n) = c_1^m$, $f(b_1^n) = d_1^m \Longrightarrow d_1^m$ is a permutation of c_1^m.

Here we will consider another kind of vector valued operations which we call "fully commutative (n,m)-operations".

Namely, let $r \geq 1$ and let $\approx$ be a relation in Q^r defined by:

$a_1^r \approx b_1^r$ iff b_1^r is a permutation of a_1^r.

It is clear that $\approx$ is an equivalence in Q^r. The factor set $Q^r/\approx$, denoted by $Q^{(r)}$, will be called "the commutative r-th power of Q". The elements of $Q^{(r)}$ will be denoted again by $a_{\alpha+1}^{\alpha+r}$, where $a_\nu \in Q$ and $\alpha \geq 0$, but now:

$a_{\alpha+1}^{\alpha+r} = b_{\beta+1}^{\beta+r} \Longleftrightarrow b_{\beta+1}^{\beta+r}$ is a permutation of $a_{\alpha+1}^{\alpha+r}$.

If $n,m \geq 1$, then every mapping $f: Q^{(n)} \to Q^{(m)}$ will be called a fully commutative (n,m)-operation.

Let $f: Q^n \to Q^m$ be a given (n,m)-operation. It is natural to ask the following question:

Under what conditions there exists a fully commutative (n,m)-operation $f': Q^{(n)} \to Q^{(m)}$ ("induced by f") such that the following diagram is commutative:

$$\begin{array}{ccc} Q^n & \xrightarrow{\quad f \quad} & Q^m \\ \Big\downarrow{\scriptstyle nat_n^{\approx}} & & \Big\downarrow{\scriptstyle nat_m^{\approx}} \\ Q^{(n)} & \xrightarrow{\quad f' \quad} & Q^{(m)} \end{array}$$

Diagram 1

where $nat_r^{\approx}$ is the canonical mapping from Q^r into $Q^{(r)}$?

Conversely, if $f': Q^{(n)} \to Q^{(m)}$ is a given fully commutative (n,m)-operation, one can ask the question of existence of (n,m)-operation $f: Q^n \to Q^m$, such that the above diagram is commutative.

Consider a more general situation, i.e. the diagram

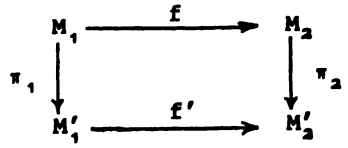


Diagram 2

where M_i, M_i' (i=1,2) are sets. It is easy to show the following:

PROPOSITION 1.1. Let $\pi_i: M_i \to M_i'$ be a surjection for i=1,2.

(i) If $f: M_1 \to M_2$ is a mapping, then there exists at most one mapping $f': M_1' \to M_2'$ such that Diagram 2 is commutative, i.e. $\pi_2 f = f'\pi_1$.

Such a mapping f' do exist iff the following condition is satisfied:

$$(\forall x,y \in M_1)(\pi_1(x)=\pi_1(y) \Longrightarrow \pi_2(f(x)) = \pi_2(f(y))). \qquad (1.1)$$

(ii) If $f': M_1' \to M_2'$ is a mapping, then there exists a mapping $f: M_1 \to M_2$ such that $\pi_2 f = f'\pi_1$.

In general, there are more than one such mappings f, defined in the following way:

$$f = \bigcup_{x' \in M_1'} f_{x'}, \text{ where } f_{x'}: \pi_1^{-1}(x') \to \pi_2^{-1}(f'(x'))$$

is arbitrary. □

In the special case when $f:Q^n \to Q^m$ is an (n,m)-operation, the condition (1.1) has the following meaning: if y is a permutation of x, then f(y) is a permutation of f(x). Thus, we have the following:

PROPOSITION 1.2. Let $f: Q^n \to Q^m$ be an (n,m)-operation on a nonempty set Q. There exists at most one fully commutative (n,m)-operation $f': Q^{(n)} \to Q^{(m)}$ on Q such that the diagram 1 is commutative. Such an operation f' exists iff f is weakly commutative.

Conversely, any fully commutative (n,m)-operation f' is induced by a set of weakly commutative (n,m)-operations, between which there are commutative ones.

If $f: Q^{(n)} \to Q^{(m)}$ is a fully commutative (n,m)-operation, then $\underline{Q}=(Q;f)$ will be called a fully commutative (n,m)-groupoid. Further on, we will consider fully commutative (n,m)-groupoids (or -operations) only. Therefore we will usually omit the words "fully commutative"; also, the integers n,m will be usually considered as fixed and so we will often say simply "groupoid" (or "operation") instead of "fully commutative (n,m)-groupoid" (or "fully commutative (n,m)-operation").

We will introduce here several concepts which will be used later.

Let $\underline{Q}=(Q;f)$ be a groupoid and H a nonempty subset of Q. H is called a subgroupoid of $\underline{Q}$, in notation $H \leq \underline{Q}$, iff

$$a_1^n \in H^{(n)} \Longrightarrow f(a_1^n) \in H^{(m)}.$$

Clearly, the following proposition is true:

PROPOSITION 1.3. If $\{H_\alpha \mid \alpha \in A\}$ is a nonempty family of subgroupoids of a groupoid $\underline{Q}$ and if $H = \bigcap_\alpha H_\alpha$ is a nonempy set, then H is a subgroupoid of $\underline{Q}$. □

A subgroupoid H of a groupoid $\underline{Q}$ is said to be generated by a nonempty subset B of Q iff

(i) $B \subseteq Q$, (ii) $K \leq \underline{Q}$ & $B \subseteq K \Longrightarrow H \leq K$.

Proposition 1.3 implies that:

PROPOSITION 1.4. If $\underline{Q}$ is a groupoid and B is a nonempty subset of Q, then there exists a uniquely determined subgroupoid of $\underline{Q}$ which is generated by B. □

A description of the subgroupoid of $\underline{Q}$ generated by a set $B \subseteq Q$ can be given in the following way. Let $B_0, B_1, B_2, \ldots$ be a sequence of subsets of Q defined as follows:

$$B_0 = B, \quad B_{p+1} = B_p \cup C_{p+1},$$

where $C_{p+1} = \{b \in Q \setminus B_p \mid (\exists a_1^n \in B_p^{(n)}) f(a_1^n) = b\, b_2^m\}$. Then the set $\langle B \rangle = \bigcup_{p \geq 0} B_p$ is the subgroupoid of $\underline{Q}$ generated by B.

To every element $c \in \langle B \rangle$ we assign a number $\chi_B(c)$, called the hierarchy of c, relative to B, defined by:

$$\chi_B(c) = \min\{p \mid c \in B_p\}.$$

The notion of homomorphism can be introduced in a usual way. Namely, let $\underline{Q}=(Q;f)$ and $\underline{Q}'=(Q';f')$ be groupoids and ϕ a mapping from Q into Q'. We say that ϕ is a homomorphism from $\underline{Q}$ into $\underline{Q}'$ iff

$$f(a_1^n) = b_1^m \Longrightarrow f'(\bar{a}_1^n) = \bar{b}_1^m,$$

where $\bar{c}=\phi(c)$, $c\in Q$. If, in addition, ϕ is bijective, then ϕ is called an isomorphism. It is easy to show that:

PROPOSITION 1.6. $\phi: \underline{Q} \to \underline{Q}'$ is an isomorphism iff $\phi^{-1}: \underline{Q}' \to \underline{Q}$ is an isomorphism. □

The notions of an endomorphism and automorphism have the usual meanings.

2. FREE FULLY COMMUTATIVE (n,m)-GROUPOIDS

We will give here a description of free fully commutative (n,m)-groupoids which we will call, shortly again, free groupoids.

A groupoid $\underline{Q}=(Q;f)$ is said to be free with a basis B iff the following conditions are satisfied:

(i) B is a generating set for $\underline{Q}$;

(ii) if $\underline{Q}'=(Q';f')$ is a groupoid and $\psi: B \to Q'$, then there exists a homomorphism $\phi: \underline{Q} \to \underline{Q}'$ which is an extension of ψ.

In order to give a description of free groupoids, let B be a nonempty set and let $(B_p \mid p \geq 0)$ be a sequence of sets defined as follows:

$$B_0 = B, \quad B_{p+1} = B_p \cup \mathbb{N}_m \times B_p^{(n)},$$

where $\mathbb{N}_m$ denotes the set $\{1,2,\ldots,m\}$. If $u\in B_{p+1}\setminus B_p$, then we say that u has the hierarchy p+1 and we write $\chi(u)=p+1$; if $b\in B$, then we set $\chi(b) = 0$.

Let $[B]=\bigcup_{p\geq 0} B_p$ and define an (n,m)-operation $f:[B]^{(n)} \to [B]^{(m)}$ by:

$$f(u_1^n) = (1,u_1^n)(2,u_1^n)\ldots(m,u_1^n). \tag{2.1}$$

So we obtain a groupoid $\underline{[B]}=([B];f)$ with a generating set B. Here, the notion of hierarchy of $u\in[B]$ coincides with the notion of the hierarchy relative to B introduced in 1.

Suppose now that $\underline{Q}'=(Q';f)$ is a groupoid and $\psi: B \to Q'$ an arbitrary mapping from B into Q'. We will show that there exists a homomorphism $\phi: [\underline{B}] \to \underline{Q}'$ which is an extension of ψ.

First, for $b \in B$, we set $\phi(b)=\psi(b)$. Suppose that $\phi(u)=\bar{u} \in Q'$ is a well defined element of Q' if $u \in Q$ has a hierarchy $\leq p$. If $v \in [B]$ has a hierarchy p+1, then v has the form $v=(i,u_1^n)$, where $i \in \mathbb{N}_m$, $u_1^n \in [B]^{(n)}$, $\chi(u_\nu) \leq p$ and $\chi(u_\alpha)=p$ for some α. Then, setting $v_j=(j,u_1^n)$, we obtain that $\chi(v_j)=p+1$ for every $j \in \mathbb{N}_m$. Since $\bar{u}_1^n \in Q'^{(n)}$, there exists $c_1^m \in Q'^{(m)}$ such that $f'(\bar{u}_1^n)=c_1^m$. Then, if we put $\phi(v_j)=c_j$, we obtain that $\phi(v_j) \in Q'$ is a well-defined element for every $j \in \mathbb{N}_m$.

(Note that, in general, there are many ways of defining $\phi(v_1),\phi(v_2),\ldots,\phi(v_m)$, but not more than m!)

Thus, by induction on hierarchy, we defined a mapping $\phi: [B] \to Q'$ which is an extension of ψ.

By the definitions of $f: [B]^{(n)} \to [B]^{(m)}$ and $\phi: [B] \to Q'$, it is clear that $\phi: [\underline{B}] \to \underline{Q}'$ is a homomorphism. Thus, we proved the following:

PROPOSITION 2.1. $[\underline{B}]$ is a free groupoid with a basis B. □

Now we will prove that:

PROPOSITION 2.2. If ξ is an endomorphism on $[\underline{B}]$ such that

$$(\forall b \in B)\ \xi(b) = b, \tag{2.2}$$

then ξ is an automorphism on $[\underline{B}]$.

Proof. If $p \geq 0$, then we denote by S_p the set $\{u \in [B] |\ \chi(u)=p\}$. By the above assumption, ξ induces the identity bijection from S_0 into S_0. Suppose that ξ induces a bijection from the set S_p into S_p. Let $v \in S_{p+1}$. Then v has the form $v=(i,u_1^n)$ for some $i \in \mathbb{N}_m$ and $u_1^n \in S_p^{(n)}$, where there exists $\nu \in \mathbb{N}_m$, such that $\chi(u_\nu)=p$. Put $v_\alpha=(\alpha,u_1^n)$. Then $f(u_1^n)=v_1^m$, and thus $f(\bar{u}_1^n)=\bar{v}_1^m$, where $\xi(u_\nu)=\bar{u}_\nu \in S_p$, $\bar{v}_\alpha=\xi(v_\alpha)=\xi(v)$. Now, $\xi(v)=(j,\bar{u}_1^n)$, where $\xi(u_\nu)=\bar{u}_\nu$ and $j \in \mathbb{N}_m$. Therefore, using the hypothesis that $\xi(S_p)=S_p$, we have $\xi(v) \in S_{p+1}$. This implies that if $\xi(v)=\xi(w)$, then $w=(s,u_1^n)$ for some $s \in \mathbb{N}_m$. Setting $v_\alpha=(\alpha,u_1^n)$, we obtain that $\xi(v_\alpha)=(\ell_\alpha,\bar{u}_1^n)$, where $\alpha \mapsto \ell_\alpha$ is a permutation of $\mathbb{N}_m$, and this implies that

$$\xi(v) = \xi(w) \Longrightarrow v = w_1$$

Thus the restriction of ξ on S_{p+1} is an injection. It remains to show that this restriction is a surjection. Let $u=(i,u_1^n)\in S_{p+1}$. Then $u_\mu \in S_p$, and thus there exist $v_\mu \in S_p$ such that $\xi(v_\mu)=(u_\mu)$. If we put $w_\beta=(\beta,v_1^n)$, then we obtain that there exists $\gamma\in N_m$ such that $\xi(w_\gamma)=u$. This completes the proof that ξ is a bijection and thus an automorphism.

(Note that the set of automorphisms ξ on $[\underline{B}]$, with (2.2) is infinite.) □

If $\underline{Q}=(Q;f)$ is an another free (n,m)-groupoid with a basis B, then there exist homomorphisms $\zeta\colon [\underline{B}] \to \underline{Q}$, $\eta\colon \underline{Q} \to [\underline{B}]$, such that

$$(\forall b\in B)\ \zeta(b) = \eta(b) = b. \tag{2.3}$$

Clearly, $\xi=\eta\zeta$ is an endomorphism on $[\underline{B}]$ with the property (2.2). Thus ξ is an automorphism on $[\underline{B}]$, which implies that ζ is an injective homomorphism.

By induction on hierarchy of elements of $Q=\langle B\rangle$ we will show that ζ is surjective as well. Let $c\in Q$ has the hierarchy p+1 (relative to B). Then there exist $c_1^m\in Q^{(m)}$ such that $c_i=c$ for some $i\in N_m$, and $d_1^n\in Q^{(n)}$ such that $g(d_1^n)=c_1^m$ and $d_1^n\in T_p^{(n)}$, where $T_p=\{d\in Q \mid \chi_B(d) \le p\}$. These assumptions imply that there exists $u_1^n\in [B]^{(n)}$ such that $\zeta(u_\nu)=d_\nu$. If $f(u_1^n)=v_1^m$, then $f(d_1^n)=\bar{v}_1^m$, where $\bar{v}_\alpha=\zeta(v_\alpha)$. Thus $c_1^m=\bar{v}_1^m$, i.e. $c=\bar{v}_\alpha=\zeta(v_\alpha)$ for some α, which proves that ζ is surjective.

We will restate the above results (P.2.1, P.2.2 and the last one) as the following:

THEOREM 2.3. (i) Every nonempty set B is a basis of a free fully commutative (n,m)-groupoid.

(ii) If B is a basis of a free fully commutative (n,m)-groupoid, then the set of its automorphisms which fix the all elements of B is infinite.

(iii) Free groupoids with a same basis are isomorphic. □

(We note that (ii) is something different from the usual algebras.)

3. FULLY COMMUTATIVE VECTOR VALUED QUASIGROUPS

In this section we will assume that $n-m = k \geq 1$ and $m \geq 2$.

A groupoid $\underline{Q}=(Q;f)$ is said to be cancellative iff for every $a \in Q^{(k)}$, $x,y \in Q^{(m)}$ the following implication is true:

$$f(ax) = f(ay) \Longrightarrow x = y. \tag{3.1}$$

A groupoid $\underline{Q}$ is called a fully commutative (n,m)-quasigroup or, shortly, a quasigroup iff for every $a \in Q^{(k)}$, $b \in Q^{(m)}$ the equation

$$f(ax) = b$$

is uniquely solvable on x in $Q^{(m)}$.

Clearly, every quasigroup is a cancellative groupoid, and every finite cancellative groupoid is a quasigroup.

We will show below that every cancellative groupoid is a subgroupoid of a quasigroup.

First we will consider a more general concept of fully commutative partial (n,m)-groupoid. Namely, if $Q \neq \emptyset$, $\mathcal{D} \subseteq Q^{(n)}$ and $f: \mathcal{D} \to Q^{(m)}$, then we call $(Q;\mathcal{D};f)=\underline{Q}$ a fully commutative partial (n,m)-groupoid. As in §1 we will omit the words "fully commutative" and "(n,m)-".

A partial groupoid $\underline{Q}=(Q;\mathcal{D};f)$ is said to be cancellative iff for every $a \in Q^{(k)}$, $x,y \in Q^{(m)}$ such that $ax, ay \in \mathcal{D}$, the following implication is true:

$$f(ax) = f(ay) \Longrightarrow x = y.$$

In this case we say also that $\underline{Q}$ is a partial quasigroup, i.e. a partial groupoid $\underline{Q}$ is a partial quasigroup iff $\underline{Q}$ is cancellative. In particular: every cancellative groupoid is a partial quasigroup.

We will prove first the following more general result: every partial quasigroup is a partial subgroupoid of a quasigroup. (Note that $(Q;\mathcal{D};f)$ is a partial subgroupoid of a partial groupoid $(Q';\mathcal{D}';f')$ iff

$$Q \subseteq Q',\ \mathcal{D} \subseteq \mathcal{D}' \text{ and } a_1^n \in \mathcal{D} \Longrightarrow f(a_1^n) = f'(a_1^n).)$$

For this purpose we will consider first two kinds of extensions of partial groupoids.

Let $\underline{Q}=(Q;\mathcal{D};f)$ be a partial groupoid with the domain $\mathcal{D}$. Define two partial groupoids, $\underline{Q}^{\Delta}=(Q^{\Delta};\mathcal{D}^{\Delta};f^{\Delta})$ and $\underline{Q}^{\bullet}=(Q^{\bullet};\mathcal{D}^{\bullet};f^{\bullet})$, in the following way:

1) $Q^{\Delta} = Q\cup\{(i,a_1^n) \mid i\in N_m,\ a_1^n\in Q^{(n)}\setminus\mathcal{D}\}$, $\mathcal{D}^{\Delta} = Q^{(n)}$,

$a_1^n\in\mathcal{D} \Longrightarrow f^{\Delta}(a_1^n) = f(a_1^n)$,

$a_1^n\in Q^{(n)}\setminus\mathcal{D} \Longrightarrow f^{\Delta}(a_1^n) = (1,a_1^n)(2,a_1^n)\dots(m,a_1^n)$;

2) $Q^{\bullet} = Q\cup R$, $\mathcal{D}^{\bullet} = \mathcal{D}\cup\mathcal{E}$, where:

$R = \{(i;a,b) \mid i\in N_m,\ a\in Q^{(k)},\ b\in Q^{(m)},$

$(\forall x\in Q^{(m)})[ax\notin\mathcal{D} \text{ or } (ax\in\mathcal{D} \text{ and } f(ax)\neq b)]\}$,

$\mathcal{E} = \{a(1;a,b)(2;a,b)\dots(m;a,b) \mid (i;a,b)\in R\}$,

$a_1^n\in\mathcal{D} \Longrightarrow f^{\bullet}(a_1^n) = f(a_1^n)$,

$f^{\bullet}(a(1;a,b)\dots(m;a,b)) = b$, for every $(i;a,b)\in R$.

It is easy to show that, if $\underline{Q}$ is a partial quasigroup, then $\underline{Q}^{\Delta}$ and $\underline{Q}^{\bullet}$ are partial quasigroups as well.

Now suppose that $\underline{Q}_1,\underline{Q}_2,\dots,\underline{Q}_{\alpha},\underline{Q}_{\alpha+1},\dots$ is a sequence of partial groupoids such that $\underline{Q}_{\alpha}$ is a partial subgroupoid of $\underline{Q}_{\alpha+1}$. Setting

$$Q = \bigcup_{\alpha\geq 1} Q_{\alpha},\quad \mathcal{D} = \bigcup_{\alpha\geq 1}\mathcal{D}_{\alpha}$$

and

$$f(a_1^n) = b_1^m \iff (\exists\alpha)(a_1^n\in\mathcal{D}_{\alpha} \ \&\ f_{\alpha}(a_1^n) = b_1^m),$$

we obtain a partial groupoid $(Q;\mathcal{D};f)=\underline{Q}$ where $\underline{Q}_{\alpha}$ is a partial subgroupoid of $\underline{Q}$ for every $\alpha\geq 1$. It is clear also that, if $\underline{Q}_{\alpha}$ is a partial quasigroup, then $\underline{Q}$ is a partial quasigroup too. (In general, $\underline{Q}$ may not be a quasigroup, even in the case when all of $\underline{Q}_{\alpha}$ are cancellative groupoids.)

Now suppose that $\underline{Q}$ is a given partial quasigroup and that the sequence of partial groupoids $\underline{Q}_0,\underline{Q}_1,\dots,\underline{Q}_{\alpha},\underline{Q}_{\alpha+1},\dots$ is formed in the following way:

$$\underline{Q}_0 = \underline{Q},\ \underline{Q}_{2\alpha+1} = \underline{Q}_{2\alpha}^{\bullet},\ \underline{Q}_{2\alpha} = \underline{Q}_{2\alpha-1}^{\Delta}.$$

Then the union $S(\underline{Q})$ of the obtained sequence is a quasigroup.

A complete proof of this one can obtain easily by the assumption that $\underline{Q}$ is a partial quasigroup and by the definition of the functors Δ and $\bullet$. We note that a similar construction in

the case of (usual) binary quasigroups is known. (See, for example, [2] ch. I.)

If B is a given set and if we put $\mathcal{D}=\emptyset$, then we obtain a partial quasigroup $(B;\emptyset;f)=\underline{B}$. The quasigroup which in this case one obtaines by B is the free quasigroup with a basis B.

It is natural to ask the question for existence of quasigroups with a given carrier Q. By the construction of $Q^{\bullet}$ and Q^{Δ} it is clear that: if Q is an infinite set, then Q is equivalent with the both sets $Q^{\bullet}$ and Q^{Δ}. Therefore, if $(Q;\mathcal{D};f)=\underline{Q}$ is a partial quasigroup and $S(\underline{Q})$ is the quasigroup obtained above, then Q and $S(\underline{Q})$ has the same cardinal number. This implies the following result:

THEOREM 3.1. Every infinite set is a carrier of a quasigroup. □

Note that if one starts by a partial groupoid $\underline{Q}=(Q;\mathcal{D};f)$ and forms the sequence of partial groupoids $(\underline{Q}_p \mid p \geq 0)$ such that $\underline{Q}_0=\underline{Q}$, $\underline{Q}_{p+1}=\underline{Q}_p^{\Delta}$, then one obtains that the union $S(\underline{Q})$ of this sequence is a groupoid which is a free extension of $\underline{Q}$. (Here, it is not necessary to assume that $n>m$.) In particular, if we assume that $\mathcal{D}=\emptyset$, then we obtain that $S(\underline{Q})$ is the free groupoid with a basis Q.

Now let Q be a nonempty set and let Φ be the family defined by

$$\Phi = \{(Q;\mathcal{D};f) \mid (Q;\mathcal{D};f) \text{ is a partial quasigroup}\}.$$

It is natural to define a partial ordering $\leq$ in Φ by:

$$(Q;\mathcal{D};f) \leq (Q;\mathcal{D}';f') \text{ iff } \mathcal{D}\subseteq\mathcal{D}' \text{ and } f \text{ is a restriction of } f'.$$

It is clear that the conditions of Zorn's lemma are satisfied. Therefore:

PROPOSITION 3.2. Every partial quasigroup on a set Q is a partial subgroupoid of a maximal partial quasigroup on Q. □

It is also clear that:

PROPOSITION 3.3. Every cancellative groupoid on Q is a maximal partial quasigroup on Q. □

PROPOSITION 3.4. A partial quasigroup $(Q;\mathcal{D};f)$ is maximal on Q iff for every $x\in Q^{(n)}\setminus\mathcal{D}$, $y\in Q^{(m)}$, there exist $a\in Q^{(k)}$, $u,v\in Q^{(m)}$ such that $x=au$, $av\in\mathcal{D}$, $f(av)=y$. □

4. FINITE FULLY COMMUTATIVE (n,m)-QUASIGROUPS

In this section we will assume that the set Q is finite with $q+1$ elements, i.e. that $Q=\{0,1,2,\ldots,q\}$ and also that n,m,k are given positive integers such that $n-m=k\geq 1$ and $m\geq 2$.

Note that the elements of the set $Q^{(r)}$ can be thaught of as monotone sequences (of r members) of the elements of Q, i.e. that

$$Q^{(r)} = \{a_1a_2\ldots a_r \mid a_\nu\in Q,\ 0\leq a_1\leq\ldots\leq a_r\leq q\}.$$

Therefore (see, for example, [1], III.1.6, p. 137):

PROPOSITION 4.1. If $|Q|=q+1$, then $|Q^{(r)}| = \binom{q+r}{r}$. □

The first question which commes naturally is the existence of (n,m)-quasigroups with the carrier Q.

By obvious reason we consider first the case $q=1$, i.e. $Q=\{0,1\}$.

Let $(Q;f)$ be an (n,m)-quasigroup. Then $\sigma: x\longmapsto f(0^kx)$ is a permutation of $Q^{(m)}$, and $f(0^{k-1}1^{m+1}) \neq f(0^{m+k-i}1^i)$, for every $i\in\mathbb{N}_m$. This implies that $f(0^{k-1}1^{m+1}) = f(0^{m+k})$. Similarly, if $k\geq 2$, we have:

$$f(0^{k-2}1^{m+2}) = f(0^{m+k-1}1),\ f(0^{k-3}1^{m+3}) = f(0^{m+k-2}1^2),$$

and more generally:

$$f(0^{k-i-1}1^{m+1+i}) = f(0^{m+k-j}1^j),$$

where $i\equiv j \pmod{m+1}$, $0\leq i\leq k-1$, $0\leq j\leq m$.

Conversely, let $\sigma: x\longmapsto\sigma(x)$ be a permutation of $Q^{(m)}$, and let an (n,m)-operation $f: Q^{(n)}\to Q^{(m)}$ be defined by:

$$f(0^kx) = \sigma(x) \text{ for every } x\in Q^{(m)}$$

$$f(0^{k-i-1}1^{m+1+i}) = \sigma(0^{m-j}1^j),$$

where i and j are as above. Then $(Q;f)$ is an (n,m)-quasigroup.

Thus, we have showed the following:

PROPOSITION 4.2. If $Q=\{0,1\}$, then there exist $(m+1)!$ (n,m)-quasigroups on Q. □

In the case $q \geq 2$, we have the following:

PROPOSITION 4.3. If $2 \leq q \leq m$, then there does not exist an (n,m)-quasigroup with $q+1$ elements.

Proof. Assume that $Q=\{0,1,2,\ldots,q\}$, and that $(Q;\mathcal{O};f)$ is a partial (n,m)-quasigroup such that $0^k x \in \mathcal{O}$ for every $x \in Q^{(m)}$, $u=0^{k-1}1^{m-q+1}2.3\ldots q \in \mathcal{O}$. Then $v=0^{k-1}1\ 2^{m-q+2}3\ldots q \notin \mathcal{O}$. Namely, if $v \in \mathcal{O}$ we would have $f(u) \neq f(0^k x)$, $f(v) \neq f(0^k x)$ for every $x \in Q^{(m)} \setminus \{0^m\}$, and this would imply $f(u)=f(0^m)=f(v)$, which is impossible, for $u=0^{k-1}1y$, $v=0^{k-1}1z$, and $y \neq z$. □

Thus, if $(Q;f)$ is an (n,m)-quasigroup with $q+1$ elements where $m \geq 2$, $q > 1$, it must be $q > m$.

EXAMPLE 4.4. Define a $(4,3)$operation on the set $Q=\{0,1,2,3,4\}$ as follows:

0) $f(0x) = x$, for every $x \in Q^{(3)}$

1.1) $f(1^2ij) = 0^2k$, $f(1i^2j) = 0k^2$, $f(1ij^2) = k^3$, where $\{i,j,k\}=\{2,3,4\}$, $i < j$;

1.2) $f(1^3i) = 0jk$, $f(1^2i^2) = j^2k$, $f(1i^3) = jk^2$, where $\{i,j,k\} = \{2,3,4\}$, $j < k$;

1.3) $f(1\,2\,3\,4) = 0^3$, $f(1^4) = 234$;

2.1) $f(2^3i) = 01j$, $f(2^2i^2) = i^2j$, $f(2i^3) = 1j^2$, where $i \neq j$;

2.2) $f(2^234) = 0^21$, $f(23^24) = 01^2$, $f(234^2) = 1^3$

$f(2^4) = 134$;

3) $f(3^34) = 012$, $f(3^34^2) = 1^22$, $f(34^3) = 12^2$

$f(3^4) = 124$;

4) $f(4^4) = 123$.

It is easy to show that $(Q;f)$ is a $(4,3)$-quasigroup.

More generally, it can be shown that:

PROPOSITION 4.5. If $Q=\{0,1,2,\ldots,q\}$, $q \geq 3$, then there exists a $(q,q-1)$-quasigroup. □

REFERENCES

[1] Aigner M.: *Kombinatorik I*, Springer-Verlag, Berlin, 1975

[2] Bruck R.: *A survay of binary systems*, Springer-Verlag, Berlin, 1958

[3] Čupona G., Ušan J., Stojaković Z.: *Multiquasigroups and some related structures*, Maced. Acad. Sci. and Arts, Contributions I 2 - Sect. math. tech. sc. (1980), 5-12

[4] Čupona G., Celakoski N., Markovski S., Dimovski D.: *Vector valued groupoids, semigroups and groups*, Maced. Acad. Sci. and Arts (in print)

PMF, p.f. 162
91000 Skopje
Yugoslavia

Mašinski fakultet
91000 Skopje
Yugoslavia

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

ON THE LEVITZKI RADICAL IN SOME NEAR-RINGS

Vučić Dašić

Abstract. In this note we consider some properties of locally nilpotent ideals and we prove some results about the Levitzki radical in near-rings with a defect of distributivity.

We first give some definitions. We recall that a (left-zero-symmetric) near-ring is a system $(R,+,.)$ where:

(i) $(R,+)$ is a (not necessarily abelian) group;

(ii) $(R,.)$ is a simigroup;

(iii) $x(y+z)=xy+xz$ for all x,y,z in R;

(iv) $ox=o$ for all x in R (o is the identity of $(R,+)$).

Let R be a near-ring and let $(S,.)$ be a multiplicative subsemigroup of $(R,.)$ whose elements generate $(R,+)$. Thus, every element $r \in R$ can be represented as a finite sum $\sum_i (\pm s_i)$, $(s_i \in S)$. The normal subgroup D of the group $(R,+)$ generated by the set

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

is called the defect of distributivity. It was proved in [1] that D is an ideal of R. If $S \subseteq R$ is a fixed subset of R, then we say that R is a near-ring with the defect D. If we wish to stress the set S, then we write (R,S). Thus, in the near-ring (R,S) with the defect D, for all $x,y \in R$ and $s \in S$ there exists $d \in D$ such that

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

Specially, if $D=o$ then R is a distributively generated (briefly d.g.) near-ring. Then every $s \in S$ becomes a distributive element in R. If $S=R$, then we say that R is a D-distributive near-ring and then for all x,y,z in R there exists $d \in D$ such that

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

If in this case $D=o$, then R becomes a distributive near-ring.

A right ideal B of R is a normal subgroup of (R,+), such that

$(x+b)y-xy \in B$ for all $x,y \in R$, $b \in B$.

An ideal A of R is a right ideal of R such that $ra \in A$ for all $r \in R$, $a \in A$.

We say that a near-ring R is locally nilpotent if for every finite subset H of R there exists a positive integer n=n(H), such that the product of every n elements from H is zero. An ideal of R is locally nilpotent if it is locally nilpotent as a near-ring. The sum of all locally nilpotent ideals of R is called the Levitzki radical L(R) of R. We say that R is semisimple if L(R)=0.

LEMMA 1. Let (R,S) be a near-ring with the defect of distributivity D which is contained in the intersection of all non zero normal subgroups of the group (R,+). Then the ideal of R generated by the set A R has the elements of the form:

$$\sum_i (r_i \pm a_i s_i \pm x_i a'_i \pm y_i a''_i s'_i + m_i a'''_i - r_i) \qquad (1)$$

($r_i, x_i, y_i \in R$, $s_i, s'_i \in S$, $a_i, a'_i, a''_i, a'''_i \in A$, m_i-integers).

Proof. By Proposition 3.1. of [1] the normal subgroup $\bar{A}$ generated by the subset AURAUASURAS has the elements of the above form. Since $D \subseteq \bar{A}$ it follows, by Corollary 1 of the Lemma 1.1. in [2], that the ideal of R generated by the subset A has the elements of the form (1).

THEOREM 1. Let (R,S) be a near-ring with the defect of distributivity D which is contained in the intersection of all nonzero normal subgroups of (R,+) and let A be an ideal of R which is distributively generated as a near-ring. If C is an ideal of R generated by an ideal B of A, then C B.

Proof. By Lemma 1, the ideal C has the elements of the form:

$$\sum_i (r_i \pm b_i s_i \pm x_i b'_i \pm y_i b''_i s'_i + m_i b'''_i - r_i)$$

($r_i, x_i, y_i \in R$, $s_i, s'_i \in S$, $b_i, b'_i, b''_i, b'''_i \in B$, m_i - integers). Since $C \subseteq A$, we have $C^3 \subseteq ACA = A(\sum_i (r_i \pm b_i s_i \pm x_i b'_i + y_i b''_i s_i + m_i b'''_i - r_i))A$. Thus, for all $x \in C^3$:

$$x = a_1(\sum_i (r_i \pm b_i s_i \pm x_i b'_i \pm y_i b''_i s_i + m_i b'''_i - r_i))a$$

$$x = \sum_i (a_1 r_i \pm a_1 b_i s_i \pm a_1 x_i b'_i \pm a_1 y_i b''_i s'_i + m_i a_1 b'''_i - a_1 r_i)a$$

$(a,a_1 \in A)$. But (A,S') is a d.g. near-ring for some subset $S' \subseteq A$ of distributive elements of A. Therefore, for each $a \in A$, $a = \sum_j (\pm s'_j)$ $(s'_j \in S')$ and we obtain:

$$x = \sum_i (a_1 r_i \pm a_1 b_i s_i \pm a_1 x_i b'_i \pm a_1 y_i b''_i s_i + m_1 a_1 b'''_i - a_1 r_i) \sum_j (\pm s'_j)$$

$$x = \sum_j (\pm \sum_i (a_1 r_i s'_j \pm a_1 b_i s_i s'_j \pm a_1 x_i b'_i s'_j \pm a_1 y_i b''_i s'_i s'_j + m_1 a_1 b'''_i s'_j - a_1 r_i s'_j))$$

Since $a_1 r_i s'_j \in A$, $a_1 b_i s_i s'_j \in B$, $a_1 x_i b'_i s'_j \in B$, $a_1 y_i b''_i s'_i s'_j \in B$, $m_1 a_1 b'''_i s'_j \in B$, it follows that $x \in B$ (Proposition 6.5, [4]). Hence $C^3 \subseteq B$.

If R is a d.g. near-ring, then D=o and we have the following

COROLLARY 1. Let R be a d.g. near-ring and A be an ideal of R which is distributively generated as a near-ring. If C is an ideal of R generated by an ideal B of A, then $C^3 \subseteq B$.

THEOREM 2. Let R be a near-ring with the defect of distributivity D which is contained in the intersection of all nonzero normal subgroups of (R,+) and let A be an ideal of R which is distributively generated as a near-ring. Then every ideal B of A such that A/B has no proper non-zero nilpotent ideals, is an ideal of R.

Proof. Let C be an ideal of R generated by the subset B. Thus $B \subseteq C \subseteq A$. On the other hand, by Theorem 1 $C^3 \subseteq B$. By hypothesis A/B has no non-zero nilpotent ideals and thus $C \subseteq B$, i.e. C=B.

COROLLARY 2. Let R be a d.g. near-ring and A be an ideal of R which is distributively generated as a near-ring. Then every ideal B of A such that A/B has no proper non-zero nilpotent ideals, is an ideal of R.

THEOREM 3. Let R be a near-ring with the defect D which is contained in the intersection of all normal nonzero subgroups os (R,+). If A is an ideal of R which is distributively generated as a near-ring, then L(A) is a locally nilpotent ideal of R and $L(A)=L(R) \cap A$.

Proof. Since L(A) is an locally nilpotent ideal of A, then by Theorem 2 L(A) is an loccaly nilpotent ideal of R. Thus, $L(A) \subseteq L(R) \cap A$. On the other hand, $L(R) \cap A$ is a locally nilpotent ideal in A, i.e. $L(R) \cap A \subseteq L(A)$. Hence $L(R) \cap A = L(R)$.

COROLLARY 3. Let R be a d.g. near-ring and A be an ideal of R which is distributively generated as a near-ring. Then L(A) is a locally nilpotent ideal of R and $L(A)=L(R)\cap A$.

THEOREM 4. Let R be a near-ring with the defect D and A be an ideal of R such that R/A is distributively generated. If B is an ideal of A such that $B\cap D=0$ and A/B is locally nilpotent, then D is a locally nilpotent ideal of R and R/L(R) is distributively generated.

Proof. Since R/A is distributively generated, it follows that $D\subseteq A$ (Corollary of Theorem 2.6. [1]). Thus D+B is an ideal in A. By the First isomorphism theorem we have

$$\frac{D+B}{B}\simeq\frac{D}{D\cap B}=\frac{D}{0}\simeq D$$

But $\frac{D+B}{B}$ is an ideal in A/B which is, by assumption, locally nilpotent and hence D is locally nilpotent. Consequently $D\subseteq L(R)$ and by Corollary of Theorem 2.6. of [1] , R/L(R) is d.g. near-ring.

COROLLARY 4. Let R be a near-ring with the defect $D\neq 0$ and A be an ideal of R such that R/A is distributively generated. If B is an ideal of A such that $B\cap D=0$ and A/B is locally nilpotent, then D is locally nilpotent and R can not be semisimple.

Proof. By Theorem 4,D is locally nilpotent and $D+L(R)=L(R)$ i.e. $L(R)\neq 0$.

LEMMA 2. If R is a D-distributive near-ring with identity, then the commutator subroup R' of (R,+) is contained in the defect D.

Proof. By Corollary 2 of Proposition 2.7 in [1] we have $R'R\subseteq D$ and $RR'\subseteq D$, Since R has an identity, it follows $R\subseteq D$.

THEOREM 5. If R is a D-distributive near-ring with identity, such that D as a near-ring is distributive then R/L(R) is a ring.

Proof. By Theorem 1 of [3] it follows $D^3=0$ and thus $D\subseteq L(R)$. According to Corollary of Theorem 2.6. in [1] , R/L(R) is distributively generated. From Lemma 2 $R'\subseteq D$ and the additive group of a factor near-ring R/L(R) is abelian. Hence R/L(R) is a ring (Proposition 6.6c. [4]).

REFERENCES

[1] V.Dašić, A defect of distributivity of the near-rings, Mathematica Balkanica 8:8(1978), 63-74.

[2] V.Dašić, On the radicals of near-rings with defect of distributivity, Publ. Inst.Math. (Beograd) 28(42) 1980, 51-59.

[3] V.Dašić, Some properties of D-distributive near-rings, Glasnik matematički, 18(38) 1983, 237-242.

[4] G.Pilz, Near-rings, North-Holland, Amsterdam 1983.

INSTITUT ZA MATEMATIKU I FIZIKU
Univerzitet u Titogradu
81000 Titograd
Jugoslavija

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

NONEXISTENCE OF CONTINUOUS (4,3)-GROUPS ON R

Dončo Dimovski and Kostadin Trenčevski

Abstract. In this paper we show that continuous (4,3)-groups on R do not exist.

0. Introduction. Let $m,n,k=n-m$ be positive integers. A set $G\neq\emptyset$ together with a map $[\ ]:G^n \to G^m$ is called an (n,m)-group if:

(1) $[[x_1^n]x_{n+1}^{n+k}] = [x_1^i[x_{i+1}^{i+n}]x_{i+n+1}^{n+k}]$ for each $1 \le i \le k$; and

(2) For given $a_1^k, b_1^k \in G^k$, $c_1^m \in G^m$, there exist $x_1^m, y_1^m \in G^m$ such that $[a_1^k\ x_1^m]=c_1^m=[y_1^m\ b_1^k]$ (see [1], where this notion was introduced). Above, x_1^t denotes the vector $(x_1,\ldots,x_t)\in G^t$, and $[x_1^n]$ denotes the image of x_1^n under the map $[\ ]$. We will denote by $\overset{t}{a}$ the vector $(a,a,\ldots,a)\in G^t$.

We say that $(G;[\ ])$ is a continuous (n,m)-group, if: G is a topological space; $(G;[\ ])$ is an (n,m)-group; and the map $[\ ]$ is continuous, where G^n, G^m are equiped with the product topology.

If $(G;[\ ])$ is a $(2m,m)$-group, then $(G^m,\bullet)$ where $x_1^m \bullet y_1^m = [x_1^m\ y_1^m]$, is a group with identity element $\overset{m}{e}$, for some $e\in G$ (see [2]). We say that e is the identity of the $(2m,m)$-group $(G;[\ ])$. A $(2m,m)$-group $(G;[\ ])$ is called a topological $(2m,m)$-group, if G is a topological space and $(G^m,\bullet)$ is a topological group.

If $(G;[\ ])$ is an $(m+1,m)$-group, then $(G;[\ ]')$ where $[x_1^{2m}]'=[x_1^{2m}]$, is a $(2m,m)$-group, induced by $(G;[\ ])$. So, if $(G;[\ ])$ is an $(m+1,m)$-group, then there exists an element $e\in G$, such that $[x_1^m\ \overset{m}{e}]=[\overset{m}{e}\ x_1^m]=x_1^m$, and moreover $[x\ \overset{m}{e}] = [\overset{m}{e}\ x]$

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

(see [3]). We say that an (m+1,m)-group is a topological (m+1,m)-group if its induced (2m,m)-group is a topological (2m,m)-group.

In [5] it was shown that continuous (3,2)-groups on R (where R is the set of the real numbers equiped with the usual topology) do not exist, but in [4] it was shown that topological (4,2)-groups on R do exist. The examples produced in [4] were obtained using Lie groups and Lie algebras.

In this paper we give an elementary proof that continuous (4,3)-groups on R do not exist. Also, we will give a sketch of a proof, that topological (4,3)-groups on R do not exist, using Lie groups and Lie algebras. Although the second result is a consequence of the first one, we include its proof, because of its method, which may be used for answering the existence question about topological (m+1,m)-groups for $m \geq 4$. Similar methods were used in [4].

1. Elementary algebraic results

We need several elementary results about (4,3)-groups, which are in fact, special cases of more general results about (m+1,m)-groups. Let $(G,[\ ])$ be a (4,3)-group, with identity element $e \in G$.

PROPOSITION 1. The following conditions are equivalent:

(1) $|G|=1$, i.e. G has only one element;

(2) $[x\,e\,e] = e$, for some $x \in G$;

(3) $[x\,y\,e] = e$, for some $x,y \in G$; and

(4) $[x\,y\,e] = [z\,e\,e]$, for some $x,y,z \in G$.

Proof. It is obvious that (1) $\Rightarrow$ (2), (1) $\Rightarrow$ (3) and (1) $\Rightarrow$ (4). If $[x\,e\,e] = e$ for some $x \in G$, then $xyz=[xyze]=[xe[eyz]]=[eyz]=[yze]=[yzxe]=yzx$, for each $y,z \in G$, implies that $|G|=1$; hence (2) $\Rightarrow$ (1). If $[xye]=e$ for some $x,y \in G$, then

$[xyxz]=[xy\overset{3}{e}xz]=[\overset{3}{e}xz]=[xz\overset{3}{e}]=[xzxy\overset{3}{e}]=[xzxy]$, for each $z\in G$, implies that $z=y$, i.e. $|G|=1$; hence (3) $\Longrightarrow$ (1). If $[xy\overset{3}{e}]=[z\overset{3}{e}]$ for some $x,y,z\in G$, then $xyz=[xyz\overset{3}{e}]=[xyxy\overset{3}{e}]=[xy\overset{3}{e}xy]=[z\overset{3}{e}xy]=zxy$, implies that $z=x$, and so, $[y\overset{3}{e}]=\overset{3}{e}$. Hence (4) $\Longrightarrow$ (2). ∎

For given $x,y\in G$, let $\alpha_x\beta_x\gamma_x$, $\alpha_{xy}\beta_{xy}\gamma_{xy}$ denote the vectors $[x\overset{3}{e}]$ and $[xy\overset{3}{e}]$ respectively.

PROPOSITION 2. The following conditions are equivalent:

(1) $|G|=1$;

(2) $\alpha_x = x$ or $\gamma_x = x$ for some $x\in G$;

(3) $\alpha_x = \gamma_y$ for some $x,y\in G$;

(4) $\alpha_{xy} = x$ or $\gamma_{xy} = y$ for some $x,y\in G$;

(5) $\alpha_x\beta_x = \beta_y\gamma_y$ for some $x,y\in G$;

(6) $\alpha_{xy}\beta_{xy} = \beta_{zt}\gamma_{zt}$ for some $x,y,z,t\in G$;

(7) $\alpha_x\beta_x = \alpha_{xy}\beta_{xy}$ or $\beta_x\gamma_x = \beta_{yx}\gamma_{yx}$ for some $x,y\in G$.

Proof. It is obvious that (1) $\Longrightarrow$ (k) for each $k=2,\ldots,7$. If $\alpha_x=x$ or $\gamma_x=x$, then $[\beta_x\ \gamma_x\ \overset{3}{e}]=\overset{3}{e}$ or $[\alpha_x\ \beta_x\ \overset{3}{e}]=\overset{3}{e}$, which implies that $|G|=1$, by P.1; hence (2) $\Longrightarrow$ (1). If $\alpha_x=\gamma_y$, then $\alpha_y\beta_y\ x = [\alpha_y\beta_y\ x\ \overset{3}{e}]=[\alpha_y\beta_y\alpha_x\beta_x\gamma_x]=[\alpha_y\beta_y\gamma_y\beta_x\gamma_x]=[y\ \overset{3}{e}\ \beta_x\gamma_x]=y\beta_x\gamma_x$, implies that $x=\gamma_x$; hence (3) $\Longrightarrow$ (2). If $\alpha_{xy}=x$ or $\gamma_{xy}=y$, then $[\beta_{xy}\gamma_{xy}\overset{3}{e}]=[y\overset{3}{e}]$ or $[\alpha_{xy}\beta_{xy}\overset{3}{e}]=[x\overset{3}{e}]$, which implies that $|G|=1$ by P.1; hence (4) $\Longrightarrow$ (1). If $\alpha_x\beta_x=\beta_y\gamma_y$, then $[\alpha_y\ x\ \overset{3}{e}]=[\alpha_y\alpha_x\beta_x\gamma_x]=$ $=[\alpha_y\beta_y\gamma_y\gamma_x]=[y\ \overset{3}{e}\ \gamma_x]=[y\ \gamma_x\ \overset{3}{e}]$ implies that $x=\gamma_x$; hence (5) $\Longrightarrow$ (2). If $\alpha_{xy}\beta_{xy}=\beta_{zt}\gamma_{zt}$, then $\alpha_{zt}\ x\ y=[\alpha_{zt}\ x\ y\ \overset{3}{e}]=$ $=[\alpha_{zt}\alpha_{xy}\beta_{xy}\gamma_{xy}]=[\alpha_{zt}\beta_{zt}\gamma_{zt}\gamma_{xy}]=[z\ t\ \overset{3}{e}\ \gamma_{xy}]=z\ t\ \gamma_{xy}$, implies that $y=\gamma_{xy}$; hence (6) $\Longrightarrow$ (4). If $\alpha_x\beta_x=\alpha_{xy}\beta_{xy}$, then $\alpha_{xy}\beta_{xy}\gamma_{xy}=$ $=[x\ y\ \overset{3}{e}]=[\overset{3}{e}\ x\ y]=[\alpha_x\beta_x\gamma_x\ y]=[\alpha_{xy}\beta_{xy}\gamma_x\ y]$ implies that $[\gamma_{xy}\ \overset{3}{e}]=[\gamma_x\ y\ \overset{3}{e}]$, which implies that $|G|=1$, by P.1; hence (7) $\Longrightarrow$ (1). ∎

PROPOSITION 3. The element $\alpha_e\beta_e\gamma_e$ is in the centre of the group $(G^3,\bullet)$ (where $xyz\bullet uvw=[xyzuvw]$), if and only if $|G|=1$.

Proof. If $\alpha_e\beta_e\gamma_e\bullet xyz = xyz\bullet\alpha_e\beta_e\gamma_e$ for each $xyz\in G^3$, then $[exyz]=[xyze]$ for each $x,y,z\in G$. For $x=e$, this implies $eyz=yze$ i.e. $y=z=e$; hence $|G|=1$. ∎

2. Nonexistence of continuous (4,3)-groups on R.

We start with the assumption that there is a continuous (4,3)-group on R, and denote it by $(R;[\ ])$. We denote by $[\ ]_1$, $[\ ]_2$, $[\ ]_3$ the components of $[\ ]$, i.e.

$$[xyzt] = [xyzt]_1[xyzt]_2[xyzt]_3.$$

Since $[\ ]$ is continuous, it follows that $[\ ]_i$, $i=1,2,3$, are also continuous. In the following several steps, the assumption that $(R;[\ ])$ is a continuous group will bring us to a contradiction.

Step 1. Let $\phi:R^3\to R$ be defined by $\phi(xyz)=[xyze]_1-x$. Since $[\ ]_1$ and $-$ are continuous, it follows that ϕ is also continuous.

Fact 1. $\phi^{-1}(0)\neq\emptyset$, i.e. there exists $xyz\in R^3$, such that $\phi(xyz)=0$, where 0 is the zero in R.

Proof. Consider $\phi(xee)=\alpha_x-x$, $\phi(\alpha_x\beta_x\gamma_x)=\alpha_{xe}-\alpha_x$ and $\phi(\alpha_{xe}\beta_{xe}\gamma_{xe})=x-\alpha_{xe}$. If $\phi(\alpha_x\beta_x\gamma_x)=0$, then $\phi^{-1}(0)\neq\emptyset$. So suppose that $\phi(\alpha_x\beta_x\gamma_x)\neq 0$. Since $|R|>1$, P.2. implies that $\phi(xee)\neq 0$ and $\phi(\alpha_{xe}\beta_{xe}\gamma_{xe})\neq 0$. It is not possible all of the α_x-x, $\alpha_{xe}-\alpha_x$, $x-\alpha_{xe}$ to have the same sign, since their sum is equal to 0. So, two of them have different signs. This, together with the facts that ϕ is continuous and R is connected, implies that $\phi^{-1}(0)\neq\emptyset$. ∎

Step 2. Let $c,a,b\in R$ be such that $\phi(cab)=0$, i.e. $[cabe]=cuv$ for some $u,v\in R$. This implies that $[ab^2e]=uve$, $[ab^3e]=[uv^2e]$

and $abe=[uve^3]$, i.e. $\alpha_{uv}=a$, $\beta_{uv}=b$, $\gamma_{uv}=e$. Now, let $\psi:R^2 \to R$ be defined by $\psi(xy)=[xye^2]_1-x$. Again, since $[\ ]_1$ and $-$ are continuous, it follows that ψ is continuous.

Fact 2. $\psi^{-1}(0)\neq\emptyset$, i.e. there exists $xy\in R^2$ such that $\psi(xy)=0$.

Proof. Consider $\psi(uv)=\alpha_{ab}-u$ and $\psi(ab)=u-a$. Since the map $\eta:R^2 \to R$ defined by $\eta(xy)=[xye^3]_1-x$ is continuous, $|R|>1$ and R is connected, P.2. implies that $\alpha_{xy}<x$ for each $x,y\in R$, or $\alpha_{xy}>x$ for each $x,y\in R$. If $u=a$, then $\psi^{-1}(0)\neq\emptyset$. If $u-a<0$, i.e. $u<a=\alpha_{uv}$, then $\alpha_{xy}>x$ for each $x,y\in R$. So $\alpha_{ab}-u>a-u>0$, i.e. $\psi(uv)>0$. This, together with $\psi(ab)<0$, implies that $\psi^{-1}(0)\neq\emptyset$. If $u-a>0$, i.e. $u>a=\alpha_{uv}$, then $\alpha_{xy}<x$ for each $x,y\in R$. So $\alpha_{ab}-u<a-u<0$, i.e. $\psi(uv)<0$. This, together with $\psi(ab)>0$, implies that $\psi^{-1}(0)\neq\emptyset$.

Step 3. Let $p,q\in R$ be such that $\psi(pq)=0$, i.e. $[pqe^2]=prs$ for some $r,s\in R$. This implies that $[rse^3]=qe^2$, i.e. $\beta_{rs}\gamma_{rs}=e^2$.

Step 4. Symmetrically, there exist $z,w\in R$ such that $\alpha_{zw}\beta_{zw}=e^2$. (When we say symmetrically, we mean: change $[xyze]_1-x$ in Step 1, by $[exyz]_3-z$ and $[xye^2]_1-x$ in Step 2, by $[e^2xy]_3-y$.)

Now, Step 3, Step 4 and P.2. imply that $|R|=1$, which is a contradiction.

3. The Lie groups and Lie algebras method

Now we will give a sketch of a proof, via Lie groups and Lie algebras, that topological (4,3)-groups on R do not exist. If $(R;[\ ])$ is a topological (4,3)-group, then $(R^3,\cdot)$ (where $xyz\cdot uvw=[xyzuvw]$) is a topological group. Using the positive answer to the Fifth Hilbert Problem [8] we obtain that $(R^3,\cdot)$ is a Lie group on R^3. The element $\alpha_e\beta_e\gamma_e\in R^3$ in this Lie group has the following properties: $(\alpha_e\beta_e\gamma_e)^3=\alpha_e\beta_e\gamma_e\cdot\alpha_e\beta_e\gamma_e\cdot\alpha_e\beta_e\gamma_e=e^3$; $\alpha_e\beta_e\gamma_e\neq e^3$; and $\alpha_e\beta_e\gamma_e$ is not in the centre of $(R^3,\cdot)$, by P.2 and P.3. We will prove that in arbitrary Lie group on R^3 there does not exist an element x satisfying these properties.

Suppose that $(R^3,*)$ is a Lie group, with the identity element e, and, $x \in R^3$ such that $x^3=e$, $x \neq e$ and x is not in the centre of $(R^3,*)$. The map $\psi: R^3 \to R^3$ defined by $\psi(y)=x*y*x^{-1}$ is an automorphism of R^3 of order 3, i.e. $\psi^3=id_{R^3}$ and $\psi \neq id_{R^3}$. Since R^3 is simply-connected manifold, there exists a bijection between the automotphisms of the Lie group and the automorphisms of its corresponding Lie algebra [6]. So, ψ corresponds to an automorphism, again denoted by ψ, of the corresponding Lie algebra on R^3, such that $\psi^3=id$ and $\psi \neq id$.

It is easy to check that if ψ is an autmorphism of a Lie algebra on R^3 of order 3, then there is a vector $X \in R^3$ such that X, $\psi(X)=Y$ and $\psi^2(X)=Z$ is a basis for the vector space R^3. Let the bracket on the Lie algebra be defined on X, Y by $[X,Y]=aX+bY+cZ$, for some $a,b,c \in R$. This implies that $[Y,Z]=cX+aY+bZ$, $[Z,X]=bX+cY+aZ$. The Jacobi identity implies that $(b-a)(a+b+c)=0$. So, the Lie algebras on R^3 with such an automorphism, can be classified into two classes:

Class 1, when a=b; and
Class 2, when a+b+c=0.

We will show that for each Lie algebra from these classes, which is a corresponding Lie algebra to a Lie group on R^3, in the Lie group there does not exist an element x such that $x \neq e$, $x^3=e$. This will complete the proof that topological (4,3)-groups on R do not exist, via this method.

If a=b=c=0, then the corresponding Lie group, up to isomorphism, is $(R^3,+)$ where + is the usual addition of vectors. So if $x^3=e$, then x=e.

Now, let $a^2+b^2+c^2 \neq 0$.

Case 1. Consider the Lie algebras from the class 1, i.e. when a=b. If $c \neq a$ and $c \neq -2a$, then each such Lie algebra is simple. It is known (see [7] p. 429) that there are only two

3-dimensional simple Lie groups up to a local isomorphism. So there are only two non-isomorphic simple Lie algebras on R^3. The following two Lie algebras:

1) a=b=1, c=0; and

2) a=b=0, c=1

on R are simple. They are not isomorphic, because the first one contains a 2-dimensional Lie subalgebra (generated by X and Y), and second does not, since in the second, the product-bracket is the usual vector-product on R^3. The second Lie algebra (i.e. a=b=0, c=1) is semisimple compact Lie algebra (see [7], p. 453). The Weyl's theorem ([7], p. 444), says that a connected Lie group with a semisimple compact Lie algebra must be compact. So there does not exist a Lie group on R^3 whose corresponding Lie algebra is isomorphic to the Lie algebra 2) i.e. a=b=0, c=1.

Next, we will give an example of a simple Lie group on a manifold homeomorphic to R^3, whose corresponding Lie algebra is isomorphic to the Lie algebra 1) i.e. a=b=1, c=0. Let $D=\{z\in C: |z|<1\}$ where C is the set of complex numbers, and $|\ |$ is the module. The map $z \to (1+z)/(1+\bar{z})$ from D into the set $\{z: z\in C, z\neq -1, |z|=1\}$ is continuous. Hence, for each $z\in D$, there is a unique $t\in(-\pi,\pi)$ such that $\exp(it)=(1+z)/(1+\bar{z})$, and we shall denote that number t by $(-i)\ln((1+z)/(1+\bar{z}))$. Define a binary operation on $R\times D$ by:

$$(x,u)\cdot(y,v)=(x+u+t,\frac{u+v(\exp(2iy))}{(\exp(2iy))+u\bar{v}}),$$

where $t=\frac{1}{2}(-i)\ln\frac{1+u\bar{v}(\exp(-2iy))}{1+\bar{u}v(\exp(2iy))}$. Then $(R\times D,\cdot)$ is a covering group for SL(2), and it is a semisimple Lie group (see [8], p.-417). In this group, $(x,u)^3=(0,0)$ implies $(x,u)=(0,0)$.

Now we consider the Lie algebras from Class 1, which are not simple. The Lie algebra for c=-2a, will be considered later as a Lie algebra from Class 2. So, we examine the Lie algebra for c=a, and hence a=b=c. The matrix group

$$G = \left\{ \begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix} : x,y,z \in R \right\}$$

can be considered as a Lie group on R^3. The corresponding Lie algebra is

$$\left\{ \begin{bmatrix} 0 & x & y \\ 0 & 0 & z \\ 0 & 0 & 0 \end{bmatrix} : x,y,z \in R \right\}$$

where $[A,B]=AB-BA$, and the map

$$\phi(X) = \begin{bmatrix} 0 & 1 & 1/a \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \quad \phi(Y) = \begin{bmatrix} 0 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, \quad \phi(Z) = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & 0 & 0 \end{bmatrix}$$

is an isomorphism between this Lie algebra and the Lie algebra for $a=b=c$. In the matrix group G, if

$$\begin{bmatrix} 1 & x & y \\ 0 & 1 & z \\ 0 & 0 & 1 \end{bmatrix}^3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \text{ then } x=y=z=0.$$

Case 2. Now consider the Lie algebras from Class 2, i.e. $a+b+c=0$. Let us suppose that the numbers $x,y,z,u,v,w \in R$, satisfy the conditions: $x+y+z=u+v+w=0$, $x^2+y^2+z^2 \neq 0 \neq u^2+v^2+w^2$ and $(x,y,z) \neq t(u,v,w)$. Then the vector product $(x,y,z) \times (u,v,w) = (t,t,t)$ for $t \neq 0$. It is easy to verify that the subspace U, of the Lie algebra for $a+b+c=0$, generated by the vector $xX+yY+zZ$ and $uX+vY+wZ$ is an invariant subalgebra. Moreover, it is a commutative Lie algebra. Suppose that Lie algebra for $a+b+c=0$, is a corresponding Lie algebra for a Lie group on R^3. Then, this Lie group contains a commutative connected 2-dimensional Lie subgroup H, whose corresponding Lie algebra is U (see [8]). Since R^3 is simply-connected, it follows that R^3/H is simply-connected Lie group (see [8], p. 255). Since $\dim(R^3/H)=1$, it follows that R^3/H is isomorphic to $(R,+)$. Let $x \in R^3$ such that $x^3=e$, and x is not in the centre of the Lie group on R^3. Then $(xH)^3=H$ and so $xH=H$, i.e. $x \in H$. Since H is a commutative subgroup, it follows that $\psi(z)=z$ for each $z \in H$, and hence $\psi(W)=W$ for each $W \in U$. Since $X+Y+Z \notin U$, and $\psi(X+Y+Z)=Y+Z+X=X+Y+Z$, it follows that $\psi=id$, hence $x=e$.

REFERENCES

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

[2] G.Čupona, D.Dimovski, On a class of vector valued groups, Proceedings of the Conf. "Algebra and Logic", Zagreb 1984, 29-37.

[3] D.Dimovski, Some existence conditions for vector valued groups, God. Zbor. Matem. fak. 33-34 (1982-1983), 99-103.

[4] K.Trenčevski,D.Dimovski, One-dimensional (4,2)-Lie groups, Vector valued semigroups and groups, Skopje, 1988, 91-102.

[5] K.Trenčevski, A note on non-existence for some classes of continuous (3,2)-groups, Proceedings of the Conf. "Algebra and Logic", Cetinje 1985,

[6] C.Chevalley, Theory of Lie groups, Princeton University Press, Princeton 1946.

[7] Л.С.Понтрягин, Непрерывные группы, Наука, Москва 1973.

[8] М.Постников, Группы и алгебры Ли, Наука, Москва 1982.

Institut za matematika
Prirodno-matematički fakultet
p.f. 162, 91000 Skopje
Yugoslavia

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

TWO COMMUTATIVITY THEOREMS FOR RINGS

Milan Janjić

Abstract. In this paper we prove two commutativity results for rings with identitety 1.

Throughout the present note, R will represent a ring with identity, N the set of nilpotent elements of R, C(R) the commutator ideal of R and Z(R) the center of R. As usual we shall denote $[x,y] = xy-yx$.

The first theorem that we shall prove is a generalisation of our recent result [4, Theorem 1.] . It also includes a result by Ming Lai Lin [6] .

We first state the following lemma which is easily to prove.

LEMMA 1. If R is a ring with identity 1 and $x,y \in R$ then

(i) $(x+1)^n y = x^n y = 0$ implies $y=0$,

(ii) if x commutes with $[x,y]$ then $[x^n,y] = nx^{n-1}[x,y]$,

for any $n \geq 1$.

THEOREM 1. Let R be a ring with identity 1. Suppose for any finite subset F of R there exists an integer $m=m(F)>1$ such that

---

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

(1) $(x+y)^m = x^m+y^m$, for every x,y of F.

Assume further for each x,y of F there exists an integer $n=n(x,y)\geqslant 1$, relatively prime to m, such that

(2) $x^s\left[x^n,y^n\right] = o$, for some $s=s(F)\geqslant o$.

Then R is commutative.

Proof. Note first that n, in (2), may be chosen that it depends not of each pair of elements of F, but of the whole subset F. For, it is enough to take $n=n(F)=\prod_{x,y\in F} n(x,y)$, applying Lemma 1. in [5]. Let $a\in N$ be arbitrary. Consider the set $F=\{1,a\}$. In the same way as in the proof of Theorem 1. [5] we conclude that

(3) $m^t a = o$, where $m=m(F)>1$ and $t\geqslant 1$.

We shall now prove that C(R) is a nil-ideal. To settle this it is enough to show that a prime ring without nonzero nil-ideals which satisfies the condition of our theorem must be commutative. Assume thus that R is a prime ring without nonzero nil-ideals. Let $a\in N$ and $x\in R$ be arbitrary. Take the set $F=\{1,1+a,a,x\}$. Let m,n and s be as in theorem. In view of (3) we have $m^t a=o$, for some integer $t\geqslant 1$. It is well-known fact that the caracteristic of a prime ring is either zero or a prime number $p\neq o$. If charac R=o we have a=o. If charac R=$p\neq o$ and $p\nmid m$ we also have a=o. Thus, in both cases we get a=o, that is, a belongs to Z(R). Assume now that charac R=$p\neq o$ and $p \mid m$. We want to prove that a lies in Z(R). We use the induction by the nilpotency index of a. If $a^2=o$ then (2) implies $(1+a)^s\left[(1+a)^n,x^n\right]=o$, that is, $n\left[a,x^n\right] = o$. Since $(m,n)=1$ and $p \mid m$ we deduce that $p\nmid n$ which yields $\left[a,x^n\right] = o$. Thus a belongs to the hyper-

center of R and by a result of Herstein [1] a belongs to Z(R). Let k be nilpotency index of a. Assume that each nilpotent element of R which nilpotency index is less then k lies in Z(R). It follows that elements $a^2, a^3, \ldots$ lie in Z(R) and in the same way as before from $(1+a)^s[(1+a)^n, x^n]=0$ we deduce that $a \in Z(R)$. We have thus proved that all nilpotent elements of R belong to Z(R). But there are no nilpotent elements in the center of a prime ring, hence R has no nilpotent elements. It follows that R has no zero-divisors and thus our condition (2) becomes $[x^n, y^n] = 0$. By the result of Herstein [2] we get that R is commutative. We have thus proved that $C(R) \subseteq N$.

Using the same arguments as in the proof of Theorem 1 [4] we may prove that nilpotent elements of R lie in Z(R). So we get

$$C(R) \subseteq N \subseteq Z(R).$$

For arbitrary x,y of R (2) and (3) imply

$$m^s[x,y] = x^s[x^n, y^n] = 0, \quad (m,n)=1, \quad s \geqslant 0.$$

It follows by Lemma 1.(ii) that

$$m^s[x,y] = n^2 x^{s+n-1} y^{n-1}[x,y] = 0.$$

Since $(m^s, n^2)=1$ this implies $x^K y^K [x,y] = 0$. Repeating the same by x+1 instead of x and using Lemma 1.(i) we get $y^N [x,y] = 0$, for some $N \geqslant 1$. Repeating the same by y+1 instead of y and using Lemma 1.(i) again we finally get $[x,y] = 0$, that is, R is commutative.

Next corollary extends a result of [6].

COROLLARY 1. Let R be a ring with 1. Suppose for any finite subset F of R there exist relatively prime integers $m=m(F)>1$

and $n=n(F)\geqslant 1$ such that

$$(x+y)^m = x^m+y^m,\ (xy)^n=x^ny^n \text{ and } (xy)^{n+1}=x^{n+1}y^{n+1},$$

for all x,y of F. Then R is commutative.

Proof. By our assumpotion we get $(xy)^{n+1}=xy(xy)^n=xyx^ny^n=$ $=x^{n+1}y^{n+1}$ which implies $x\left[x^n,y\right]y^n = o$. If we repeate the same by $y+1$ instead of y and use Lemma 1.(i) and Lemma 1. in [5] we get $x^n\left[x^n,y^n\right] = o$. Hence R is commutative by Theorem 1.

THEOREM 2. Let R be a ring with 1. Suppose for any subst F of R containing three elements there exist relatively prime integers $m=m(F)\geqslant 1$, $n=n(F)\geqslant 1$ and two integers $k=k(F)\geqslant o$ and $r=r(F)\geqslant o$ such that

$$x^k\left[x,y^m\right]y^r = o = \left[x,(xy)^n\right] \text{ for all } x,y \text{ of } F.$$

Then R is commutative.

Proof. If $a\in N$ and $x\in R$ take $F = \left\{1+a,x,(1+a)^{-1}x\right\}$. By our hipothesis there exist integers $m=m(F)\geqslant 1$, $n=n(F)\geqslant 1$, $(m,n)=1$ and integers $k=k(F)\geqslant o$, $r=r(F)\geqslant o$ such that

$$(1+a)^k\left[a,x^m\right]x^r = o=\left[a,\left\{(1+a)(1+a)^{-1}x\right\}^n\right]=\left[a,x^n\right].$$

Since $1+a$ is invertible we have

$$\left[a,x^m\right]x^r = o =\left[a,x^n\right].$$

Being $(m,n)=1$ from this we easily conclude that

$$\left[a,x\right]x^N=o, \text{ for some } N\geqslant 1.$$

Repeating the same by $x+1$ instead of x and using Lemma 1.(i) we get $\left[a,x\right] = o$, that is, $N\subseteq Z(R)$. Theorem 2 [3] implies that the commutator ideal $C(R)$ is a nil-ideal. We have thus shown that

$$C(R)\subseteq N\subseteq Z(R).$$

For each integer $n\geqslant 1$ the element $x^ny^n-(xy)^n$ belongs to $C(R)$

that is, lies in Z(R). It follows that the condition $[x,(xy)^n] = o$ implies the condition $x^n[x,y^n] = o$. Thus for each x,y of R we have

$$x^k[x,y^m]y^r = o = x^n[x,y^n] = o, \quad (m,n)=1.$$

Using Lemma 1.(ii) this implies

$$mx^k y^{r+m-1}[x,y] = o = nx^n y^{n-1}[x,y] .$$

As in the proof of the above theorem we get that R is commutative.

The following corollary extends a result by Chen Te Yen [7].

COROLLARY 2. Let R be a ring with 1. Assume for any subset F of R containing three elements there exist relatively prime positive integers $m=m(F)$ and $n=n(F)$ such that $(xy)^m = x^m y^m$, $(xy)^{m+1} = x^{m+1}y^{m+1}$ and $[x,(xy)^n] = o$, for all $x,y \in F$. Then R is commutative.

Proof. We have seen that first two condition imply $x[x^m,y]y^m = o$, and R is commutative by Theorem 2.

REFERENCES

1.I.N.Herstein, On the hypercenter of a ring, J.Algebra 36(1975), 151-157

2. I.N.Herstein, A commutativity theorem, J.Algebra 38 (1976), 112-118

3.M.Janjić, Some commutativity results for rings, Radovi matematički Vol.2 (1986), 241-246

4.M.Janjić, A note on commutativity of rings,(to appear in Radovi matematički)

5.M.Janjić and E.Psomopoulos, Commutativity of n-torsion free rings with commuting powers,(to appear in Results in Math.)

6.M.L.Lin, A commutativity theorem for ring, Math.Japon. 26 (1981), no. 4, 375-376

7.C.T.Yen, On the commutativity of rings and cancellative semigroups, Chinese J.Math. 11 (1983), no2, 99-113

Milan Janjić, Mašinski fakultet, Sarajevo
Omladinsko šetalište bb, 71ooo Sarajevo
Yuçoslavia

AUTOMORPHIC SETS OR LEFT DISTRIBUTIVE LEFT QUASIGROUPS

Aleksandar Lipkovski

Abstract. The groupoids which satisfy the left distributivity and left quasigroup laws (that is, all left translations are automorphisms) arise naturally in some geometrical situations as noted by E.Brieskorn. In this paper some elementary properties of such groupoids are presented, with intention to raise interest for this structure among algebraists, in order to develop a general theory of these groupoids.

The theory of distributive quasigroups (groupoids with properties 1.each equation $ax = b$ and $xa = b$ has a unique solution and 2.$a(bc) = (ab)(ac)$ and $(ab)c = (ac)(bc)$ for all a,b,c), is a well developed algebraic theory (see [1]). As an example on an affine space over a field of char $\neq 2$ the operation $ab =$ arithmetic mean of a,b satisfies these properties.
However, according to [2], the interesting structure from a geometrical point of view is defined by the (one-sided) half of these properties: left distributive left quasigroups in standard terms or automorphic sets as in [2]. Here the shorter name is preferred. For the sake of completeness, some facts from [2] are incorporated in the folowing.

DEFINITION. Groupoid $(X,*)$ is an A-set if
A1. each equation $a*x = b$ has a unique solution (left quasigroup property),
A2. $a*(b*c) = (a*b)*(a*c)$ for all a,b,c (left distributivity).

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

A morphism of A-sets or simply A-morphism is a homomorphism of groupoids and we have a category $\mathcal{A}$ of A-sets as a full subcategory of the category of groupoids, with usual notions of isomorphism, A-subset etc. The set of all automorphisms of an A-set X is denoted Aut(X). For $a \in X$ the mappings $l_a : x \mapsto a*x$ and $r_a : x \mapsto x*a$ are left and right translations respectively. Denote $L(X) = \{ l_a \mid a \in X \}$, $R(X) = \{ r_a \mid a \in X \}$. Define $r_\alpha * r_\beta$ as the function $x \mapsto r_\alpha(x) * r_\beta(x)$.

PROPOSITION 1. *If* $(X, *)$ *is an A-set, then* $(R(X), *)$ *is an A-set and the mapping* $a \mapsto r_a$ *is an A-isomorphism* $X \cong R(X)$.

Proof. Obviously $r_a = r_b \Rightarrow a = b$ (A1) and $r_\alpha * r_\beta = r_{\alpha * \beta}$ (A2) □

PROPOSITION 2. *The groupoid* $(X, *)$ *is an A-set* $\Leftrightarrow L(X) \subset Aut(X)$.

Proof. Obviously A1 $\Leftrightarrow \forall a$, l_a is a bijection and A2 $\Leftrightarrow \forall a$, l_a is an A-morphism. □

This has justified the term "automorphic set". In general the set L(X) is not closed under composition nor under $*$ if we define it as for R(X).

DEFINITION. *For an A-set* X *let* I(X) *be the subgroup of* Aut(X) *generated by* L(X),

PROPOSITION 3. I(X) *is a normal subgroup of* Aut(X).

Proof. For $f \in Aut(X)$ we have $f \cdot l_a \cdot f^{-1} = l_{f(a)}$. □

Let us look at some examples of A-sets.

Example 1. Any set X becomes an A-set if we define $a*b = b$. This is the trivial A-structure on X.

Example 2. The trivial structure admits modification. If we try to define $a*b = \sigma(b)$ to be independent from a, where $\sigma : X \to X$ is a function, then we get an A-set $\Leftrightarrow \sigma$ is a bijection. Therefore for each permutation $\sigma \in S(X)$ we have an A-structure denoted by X_σ. X_σ is trivial $\Leftrightarrow \sigma = id$. The group $I(X_\sigma) = \langle \sigma \rangle$ is the cyclic subgroup of $Aut(X_\sigma)$ generated by σ.

Example 3. If G is a group, define $a*b = aba^{-1}$ (the action of inner automorphisms). Then $(G,*)$ is an A-set denoted by G^*. G^* is trivial $\Leftrightarrow$ G is commutative. All elements of G^* are idempotent, elements of the centre Z(G) are left units in G^*. The group $I(G^*) = L(G^*) = Inn(G)$ is the group of inner automorphisms of G. Any group homomorphism $h:G \to H$ defines an A-morphism $h^*:G^* \to H^*$. It is easy to see that in this way we have a functor $Gp \to \mathcal{A}l$.

PROPOSITION 4. (a) $X_\sigma \cong G^*$ for some group structure G on X $\Leftrightarrow$ $\Leftrightarrow$ the A-structure is trivial.
(b) $X_\sigma \cong X_\tau \Leftrightarrow \sigma$ and τ are conjugated in the group S(X).

Proof. (a) If $f:G^* \to X_\sigma$ is an isomorphism, $f(x) = f(e*x) = f(e)*f(x) = \sigma f(x)$ where e is the unit of G.
(b) For $f \in S(X)$, $f\sigma = \tau f \Leftrightarrow f(a*b) = f\sigma(b) = \tau f(b) = f(a)*f(b) \Leftrightarrow$ $\Leftrightarrow$ f is an A-isomorphism $X_\sigma \cong X_\tau$. □

Therefore, examples 2 and 3 define different classes of A-sets and example 2 defines many A-structures on X, their number for finite X equals the number of conjugacy classes in S(X).

There is a canonical A-morphism $X \to I(X)^*$, $a \mapsto l_a$, since we have $l_{a*b} = l_a l_b l_a^{-1} = l_a * l_b$ (Prop.3). Is the correspondence $X \mapsto I(X)$ functorial? The answer is only partly positive.

PROPOSITION 5. If $f:X \to Y$ is an A-epimorphism, then the map $L(X) \to L(Y)$, $l_a \mapsto l_{f(a)}$ extends to a group epimorphism $f_*:I(X) \to I(Y)$. This correspondence is functorial ($id_* = id$, $(fg)_* = f_* g_*$) and the diagram of A-morphisms

$$\begin{array}{ccc} X & \xrightarrow{f} & Y \\ \downarrow & & \downarrow \\ I(X)^* & \longrightarrow & I(Y)^* \end{array}$$

commutes. If f is an isomorphism, so is f_*.

Proof. If $a*b = x$ then $f(a)*f(b) = f(x)$. Therefore, $f(l_a^{-1}(x)) = l_{f(a)}^{-1}(f(x))$ and we have $l_{a_1}^{\varepsilon_1} \ldots l_{a_k}^{\varepsilon_k} = id \Rightarrow l_{f(a_1)}^{\varepsilon_1} \ldots l_{f(a_k)}^{\varepsilon_k}(f(x)) = f(x)$ for all x. But f is epi and $l_{f(a_1)}^{\varepsilon_1} \ldots l_{f(a_k)}^{\varepsilon_k} = id$. The rest is trivial. □

Remark 1. This does not hold for arbitrary A-morphisms as the simple example shows. Let e be an idempotent of Y and $f: x \mapsto e$. Then f is an A-morphism, but $f_* = \text{const}$ and it may not admit extension to I(X): let X and Y be as in Prop.12 3. and 2. respectively. Then $I(X) \cong \mathbb{Z}_3$, $I(Y) \cong \mathbb{Z}_2$ and there is an 1_a of order 3 which is sent to $1_{f(a)}$ of order 2.

Remark 2. If two group structures G, H define isomorphic A-structures on a set X, then $\mathrm{Inn}(G) \cong \mathrm{Inn}(H)$.

Example 4 (from [2]). If G is an abelian group and $f: G \to G$ its automorphism, the formula $a*b = a - f(a) + f(b)$ defines an A-structure on G, denoted by G(f). Obviously, G(id) is trivial and $G(f) \cong G_\sigma$ for some $\sigma \Leftrightarrow f = \mathrm{id}$ and $\sigma = \mathrm{id}$.

Example 5 (from [2]). Let V be an Euclidian space with scalar product $(-,-)$ and $s_a: V \to V$ the reflection of V with respect to the hyperplane orthogonal to $a \in V \setminus \{0\}$. Obviously, $s_a(x) = x - 2 \cdot \frac{(x,a)}{(a,a)} \cdot a$ and the product $a*b = s_a(b)$ defines an A-structure on $V \setminus \{0\}$. If $R \subset V \setminus \{0\}$ is a finite subset with the properties $s_a(R) \subset R$ for all $a \in R$ and $s_a(b) - b \in \mathbb{Z}a$ for all $a, b \in R$ then R is an A-subset of $V \setminus \{0\}$ and it is in fact a root system in V (see [3] Ch.VI) and vice versa. The group I(R) is exactly the Weyl group W(R) of the root system R, generated by the reflections s_a.

Remark. From the point of view of [2], the main importance of A-sets comes from this example and from the folowing. The braid group B_n with n strings is the group with presentation $B_n = \langle \sigma_1, \dots, \sigma_{n-1} \mid \sigma_i \sigma_j = \sigma_j \sigma_i \ (|i-j| \geq 2),\ \sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j \ (|i-j| = 1) \rangle$. The group B_n acts on the set of all free bases of the free group F_n of rank n by the formula
$\sigma_i(x_1, \dots, x_n) = (x_1, \dots, x_{i-1}, x_i x_{i+1} x_i^{-1}, x_i, x_{i+2}, \dots, x_n)$.
However, it is not the group structure of F_n which is responsible for this action, but the A-structure F_n^*: the relation $\sigma_i \sigma_j \sigma_i = \sigma_j \sigma_i \sigma_j$ implies the left distributivity. Moreover, it can be easily seen that for any A-set X, B_n canonically operates on X^n by means of the same formula.

Let X be an A-set. There is an important automorphism of X.

DEFINITION. For $a \in X$ let $i(a) = \bar{a}$ be the unique element of X such that $a*i(a) = a$.

PROPOSITION 6 (see [2]). (a) $\overline{a*b} = a*\bar{b} = \bar{a}*\bar{b}$;
(b) $i: X \to X$ is a central automorphism of X with the inverse $j: X \to X$, $a \mapsto a*a$;
(c) $l_a = l_{\bar{a}} = l_{a*a}$.

Proof. (a) $(a*b)*(a*\bar{b}) = a*(b*\bar{b}) = a*b \Rightarrow \overline{a*b} = a*\bar{b}$,
$a*(\bar{a}*\bar{b}) = (a*\bar{a})*(a*\bar{b}) = a*(a*\bar{b}) \Rightarrow \bar{a}*\bar{b} = a*\bar{b}$;
(b) $ij(a) = \overline{a*a} = a*\bar{a} = a$ and $ji(a) = \bar{a}*\bar{a} = a*\bar{a} = a$;
(c) is a trivial consequence. For $f \in \mathrm{Aut}(X)$, $fj = jf$ and $fi = if$. □

We see that in an A-set we have $(a*b)*(a*b) = (a*a)*(b*b)$ and the medial law (see [1]) holds for two-element subsets. An element $a \in X$ is idempotent if $i(a) = a$. In the case of distributive groupoids, the set of idempotents Id(X) helps to decompose X in a subdirect product. Here this is not possible since Id(X) is not a (both-sided) ideal.

PROPOSITION 7. (a) $a*b$ is idempotent $\Leftrightarrow$ b is idempotent;
(b) Id(X) is a left prime ideal in X;
(c) $Y = X \setminus \mathrm{Id}(X)$ is empty or an A-subset with at least two elements and $i|_Y : Y \to Y$ its automorphism.

Proof. Trivial, use the two-element medial law. □

In the example 3, the elements of the centre Z(G) are left units in G^*, and its complement is an A-subset. The same is true in the general case.

PROPOSITION 8. Let $U = U(X)$ be the set of all left units in X.
(a) $a, b \in U \Rightarrow a*b \in U$;
(b) $a*b \in U \Rightarrow b \in U$;
(c) $a \in U \Leftrightarrow \bar{a} \in U$;
(d) The sets U and $X \setminus U$ are A-subsets in X and restrictions $i|_U$ and $i|_{X \setminus U}$ are automorphisms of U and $X \setminus U$ respectively.

Proof. Note that $a \in U \Leftrightarrow l_a = \mathrm{id}$ and use Prop.6. □

Remark. Converse of (b) does not hold (see Prop.12.4).

As we see, the subdirect product seems not to be the right notion of decomposition for A-sets. The theory of root systems helps to find the right one. The root systems decompose in direct sums of orthogonal components.

DEFINITION (see [2]). In an A-set X, $a \perp b \Leftrightarrow a*b=b$ and $b*a=a$. X is a disjoint sum of its A-subsets X_1 and X_2 (notation $X=X_1 \sqcup X_2$) if $X=X_1 \cup X_2$, $X_1 \cap X_2 = \emptyset$ and $X_1 \perp X_2$.
X is irreducible if it is not a disjoint sum of its A-subsets.

PROPOSITION 9 (see [2]2.1). Every A-set X decomposes uniquely in the disjoint sum of its irreducible A-subsets.

Proof. Define the equivalence relation $\sim$ on X as a minimal transitive closure of the complement of the relation $\perp$. Then it is easy to see that the equivalence classes of $\sim$ are exactly the irreducible A-subsets of X. □

PROPOSITION 10. (a) Let $X=X_\sigma$ for some $\sigma \in S(X)$. Then X is irreducible $\Leftrightarrow \sigma \neq id$.
(b) Let $X=G^*$ for some group G. Then X is reducible and $X = \sqcup\{a \mid a \in Z(G)\} \sqcup (G \setminus Z(G))$.

Proof. (a) Obviously, $a \perp b \Leftrightarrow \sigma|_{\{a,b\}}=id$. Therefore, $X=X_1 \sqcup X_2$ implies $\sigma|_{X_1 \cup X_2} \neq \sigma = id$. □
(b) We need only to show that $Z(G) \perp G \setminus Z(G)$. This is trivial since $a \perp b \Leftrightarrow$ a and b commute in the group G. □

Remark. In the general case, U(X) and $X \setminus U(X)$ need not be orthogonal (see Prop.12.4).

It is known that the Weyl group of the direct sum of two root systems is the product of the corresponding groups. Does the analogue hold for A-sets? The answer is positive.

PROPOSITION 11. If $X=X_1 \sqcup X_2$, then $I(X) \cong I(X_1) \times I(X_2)$.

Proof. Since $X_1 \perp X_2$, for all $x_i \in X_i$ $(i=1,2)$ we have $1_{x_1} \cdot 1_{x_2} = 1_{x_2} \cdot 1_{x_1}$. It is easy to see that the correspondence $(1_{x_1}, 1_{x_2}) \mapsto 1_{x_1} \cdot 1_{x_2}$ defines an isomorphism. □

Remark. Converse does not hold: if $\sigma = (12)(345)$ is a permutation of order 6 then for $X = \{1,2,3,4,5\}$ we have $I(X_\sigma) \cong \mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$ but X_σ is irreducible according to Prop.10.

At the end, we may look at the small finite A-sets. For the set $X = \{1,2\}$ there are exactly two nonisomorphic A-structures: the trivial $X_{id} = \mathbb{Z}_2^* = \{1\} \cup \{2\}$ with $I(X)$ trivial and $\mathrm{Aut}(X) \cong \mathbb{Z}_2$ and the irreducible X_τ, $\tau = (12) \in S_2$, corresponding also to the root system A_2 ←—•—→ , with $I(X) = \mathrm{Aut}(X) \cong \mathbb{Z}_2$. Their multiplication tables are

τ	1	2
1	1	2
2	1	2

and

$*$	1	2
1	2	1
2	2	1

.

PROPOSITION 12. Let $X = \{1,2,3\}$ be the three-element set. There are exactly 6 nonisomorphic A-structures on X:

1. the trivial $X_{id} = \mathbb{Z}_3^* = \{1\} \cup \{2\} \cup \{3\}$, $I(X)$ trivial, $\mathrm{Aut}(X) \cong S_3$;
2. X_τ, $\tau = (23) \in S_3$, irreducible, $I(X) = \mathrm{Aut}(X) \cong \mathbb{Z}_2$;
3. X_σ, $\sigma = (1,2,3) \in S_3$, irreducible, $I(X) = \mathrm{Aut}(X) \cong \mathbb{Z}_3$;
4. Irreducible with $I(X) = \mathrm{Aut}(X) \cong \mathbb{Z}_2$;
5. Reducible $X = \{1\} \cup \{2,3\}$ with $I(X) = \mathrm{Aut}(X) \cong \mathbb{Z}_2$;
6. $X = \mathbb{Z}_3(f)$ with $f: \mathbb{Z}_3 \to \mathbb{Z}_3$, $f(x) = 2x$, irreducible, $I(X) = \mathrm{Aut}(X) \cong S_3$.

Their multiplication tables are as following:

1.
1	2	3
1	2	3
1	2	3

2.
1	3	2
1	3	2
1	3	2

3.
2	3	1
2	3	1
2	3	1

4.
1	2	3
1	2	3
2	1	3

5.
1	2	3
1	3	2
1	3	2

6.
1	3	2
3	2	1
2	1	3

where the heading rows and columns are omited.

Proof consists of straightforward enumeration with the help of heuristics such as Prop.6(c) and similar. □

We see that, as one should expect, already in this case we have irreducible A-sets which do not belong to any of the types mentioned.

Finally, I wish to thank M.Polonijo for pointing out the book [1] to me. I hope that this elementary notes may help to stimulate the development of the structure theory of A-sets or left distributive left quasigroups in the purely algebraic context.

REFERENCES

1. J.Ježek, T.Kepka, P.Němec, Distributive groupoids, Rozpravy Československé Akademie Věd 3(1981), 1-94.

2. E.Brieskorn, Automorphic sets and braids and singularities, Lecture on the Conference on Artin's braid groups, University of California, Santa Cruz, 1986.

3. N.Burbaki, Gruppy i algebry Li, IV-VI, Mir, Moskva 1972.

University of Belgrade
Mathematical faculty
Studentski trg 16
11000 Beograd, Yugoslavia

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

ON BIPLANES OF ORDER 14

Alija Mandak

Abstract: The number 14 is the smallest one that can be the order of a biplane, but still it is not known whether such a biplane exists. Here we show that such a biplane does not admit a colineation of order 13.

A biplane with parameters (v, k, λ) is a set P of v points and a family B of v subsets of P (every such subset is called a line or a block) which satisfy the following conditions: i) every line contains exactly k points; ii) any two distinct points are joined by exactly 2 lines. The order of a biplane is $n=k-2$. A biplane of order $n=16-2=14$ has parameters (121, 16, 2) which satisfy the number-theoretic conditions of the Bruck, Chowla, Ryser theorem (see [3], p.100).

A colineation of a biplane D is a one-to-one correspondence taking P to P and B to B and preserving the incidence, that is, $P \in l$ if and only if $P^{\varphi} \in l^{\varphi}$. The set of all colineations of a given biplane D forms a group which is called the full colineation group of D and denoted by G(D). A colineation φ of order 13 of a biplane D of order 14 satisfies the condition of the fundamental theorem Aschbacher (see [2], p. 274). In this paper we prove the following result.

THEOREM. A biplane D of order 14 does not admit a colineation φ of order 13.

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

Proof. Let D be a biplane of order 14 which admits a collineation ϱ of order 13. Here ϱ acts on the set P of 121 points and set B of 121 lines. Since $121 = 9 \cdot 13 + 4$ it follows that ϱ has exactly four fixed points (four point-orbits of the length 1) and exactly nine point-orbits of the length 13. We may put

$$\varrho = (\infty_1)(\infty_2)(\infty_3)(\infty_4)(1_0 1_1 \dots 1_{12})(2_0 2_1 \dots 2_{12}) \dots (9_0 9_1 \dots 9_{12})$$

where $\infty_1, \infty_2, \infty_3, \infty_4, 1_0, 1_1, \dots 1_{12}, \dots, 9_0, 9_1, \dots 9_{12}$ are all 121 points of D. The orbit structure of lines is the same. We use permutation (1 2 3 4 5 6 7 8 9) of orbit numbers and (whithout a loss of generality) for the four lines fixed by ϱ we can put

$$f_1 = \infty_1\ \infty_2\ \infty_3\ 1_0\ 1_1\ 1_2\ 1_3\ 1_4\ 1_5\ 1_6\ 1_7\ 1_8\ 1_9\ 1_{10}\ 1_{11}\ 1_{12}$$
$$f_2 = \infty_1\ \infty_2\ \infty_4\ 2_0\ 2_1\ 2_2\ 2_3\ 2_4\ 2_5\ 2_6\ 2_7\ 2_8\ 2_9\ 2_{10}\ 2_{11}\ 2_{12}$$
$$f_3 = \infty_1\ \infty_3\ \infty_4\ 3_0\ 3_1\ 3_2\ 3_3\ 3_4\ 3_5\ 3_6\ 3_7\ 3_8\ 3_9\ 3_{10}\ 3_{11}\ 3_{12}$$
$$f_4 = \infty_2\ \infty_3\ \infty_4\ 4_0\ 4_1\ 4_2\ 4_3\ 4_4\ 4_5\ 4_6\ 4_7\ 4_8\ 4_9\ 4_{10}\ 4_{11}\ 4_{12}$$

There are exactly 9 line-orbits of the length 13 which are represented by lines $l_1, l_2, \dots, l_9$. In construction of these lines we omit the indexes 0, 1, 2, ..., 12, and write only orbit numbers 1, 2, 3, ... 9. Let l_1, l_2, l_3, l_4 contain $\infty_1, \infty_2, \infty_3, \infty_4$, respectively, so that we can take:

$$l_1 = \infty_1 m_{11} m_{12} m_{13} m_{14} m_{15} m_{16} m_{17} m_{18} m_{19}$$
$$l_2 = \infty_2 m_{21} m_{22} m_{23} m_{24} m_{25} m_{26} m_{27} m_{28} m_{29}$$
$$l_3 = \infty_3 m_{31} m_{32} m_{33} m_{34} m_{35} m_{36} m_{37} m_{38} m_{39}$$
$$l_4 = \infty_4 m_{41} m_{42} m_{43} m_{44} m_{45} m_{46} m_{47} m_{48} m_{49}$$

where m_{ij} is the multiplicity with which the line l_i contains the orbit number j. Since l_i, $i=1, 2, 3, 4$ contains 16 points it follows

$$1 + \sum_{j=1}^{9} m_{ij} = 16 \qquad i = 1, 2, 3, 4 \qquad (1)$$

Since $|l_i \cap l_i \varrho^k| = 2$, $i = 1, 2, 3, 4$, $k = 1, \dots, 12$, we have

$$\sum_{j=1}^{9} m_{ij}(m_{ij}-1) = (\varrho-1)(\lambda-1) = 12 \qquad (2)$$

Therefore the fact that $|l_i \cap l_s \varrho^k| = 1$, $i \neq s$, $i, s = 1,2,3,4$ implies

$$\sum_{j=1}^{9} m_{ij}\, m_{sj} = \rho(\lambda-1) = 13 \qquad (3)$$

Only for line l_1 we may assume that

$$m_{11} \leq m_{12} \leq m_{13} \leq \dots \leq m_{19} \qquad (4)$$

Since $|l_i \cap f_j| = 2$, $i, j = 1, 2, 3, 4$ we have

$m_{11}=m_{12}=m_{13}=m_{21}=m_{22}=m_{24}=m_{31}=m_{33}=m_{34}=m_{42}=m_{43}=m_{44}=1$, $m_{14}=m_{23}=m_{32}=m_{41}=2$

The conditions (1),(2),(3),(4) give the following unique solution for lines l_1 , l_2 , l_3 , l_4 :

$$l_1 = \omega_1\ 1\ 1\ 1\ 2\ 2\ 2\ 2\ 2\ 2$$
$$l_2 = \omega_2\ 1\ 1\ 2\ 1\ 2\ 2\ 2\ 2\ 2$$
$$l_3 = \omega_3\ 1\ 2\ 1\ 1\ 2\ 2\ 2\ 2\ 2$$
$$l_4 = \omega_4\ 2\ 1\ 1\ 1\ 2\ 2\ 2\ 2\ 2$$

For the next representative line l_5 we may put

$$l_5 = 2\ 2\ 2\ 2\ m_{55}\ m_{56}\ m_{57}\ m_{58}\ m_{59}$$

where we have

$$2+2+2+2+m_{55}+m_{56}+m_{57}+m_{58}+m_{59} = 16$$

Since $|l_5 \cap l_i \rho^k| = 2$, $|l_5 \cap l_5 \rho^k| = 2$, $i = 1, 2, 3, 4$,

we have

$$2\cdot1+2\cdot1+2\cdot1+2\cdot2+2\cdot m_{55}+2\cdot m_{56}+2\cdot m_{57}+2\cdot m_{58}+2\cdot m_{59} = \rho\lambda = 26$$

$$2(2-1)+2(2-1)+2(2-1)+2(2-1)+m_{55}(m_{55}-1)+m_{56}(m_{56}-1)+m_{57}(m_{57}-1)+$$
$$+ m_{58}(m_{58}-1) + m_{59}(m_{59}-1) = (\rho-1)\lambda = 24$$

The above conditions give the following unique solution for line l_5:

$$l_5 = 2\ 2\ 2\ 2\ 4\ 2\ 2\ 0\ 0$$

Here we used the permutation (1)(2)(3)(4)(5 6 7 8 9) of orbit numbers which fixes all previously constructed lines.

Similarly for the next representative line l_6 we obtain

$$l_6 = 2\ 2\ 2\ 2\ m_{65}\ m_{66}\ m_{67}\ m_{68}\ m_{69}$$

where we have

$$\{m_{65}, m_{66}, m_{67}, m_{68}, m_{69}\}=\{4, 2, 2, 0, 0\} \quad (5)$$

The fact that $|1_5 \cap 1_6 \varrho^k| = 2$, $k= 0, 1, \ldots 12$ implies

$$2\cdot 2 + 2\cdot 2 + 2\cdot 2 + 2\cdot 2 + 4\cdot m_{65} + 2\cdot m_{66} + 2\cdot m_{67} + 0\cdot m_{68} + 0\cdot m_{69} = 26$$

which is in a contradiction with (5). The theorem is proved.

REFERENCES

1. E Ademaj, On the classification of projective planes of order 15 with a Frobenius group of order 30 as a colineation group, Archiv der Mathematic, 45 (1985) 86-96.

2. M. Aschbacher, On colineation groups of symetric block designs, J.Combin. Theory, 11 (1971) 272-181.

3. T. Beth, D. Jungnickel, H. Lenz, Design Theory, Mannheim - Wien-Zürich, 1985.

4. Z.Janko, T.V.Trung, The full colineation group of any projective plane of order 12 is a {2,3}- group, Geometriae Dedicata 12 (1982) 101-110.

Prirodno-matematički fakultet
Maršala Tita b.b.
38000 Priština
JUGOSLAVIJA

POST AND HOSSZÚ-GLUSKIN THEOREM FOR VECTOR VALUED GROUPS

S.Markovski, B.Janeva

The notion of an (m+k,m)-group was first introduced in [1], as a generalization of the notion of an n-group. Here we generalize the Post theorem for embedding of an n-group into a group ([5]) and the Hosszú-Gluskin theorem for representation of an n-group by a group ([4], [5]). Namely, in Theorem P we show that every (m+k,m)-group $(Q;[\ ])$ is embeddible into a group $(G;\cdot)$ such that $Q\subseteq G$ and $[a_1^{m+k}]=b_1^m \iff a_1\cdot a_2\cdot\ldots\cdot a_{m+k}=b_1\cdot b_2\cdot\ldots\cdot b_m$ for all $a_\lambda, b_\nu\in Q$. Using this result in Theorem HG we show that every (m+k,m)-group $(Q;[\ ])$ can be represented by a group $(Q^m;*)$. As a corrolary of these results (for m=1) we have that Hosszú-Gluskin theorem is a consequence of Post coset theorem. It is notified (in [3]) that Post had proven the Hosszú-Gluskin theorem in [6], but his proof is, in a way, given in [6] ambiguously.

First we will give some preliminary notations and definitions. If A is a nonempty set, the elements of the n-th Cartesian power A^n of A will be denoted by $(a_1,\ldots,a_n)$, or shortly by a_1^n; for n=0 we define $A^0=\{0\}$. Also, a_r^s is a notation for $(a_r,a_{r+1},\ldots,a_s)$ if $s\geq r$, and the empty symbol if $r>s$. In the case when A is a subset of a semigroup $\underline{S}=(S;\cdot)$, then for $n\geq 1$, we put $A_n=\{a_1\cdot\ldots\cdot a_n \mid a_\nu\in A\}$. This product will be, as usual, written without the operation symbol.

Thus, if $\emptyset\neq A\subseteq S$,

$$A^n = \{a_1^n=(a_1,\ldots,a_n) \mid a_i\in A\},\ n\geq 0$$

$$A_n = \{a_1\ldots a_n \mid a_i\in A\},\ n\geq 1.$$

If $a_1=a_2=\ldots=a_n = a\in A$, then $a^n=a_1^n$, and $a^n=a_1\ldots a_n$.

The free semigroup with a basis A, where A is a nonempty set, is denoted by A^+, and in this case

---

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

$$A^+ = \bigcup_{n\geq 1} A^n,\quad a_1^i \cdot a_{i+1}^{i+j} = a_1^{i+j}$$

for each $a_\nu \in A$, $i,j \geq 1$. If $a \in A^+$, then we define a length of a, $|a|$, by

$$|a| = n \text{ iff } a \in A^n.$$

We denote by $\mathbb{N}$ the set $\{1,2,\ldots\}$ of positive integers, and by $\mathbb{N}_r$ the set $\{1,2,\ldots,r\}$, for each $r \in \mathbb{N}$.

Here we will also give the formulations of the Post and Hosszú-Gluskin theorems and a definition of an $(m+k,m)$-group. Namely, Post theorem states that each n-group $(Q;[\ ])$ can be embedded into a group $(G;\cdot)$ such that $Q \subseteq G$ and for each $a_i \in Q$

$$[a_1^n] = a_1 \cdot a_2 \cdot \ldots \cdot a_n.$$

The Hosszú-Gluskin theorem gives a representation of an n-group $(Q;[\ ])$ by a group $(Q;\cdot)$ with an automorphism θ on $(Q;\cdot)$ and a fixed element $c \in Q$ such that for each $a, a_i \in Q$

$$\theta(c)=c,\ \theta^{n-1}(a)=cac^{-1},\ [a_1^n]=a_1\theta(a_2)\ldots\theta^{n-1}(a_n)c.$$

Let m,k be positive integers, $[\ ]: Q^{m+k} \to Q^m$ a mapping. We say that the pair $\underline{Q}=(Q;[\ ])$ is an $(m+k,m)$-group (or a vector valued group) if $[\ ]$ is associative, i.e. for all $a_j \in Q$

$$[[a_1^{m+k}]a_{m+k+1}^{m+2k}] = [a_1^i[a_{i+1}^{i+m+k}]a_{i+m+k+1}^{m+2k}],\ i \in \mathbb{N}_k,$$

and the equations

$$[xa_1^k] = b_1^m = [a_1^k y]$$

have solutions $x,y \in Q^m$, for each $a_1^k \in Q^k$, $b_1^m \in Q^m$.

1. Let $\underline{G}=(G;\cdot)$ be a group with the unity e, and m,k be positive integers. We say that the subset $Q \subseteq G$ is an $(m+k,m)$-subgroup of $\underline{G}$ iff the following conditions hold:

(I) The mapping $a_1^m \mapsto a_1 \ldots a_m$ is a bijection from Q^m into Q_m.

Note that if (I) holds then the mappings $a_1^r \mapsto a_1 \ldots a_r$ are bijections from Q^r into Q_r, for each $r \in \mathbb{N}_m$. In this case

we will identify a_1^r and $a_1 \ldots a_r$, i.e. we will assume $Q_r = Q^r$, for each $r \in \mathbb{N}_m$.

(II) $(\forall a \in Q_k) aQ_m = Q_m$,

where $aQ_m = \{aa_1 \ldots a_m \mid a_i \in Q\}$.

To each $(m+k,m)$-subgroup Q of a group G we associate a mapping $[\,]: Q^{m+k} \to Q^m$ defined by:

$$[a_1^{m+k}] = b_1^m \iff a_1 \ldots a_{m+k} = b_1 \ldots b_m \qquad (1.1)$$

for each $a_\nu, b_\lambda \in Q$. $[\,]$ is a well defined $(m+k,m)$-operation on Q, as (I) and (II) hold for Q. The pair $(Q; [\,])$ is said to be an $(m+k,m)$-groupoid. We will show that $(Q; [\,])$ is an $(m+k,m)$-group, but first we will give some properties of $(m+k,m)$-subgroups of a group G.

1.1° (a) $Q_{m+k} = Q_m$.

(b) $Q_i Q_j = Q_{i+j}$, for each $i,j \geq 1$.

(c) $i+j = m+k+r$, $r \geq 0 \implies Q_i Q_j = Q_{m+r}$, for each $i,j \geq 1$. □

1.2° (a) $sk \geq m \implies (e \in Q_{sk} \;\&\; (\forall a \in Q) a \in Q_{sk+1})$.

(b) $sk > m$, $a \in Q \implies a^{-1} \in Q_{sk-1}$.

(c) $H = \bigcup_{i \geq 1} Q_i$ is a subgroup of the group G.

(d) $H = Q^m \cup Q_{m+1} \cup \ldots \cup Q_{m+k-1}$.

Proof. (a) By 1.1° (c) and (II), for each $a \in Q$ there exist $x_1, \ldots, x_m \in Q$ such that

$$a^{sk} x_1 \ldots x_m = a^m,$$

where $s \geq 1$. If $sk \geq m$ we have

$$a^{sk-m} x_1 \ldots x_m = e. \qquad (1.2)$$

Thus $e \in Q_{sk}$ and

$$a = a^{sk-m+1} x_1 \ldots x_m \in Q_{sk+1}.$$

(b) If $sk > m$ we obtain from (1.2)

$$a^{-1} = a^{sk-m-1}x_1 \dots x_m \in Q_{sk-1}.$$

(c) is a consequence of (a) and (b).

(d) is a consequence of 1.1° (c), (a) and the fact that there exist an s such that $m \leq sk < m+k$. □

1.3° (a) $i \geq 1$, $j \geq m$, $a \in Q_i \Longrightarrow aQ_j = Q_j a = Q_{i+j}$.

(b) $(\forall a \in Q_k)\ aQ_m = Q_m = Q_m a$.

Proof. (a) It is obvious that $aQ_j \subseteq Q_{i+j}$, $Q_j a \subseteq Q_{i+j}$ for $a \in Q_i$. Let $a = a_1 \dots a_i$, $a_\lambda \in Q$, and $b_1 \dots b_{i+j} \in Q_{i+j}$, $b_\nu \in Q$. The equation $xa_1 \dots a_i = b_1 \dots b_{i+j}$ has a solution $x \in G$, and $x \in H$, since H is a subgroup of G. Let $sk > m$. Then $x = b_1 \dots b_{i+j} a_i^{-1} \dots a_1^{-1} \in Q_{i+j+i(sk-1)} = Q_{j+isk} = Q_j$. Thus $Q_{i+j} \subseteq Q_j a$, and by symmetry $Q_{i+j} \subseteq aQ_j$. □

1.4° If Q is an $(m+k,m)$-subgroup of a group G then the induced $(m+k,m)$-groupoid $(Q; [\![\ ]\!])$ (defined by (1.1)) is an $(m+k,m)$-group.

Proof. Let $a_\lambda \in Q$ and let $[\![a_1^{m+k}] = b_1^m$, $[\![a_{i+1}^{i+m+k}] = c_1^m$, i.e. $a_1 \dots a_{m+k} = b_1 \dots b_m$, $a_{i+1} \dots a_{i+m+k} = c_1 \dots c_m$ in G. Then we have

$$[\![[\![a_1^{m+k}] a_{m+k+1}^{m+2k}] = [\![b_1^m a_{m+k+1}^{m+2k}] = d_1^m \Longleftrightarrow d_1 \dots d_m =$$

$$= b_1 \dots b_m a_{m+k+1} \dots a_{m+2k} = a_1 \dots a_{m+k} a_{m+k+1} \dots a_{m+2k} =$$

$$= a_1 \dots a_i c_1 \dots c_m a_{m+k+i+1} \dots a_{m+2k} \Longleftrightarrow d_1^m =$$

$$= [\![a_1^i\ [\![a_{i+1}^{m+k+i}] a_{m+k+i+1}^{m+2k}]$$

for each $i \in \mathbb{N}_k$.

The solubility of the equations

$$[\![xa_1^k] = b_1^m = [\![a_1^k y]$$

for $a_\nu, b_\lambda \in Q$ is a consequence of 1.3° (b). □

1.5° If $Q = \{a\}$ is a one element subset of a group G, then Q is an $(m+k,m)$-subgroup of G iff the order of a divides k.

Proof. For each $m \geq 1$, $a^{m+k}=a^m$ iff $a^k=1$ iff the order of a devides k. □

1.6° (a) If $|Q| \geq 2$ and Q is an $(m+k,m)$-subgroup of the group G, then $aQ_{m-1} \subset Q_m$, for each $a \in Q$.

(b) If $|Q| \geq 2$ and Q is an $(m'+k',m')$-, and $(m''+k'',m'')$-subgroup of a group G, then $m'=m''$.

Proof. (a) Let $a,b \in Q$, $a \neq b$. It is clear that $aQ_{m-1} \subseteq Q_m$. Suppose $aQ_{m-1}=Q_m$. Then, there exist $a_\lambda \in Q$, such that $aa_1 \ldots a_{m-1}=b^m$, which, by (I), implies $a=b$.

(b) Let $m' < m''$, i.e. $m' \leq m''-1$. Then $m'+t=m''-1$, for some $t \geq 0$, and for each $a \in Q$

$$aQ_{m''-1} = aQ_{m'+t} = Q_{m'+t+1} = Q_{m''}$$

which contradicts the result in (a). □

1.7° If Q is an $(m+k,m)$-subgroup of a group G and $m \leq sk < m+k$, $sk=m+p$, then Q_{m+p} is an invariant subgroup of the subgroup H of G.

Proof. By 1.1° (c) $Q_{m+p}Q_{m+p} = Q_{m+p+sk} = Q_{m+p}$, and by 1.2° (a), $e \in Q_{m+p}$. Let $a_\lambda \in Q$ and $tk > m$. Then by 1.2° (b) we have $a_\lambda^{-1} \in Q_{tk-1}$ and thus

$$(a_1 \ldots a_{sk})^{-1} = a_{sk}^{-1} \ldots a_1^{-1} \in Q_{sk(tk-1)} = Q_{sk}.$$

$Q_{sk} = Q_{m+p}$ is an invariant subgroup of H by 1.3° (a). □

1.8° Let k be the least positive integer such that Q is an $(m+k,m)$-subgroup of G. Then

(a) Q is an $(m+k',m)$-subgroup of G iff $k|k'$.

(b) $m \leq i < j < m+k \Longrightarrow Q_i \cap Q_j = \emptyset$.

(c) $H/Q_{m+p} \tilde{=} Z_k$, where Z_k is the cyclic group of order k.

Proof. (a) If $k|k'$ then Q is obviously an $(m+k',m)$-subgroup of G. Let Q be an $(m+k',m)$-subgroup of G, where $k'=rk+t$, $0 < t < k$. Then for each $a \in Q_t$

$$aQ_m = Q_{m+t} = Q_{m+t+rk} = Q_{m+k'} = Q_m$$

i.e. Q is an $(m+t,m)$-subgroup of G, contradicting the choice of k.

(b) Since Q_{m+p} is an invariant subgroup of H, by 1.3^{o} we have

$$H/Q_{m+p} = \{xQ_{m+p} \mid x\in H\} = \{Q_{m+i} \mid 0 \le i < k\},$$

which implies that the sets $Q_m, Q_{m+1}, \ldots, Q_{m+k-1}$ are either equal or pairwise disjoint. Let $Q_{m+t} = Q_{m+r}$, $k > t > r \ge 0$. Then for some $a\in Q_r$

$$aQ_{m+t-r} = Q_{m+t} = Q_{m+r} = aQ_m,$$

which implies $Q_{m+t-r} = Q_m$. Thus Q is an $(m+t-r,m)$-subgroup of G, contradicting the choice of k.

(c) By 1.2^{o} (d) and (b) we obtain that the mapping $\phi: a_1 \ldots a_{m+i} \mapsto i-p$ is an epimorphism from H into Z_k, with $\ker\phi = Q_{m+p}$. □

We say that a group G is a <u>covering group</u> of its $(m+k,m)$-subgroup Q if G is generated by Q, i.e.

(III) $G = Q_m \cup Q_{m+1} \cup \ldots \cup Q_{m+k-1}$.

If, moreover, G satisfies the following condition

(IV) $m \le i < j < m+k \Longrightarrow Q_i \cap Q_j = \emptyset$

then we say that G is a <u>universal covering group</u> of its $(m+k,m)$-subgroup Q. The universal covering group of Q will be denoted by Q^{v}.

<u>1.9°. Let Q be an $(m+k,m)$-subgroup of $G=Q^{v}$, Q' an $(m+k,m)$-subgroup of a group $(G';*)$ and $\lambda: Q \to Q'$ a map, such that for all $a_i, b_j \in Q$</u>

$$a_1 \ldots a_{m+k} = b_1 \ldots b_m \Longleftrightarrow \lambda(a_1)*\ldots*\lambda(a_{m+k}) = \lambda(b_1)*\ldots*\lambda(b_m).$$

<u>Then there exists a unique homomorphism $\xi: G \to G'$ which is an extension of λ.</u> □

As a corollary of 1.8° we have

1.10°. If k is the least positive integer such that Q is an (m+k,m)-subgroup of the group G, and G is a covering group for Q, then G is a universal covering group for Q. □

Let us note that by 1.3° the following is also true:

1.11°. If G is a universal covering group of its (m+k,m)-subgroup Q, then for each $a \in Q$

$$G = Q^m \cup aQ^m \cup \ldots \cup a^{k-1}Q^m =$$
$$= Q^m \cup Q^m a \cup \ldots \cup Q^m a^{k-1}. \quad \square$$

2. Let $\underline{Q}=(Q;[\ ])$ be a given (m+k,m)-group. We will construct a group $\underline{G}=(G;\cdot)$ such that $Q \subseteq G$ is an (m+k,m)-subgroup of $\underline{G}$, and $\underline{G}$ is its universal covering group. The (m+k,m)-operation $[\![\ ]\!]$ induced by the (m+k,m)-subgroup Q, defined by (1.1), will coincides with the operation $[\ ]$ of the given (m+k,m)-group $\underline{Q}$.

Further on by $\underline{Q}=(Q;[\ ])$ a given (m+k,m)-group will be denoted. By ([2], pg. 27) Q satisfies the general associative law, and the "product" $[a_1^{m+sk}]$ is defined for all $s \geq 1$. Also, Q is cancellative, i.e.

$$[a_1^{i-1}x_1^m a_i^k] = [a_1^{i-1}y_1^m a_i^k] \Longrightarrow x_1^m = y_1^m \qquad (2.1)$$

for each $i \in N_{k+1}$, and $a_\lambda, x_\nu, y_\mu \in Q$ (see [2], pg. 54). By (2.1), for each $x,y \in Q^1$, $ab,cd \in Q^{m+sk-i}$, $i \geq 1$,

$$[axb] = [ayb] \Longrightarrow [cxd] = [cyd], \qquad (2.2)$$

(see [2], pg. 37).

Let $\underline{Q}=(Q;[\ ])$ be a given (m+k,m)-group. Define a relation $\sim$ on Q^+ by:

$$(\forall u,v \in Q^+)(u \sim v \Longleftrightarrow (\exists w \in Q^+)[uw]=[vw]). \qquad (2.3)$$

where [uw] and [vw] denote that $uw \in Q^{m+sk}$, $vw \in Q^{m+tk}$ for some $s,t \geq 0$, and we put $[a_1^m] = a_1^m$ for $a_1 \in Q$.

2.1°. (a) $u \sim v \Longrightarrow |u| \equiv |v| \pmod{k}$.

(b) The relation $\sim$ is a congruence on Q^+.

(c) $Q^+/\sim$ is a group.

(d) $a,b \in Q$, $a \sim b \Longrightarrow a=b$ (i.e. we can concider Q as a subset of $Q^+/\sim$).

Proof. (a) $u \sim v \Longrightarrow (\exists w \in Q^+)\,[uw]=[vw] \Longrightarrow |uw| \equiv |vw| \pmod{k} \Longrightarrow |u| \equiv |v| \pmod{k}$.

(b) Note that by (2.2) and (2.3) it follows that

$$u \sim v \Longrightarrow [tuw] = [tvw] \tag{2.4}$$

for all $t,w \in Q^+$ such that $|tuw| \equiv |tvw| \equiv m \pmod{k}$. Now by (2.4) we obtain that $\sim$ is a congruence on Q^+.

(c) We will show that the equations $ux \sim v$ and $zu \sim v$ have solutions on x and z for every $u,v \in Q^+$. If $|v| < m$ then for some $w,t \in Q^+$ we have $|wv| = m$ and $|wut| = sk$, $s \geq 1$. Now, since in the $(m+k,m)$-group Q the equation $[wuty] = wv$ has a solution $y \in Q^m$, we obtain that $x=ty$ is a solution of $ux \sim v$. In the other case, when $|v| \geq m$, we have $v=v'v''$ where $|v'| = m$, and the equation $[uty] = v'$ has a solution $y \in Q^m$ for some $t \in Q^r$. Now $x=tyv''$ is a solution of $ux \sim v$. Similarly we solve the equation $zu \sim v$.

(d) Let $a,b \in Q$, $a \sim b$. Then by (2.4) $[a^m]=[b^{m-1}a]$, i.e. $a^m=b^{m-1}a$ in Q^m, which implies $a=b$. □

2.2°. $Q^+/\sim \;= Q^v$.

Proof. We will show that the conditions (I)-(IV) are fulfiled for $Q^+/\sim$. It is clear that (I) holds for $Q^+/\sim$, as if $a_1^m \sim b_1^m$ in $Q^+/\sim$ it follows that $[a_1^m w] = [b_1^m w]$, which (by cancellativity of the $(m+k,m)$-operation $[\,]$) implies $a_1^m = b_1^m$.

Let $a=a_1 \ldots a_k \in Q_k$ and $b=b_1 \ldots b_m \in Q_m$ $(a_\nu, b_\lambda \in Q)$. Now, as $[a_1^k b_1^m] = c_1^m \in Q^m$, $ab \sim c_1 \ldots c_m$, and thus $ab \in Q_m$, i.e. $aQ_m \subseteq Q_m$. If $a=c_1 \ldots c_m \in Q_m$ is given, then for each $a \in Q_k$ the equation

$[ax]=c$ has a solution $x\in Q_m$, i.e. $c \sim ax$. Thus $c\in aQ_m$, i.e. $Q_m \subseteq aQ_m$, i.e. (II) is satisfied. As Q generates $Q^+/\sim$ we have (III), and (IV) follows by 2.1° (a). □

Theorem P.[1] Let $(Q;[\ ])$ be an $(m+k,m)$-group. Then there exists a group $(G;\cdot)$ such that $Q\subseteq G$ and for each $a_i,b_j\in Q$

$$[a_1^{k+m}] = b_1^m \iff a_1\ldots a_{k+m} = b_1\ldots b_m.$$

Proof. Take $G = Q^+/\sim$. □

We note that for each $(m+k,m)$-group $(Q;[\ ])$, as a consequence of the results above, the $(m+k,m)$-operation $[\![\ ]\!]$ (defined by (1.1)) and $[\ ]$ coincides, i.e. for each $a_i\in Q$,

$$[\![a_1^{m+k}]\!] = [a_1^{m+k}]. \tag{2.5}$$

3. We have seen in 2 that the $(m+k,m)$-group $(Q;[\ ])$ coincides with the $(m+k,m)$-group $(Q;[\![\ ]\!])$ induced by the $(m+k,m)$-subgroup Q of $Q^v=Q^+/\sim$. From now on we will denote by a a fixed element from Q and Q^v will be given in the form

$$Q^v = Q^m \cup Q^m a \cup Q^m a^2 \cup \ldots \cup Q^m a^{k-1}. \tag{3.1}$$

The product in Q^v is defined by

$$x_1^m a^i \cdot y_1^m a^j = z_1^m\, a^{i\oplus j}$$

where $\oplus$ is the operation in the cyclic group Z_k, and z_1^m is a solution of the equation

$$[x_1^m a^i y_1^m a^{k+j-(i\oplus j)}] = [z_1^m a^k].$$

The inverse of the element $x\in Q^v$ will be denoted by x^{-1}; and $Q_{m+p}=Q^m a^p$ is the invariant subgroup of Q^v, where $m+p \equiv 0 \pmod k$, $0 \le p < k$.

3.1°. (a) Defining an operation $*$ on Q^m by

$$x_1^m * y_1^m = [x_1^m a^p y_1^m], \tag{3.2}$$

for each $x_1^m, y_1^m \in Q^m$, a group $(Q^m;*)$ is obtained, with a unity a^{-p} and the inverse b^{-*} of $b\in Q^m$ defined by $b^{-*}=a^{-p}b^{-1}a^{-p}$.

---

[1] This property is given in [2].

(b) The mapping $\theta: x \mapsto a^{-p}xa^{p}$ is an automorphism of $(Q^m;*)$ such that

$$\theta^n(x) = a^{-np}xa^{np} \tag{3.3}$$

for each $x \in Q^m$, $n \geq 1$.

Proof. (a) By (2.5) we have

$$x_1^m * y_1^m = x_1 \ldots x_m a^p y_1 \ldots y_m$$

which implies the associativity of $*$. It is easy to check that a^{-p} is the unity, and $a^{-p}b_m^{-1}\ldots b_1^{-1}a^{-p}$ is the inverse of $b_1^m \in Q^m$. □

Note that if $b \in Q$, then $b \in Q^m a^{p+1}$. Now, if $k=tm+r$, $0 \leq r < m$, then for each $x \in Q^r$ there exists $y \in Q^m$ such that $x=ya^{p+r}$. Define a mapping $\phi: Q^r \to Q^m$ by

$$\phi(x) = ya^{r-tp}. \tag{3.4}$$

(If $r=0$, then $Q^0=\{0\}$, and $\phi(0)=a^{-tp-p}$.)

3.2°. ϕ is an injection from Q^r into Q^m. □

Let $z \in Q^r$, $x_\lambda \in Q^m$ and $x=x_0x_1\ldots x_tz \in Q^{m+k}$. Using θ and ϕ defined as above we obtain

$$\begin{aligned}
&x_0 * \theta(x_1) * \theta^2(x_2) * \ldots * \theta^t(x_t) * \theta^{t+1}(\phi(z)) = \\
&= x_0 a^p a^{-p} x_1 a^p a^p a^{-2p} x_2 a^{2p} a^p \ldots \\
&\quad \ldots a^p a^{-tp} x_t a^{tp} a^p a^{-(t+1)p} \phi(z) a^{(t+1)p} = \\
&= x_0 x_1 \ldots x_t z a^{-(p+r)} a^{r-tp} a^{(t+1)p} = \\
&= x_1 \ldots x_t z \\
&= [x].
\end{aligned}$$

Thus we have proven the following

Theorem HG. Let $(Q;[\,])$ be an $(m+k,m)$-group, where $k=tm+r$, $0 \leq r < m$. Then there exists a group $(Q^m;*)$, an automorphism $\theta \in \mathrm{Aut}(Q^m;*)$ and an injection $\phi: Q^r \to Q^m$ such that for each $x_1 \in Q^m$, $z \in Q^r$ the equality

$$[x_0 \ldots x_t z] = x_0 * \theta(x_1) * \theta^2(x_2) * \ldots * \theta^t(x_t) * \theta^{t+1}(\phi(z)) \quad (3.5)$$

holds. Furthermore, if r=0, then

$$\theta(\phi(0)) = \phi(0), \quad (3.6)$$

$$\theta^t(x) = \phi(0) * x * \phi(0)^{-*} \quad (3.7)$$

for each $x \in Q^m$. □

In the case m=1, k=n-1, the notion of (n,1)-group coincides with the notion of n-group. Thus the theorem of Hosszú-Gluskin for representation of an n-group by a group is a special case of Theorem HG. In the case of n-groups the converse is also valid, i.e. if $(G;*)$ is a group, θ an automorphism of $(G;\cdot)$ and $\phi(0) \in G$, such that (3.6) and (3.7) are valid then by (3.5) an n-ary operation $[\ ]$ on G is defined such that $(G;[\ ])$ is an n-group.

In the vector valued version of Hosszú-Gluskin theorem the converse is not generally valid, because even when r=0, the (m+k,m)-operation $[\ ]$ defined by (3.5) need not be associative (although it satisfies the condition for solubility of equations when $t \geq 1$).

Note that Theorem HG is a consequence of Theorem P. Thus in the n-ary case (when m=1) we obtain that the Post coset theorem implies the Hosszú-Gluskin Theorem.

REFERENCES

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

[2] G.Čupona, N.Celakoski, S.Markovski, D.Dimovski: Vector valued groupoids, semigroups and groups, to appear

[3] K.Glazek: Bibliography of n-groups (polyadic groups) and some group like n-ary systems, Proc. Symp. n-ARY STRUCTURES, 1982, Skopje, 253-289.

[4] L.M.Gluskin: On positional operatives, Dokl. Akad. Nauk SSSR 157 (1964), 767-770.

[5] M.Hosszú: On the explicit form of n-group operations, Publ. Math. 10 (1963), 88-92.

[6] E.L.Post: Polyadic groups, Trans. Amer. Math. Soc. 48, (1940), 208-350.

PMF, p.f. 162
91000 Skopje
Yugoslavia

INFLATION OF ALGEBRAS

Svetozar Milić

Abstract. Weintroduce the concept of an n-inflation of a universal algebra satisfying a set of identities Σ . This paper is a generalization of n-inflation of semigroups presented in [1].

0. Introduction and preliminaries

Let A be a nonempty set and $F=\{w_i \mid i<\alpha$, α an ordinal number$\}$ a nonempty set of m_i-ary operations on A. Then (A,F) is calleda universal algebra. Algebra (A,F) is an aLgebra satisfying a set of identities Σ if $A \models t_1 \doteq t_2$ for all $t_1=t_2 \in \Sigma$ (where t_1, t_2 are terms of the type F)

Subalgebra T of algebra A is ideal of A if for each $x_1,\ldots,x_{i-1},x_{i+1},\ldots,x_m \in A$, $a \in T$, $w \in F$, w is an m-ary operation on A we have $w(x_1,\ldots,x_{i-1},a,x_{i+1},\ldots,x_m) \in T$ for each $i=1,\ldots,m$.

Exemple: For the algebra (N,+,.) and all $k \in N$ the ideals are $T_k=\{x \in N \mid x \geq k\}$

Some abbreviations: The sequence $x_1,\ldots,x_m$ will be denoted by x_1^m. Identity $t_1[w_1,\ldots,w_s]=t_2[w_1,\ldots,w_s]$ where w_k (k=1,...,s) are all the operations contained in t_1 and t_2, will be denoted by $t_1[w]=t_2[w]$. The arity of an operation w will be denoted by $|w|$.

The following proposition is a generalization of the wellknown semigroup-theoretical notion of Rees congruence to universal algebras.

PROPOSITION 0.1. 2 . Let T be an ideal of algebra (A,F) and ϱ_T the following binary relation on A:

$$x \,\varrho_T\, y \quad \text{iff} \quad x=y \vee x,y \in T.$$

Then ϱ_T is a congruence on A.

If ϱ is a congruence on A with at most one non-singleton class T and T is a subalgebra of A, then T is an ideal and $\varrho = \varrho_T$.

We denote the quotient algebra A/ϱ_T by A/T and we call it Rees quotient algebra.

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

Let T and K be two disjoint algebras of type F and suppose that K has a zero element i.e. $w(x_1^{i-1},0,x_{i+1}^m)=0$ for each $w \in F$ and $i=1,\ldots,m$ ($x_1,\ldots,x_m \in K$, $0 \in K$). An algebra (A,F) is said to be an (ideal) extension of T by K if it contains T as an ideal and Rees quotient algebra $A/_T$ is isomorphic to K.

Let A be an extension of T. Then A is a retract extension if there exist a homomorphism φ of A onto T and $\varphi(x)=x$ for all $x \in T$. In this case we call φ a retraction.

Here we give one more characterization of the retract extension.

PROPOSITION 0.2. Let (T,F) be an algebra satisfying Σ. To each $a \in T$ assosiate a set Y_a such that

$$a \in Y_a\,, \quad Y_a \cap Y_b = \emptyset \quad \text{if} \quad a \neq b\,. \tag{0.1}$$

For every $w \in F$ ($|w| = m$), let

$$\begin{aligned} &\phi_w^{(a_1^m)} : Y_{a_1} \times Y_{a_2} \times \ldots \times Y_{a_m} \longrightarrow Y_{w(a_1^m)} \\ &\phi_w^{(a_1^m)}(x_1^{k-1},a_k,x_{k+1}^m) = w(a_1^m)\,, \quad k=1,\ldots,m\,, \end{aligned} \tag{0.2}$$

be functions for which from $t_1[w] = t_2[w] \in \Sigma$ it holds that

$$t_1\left[\phi_w^{(a_1^m)}\right] = t_2\left[\phi_w^{(a_1^m)}\right] \tag{0.3}$$

(where each w in the identity $t_1[w] = t_2[w]$ has been replaced by the corresporiding function $\phi_w^{(a_1^m)}$).

On the set $A = \bigcup_{a \in T} Y_a$ we define operation w^* by:

$$w^*(x_1^m) = \phi_w^{(a_1^m)}(x_1^m) \quad \text{if} \quad x_i \in Y_{a_i} \quad (i=1,\ldots,m;\ |w|=m)$$

Then (A,F^*) is an algebra of the same type satisfying Σ and (A,F^*) is a retract extension of (T,F). Conversely, every retract extension A of an algebra T can be so constructed.

Proof. Supose that A fulfills the conditions of the proposition. Let $x_i \in Y_{a_i}$ ($i=1,\ldots,m$) and $w \in F$ be an operation of arity m. Then by (0.3) for arbitrary $t_1[w] = t_2[w] \in \Sigma$ we have

$$t_1[w^*] = t_1[\phi_w^{(a_1^m)}] = t_2[\phi_w^{(a_1^m)}] = t_2[w^*] .$$

Hence (A,F^*) is an algebra of the same type satisfying Σ.

Define a mapping $\varphi: A \longrightarrow T$ by $\varphi(Y_a) = a$. It is clear that φ is onto and that $\varphi(a) = a$ for all $a \in T$. Furthermore, for an arbitrary operation $w^* \in F^*$ ($|w^*| = m$) and $x_i \in Y_{a_i}$ ($i=1,\ldots,m$), we nave

$$\varphi(w^*(x_1,\ldots,x_m)) = \varphi(\phi_w^{(a_1^m)}(x_1,\ldots,x_m)) = w(a_1,\ldots,a_m)$$

$$= w(\varphi(x_1),\ldots,\varphi(x_m)) .$$

Thus φ is a homomorphism and by (0.2) T is an ideal of A. Therefore, (A,F^*) is a retract extension of (T,F).

Conversely, let (A,F) be a retract extension of an algebra T satisfying Σ. Then there is a homomorphism φ of A onto T such that $\varphi(x) = x$ for all $x \in T$. For $a \in T$ assume that $Y_a = \varphi^{-1}(a)$. Then $A = \bigcup_{a\in T} Y_a$ and for the sets Y_a ($a \in T$) the condition (0.1) is satisfied

For any $x_1,\ldots,x_m \in A$ there exist $a_1,\ldots,a_m \in T$ such that $x_i \in Y_a$ ($i=1,\ldots,m$) so that $\varphi(x_i) = a_i$ ($i=1,\ldots,m$). From this it follows that for an arbitrary $w \in F$ of arity m, we have

$$\varphi(w(x_1,\ldots,x_m) = w(\varphi(x_1),\ldots,\varphi(x_m))$$

$$= w(a_1,\ldots,a_m) \in Y_{w(a_1^m)}$$

i.e. $w(x_1,\ldots,x_m) \in Y_{w(a_1^m)}$. Hence there exist functions

$$\phi_w^{(a_1^m)} : Y_{a_1} \times Y_{a_2} \times \ldots \times Y_{a_m} \longrightarrow Y_{w(a_1^m)}$$

and it is clear that for there functions (0.3) holds. Since T is an ideal of A we have (0.2).

1. n-inflation of algebras

We introduce here the notion of an n-inflation of a universal algebra satisfying Σ.

LEMMA 1.1. Let (T,F) be a universal algebra which satisfies Σ. To each $a \in T$ we assosiate a family of sets X_i^a ($i=1,\ldots,n$) such that $a \in X_r^a$ for some $r \in \{1,\ldots,n\}$ and

(1.1) $X_i^a \cap X_j^b = \emptyset$ *if* $i \neq j$; $X_i^a \cap X_j^b = \emptyset$ *if* $a \neq b$.

Let for nonempty sets $X_{i_1}^{a_1}, X_{i_2}^{a_2}, \ldots, X_{i_m}^{a_m}$ *and operation* $w \in F$ $(|w| = m)$,

$$\phi^{(a_1^m)}_{(i_1^m)w} : X_{i_1}^{a_1} \times X_{i_2}^{a_2} \times \ldots \times X_{i_m}^{a_m} \longrightarrow \bigcup_{v=\max(i_1^m)}^{n} X_v^{w(a_1^m)} \quad \text{if} \quad \max(i_1^m)+1 \leq n$$

(1.2)
$$\phi^{(a_1^m)}_{(i_1^m)w}(x_1,\ldots,x_m) = w(a_1,\ldots,a_m) \quad \text{if} \quad \max(i_1,\ldots,i_m)+1 > n$$

$$\phi^{(a_1^m)}_{(i_1^m)w}(x_1^{k-1}, a_k, x_{k+1}^m) = w(a_1^m) \quad \text{for all} \quad k \in \{1,\ldots,m\}$$

be functions for which: for each $t_1[w] = t_2[w] \in \Sigma$ *we have*

(1.3) $$t_1\left[\phi^{(a_1^m)}_{(i_1^m)_w}\right] = t_2\left[\phi^{(a_1^m)}_{(i_1^m)_w}\right] .$$

Let $Y_a = \bigcup_{i=1}^{n} X_i^a$ *and define the corresponding operation* w^* *by the operation* $w \in F$ *of the some length on* $A = \bigcup_{a \in T} Y_a$ *by:*

$$w^*(x_1,\ldots,x_m) = \phi^{(a_1^m)}_{(i_1^m)w}(x_1,\ldots,x_m) \quad \text{if} \quad x_s \in X_{i_s}^{a_s} \quad (1 \leq s \leq m; |w|=m)$$

Then (A,F^*) *is an algebra of the same type as the algebra* (T,F) *satisfying* Σ .

Proof. Let $x_1,\ldots,x_m \in A$ and $w \in F$ $(|w| = m)$. Then there exist $a_1, \ldots,a_m \in T$ such that $x_s \in Y_a$ $(s=1,\ldots,m)$ i.e. $x_s \in X_{i_s}^{a_s}$ for som $1 \leq i_s \leq n$ Then for arbitrary law $t_1[w] = t_2[w]$ and $|w| = m$, we have

$$t_1[w^*] = t_1\left[\phi^{(a_1^m)}_{(i_1^m)w}(x_1^m)\right] = t_2\left[\phi^{(a_1^m)}_{(i_1^m)w}(x_1^m)\right] = t_2[w^*] .$$

Therefore (A,F^*) is an algebra of type F satisfying Σ .

DENITION1.1. The algebra (A,F) satisfying Σ constructed in Lemma 1. is called an n-inflation of algebra (T,F).

The following theorem gives a characterization of an n-inflation algebras, which shows that here we have the case retract extensions.

THEOREM 1.1. *An algebra* (A,F) *satisfying* Σ *is an* n*-inflation of algebra* (T,F) *satisfying* Σ *if and only if* $A^{n(|w|-1)+1} \subset T$ *for all* $w \in F$ *and* A *is a retract extension of* T.

Proof. Let A be an n-inflation of an algebra T. Then by (1.2) T is an ideal of A. Let $w \in F$ and $u \in A^{n(|w|-1)+1}$, i.e.

$$u = t(s_1, s_2, \ldots, s_{n(|w|-1)+1})$$

where t is a term consisting of the operation w and some $s_r \in A$ $(r=1,\ldots,n(|w|-1)+1)$. Let $s_r \in X_1^{a_r}$, where $a_r \in T$. Then

$$u = t(s_1^{i-1}, w(s_i^{|w|-1+i}), s_{|w|+i}^{n(|w|-1)+1})$$

$$= t(s_1^{i-1}, \phi^{(a_i^{|w|-1+i})}_{(1,\ldots,1),w}(s_i^{|w|-1+i}), s_{|w|+i}^{n(|w|-1)+1}) .$$

If $\max(1,\ldots,1)+1=2 > n$, then $\phi^{(a_i^{|w|-1+i})}_{(1,\ldots,1),w}(s_i^{|w|-1+i}) = u_1 \in T$ so $u \in T$.

If $2 \leq n$, then

$$u = t(s_1^{i-1}, u_1, s_{|w|+i}^{n(|w|-1)+1}), \quad u_1 \in X_{t_1}^{w(a_i^{|w|-1+i})}, \quad 2 \leq t_1 \leq n .$$

Further on,

$$u = t(s_1^{j-1}, \phi^{h}_{(1,\ldots,1,t_1,1,\ldots,1),w}(s_j, \ldots, u_1, \ldots, s_{|w|-1+j}), s_{|w|+j}^{n(|w|-1)+1})$$

where $h = (a_j, \ldots, w(a_i^{|w|-1+i}), \ldots, a_{|w|-1+j})$.

If $t_1+1 > n$, then $\phi^{h}_{(1,\ldots,1,t_1,1,\ldots,1),w}(s_j, \ldots, u_1, \ldots, s_{|w|-1+j}) =$

$= u_2 \in T$ so $u \in T$.

If $t_1+1 \leq n$, then

$$u = t(s_1^{j-1}, u_2, s_{|w|+j}^{n(|w|-1)+1}), \quad u_2 \in X_{t_2}^{w(h)}, \quad 3 \leq t_2 \leq n.$$

Continuing this procedure we have that:

If $t_{n-2}+1 > n$, then $\phi^{(b_1^{|w|})}_{(1,\ldots,1,t_{n-1},1,\ldots,1),w}(s_1^{p-1}, u_{n-2}, s_{p+1}^{|w|}) =$

$= u_{n-1} \in T$, for some $b_1^{|w|}$, so $u \in T$.

If $t_{n-1}+1 \leq n$, then $u = \phi^{(c_1^{|w|})}_{(1,\ldots,n,\ldots,1),w}(s_1^{l-1}, u_{n-1}, s_{l+1}^{|w|}) =$

$= u_{n-1} \in T$, for some $c_1^{|w|}$, (since $n+1 > n$).

In other cases ($s_r \in X_{k_r}$, $1 < k_r \leq n$) we have also that $u \in T$.

Thus $A^{n(|w|-1)+1} \subset T$.

Define a mapping $\varphi: A = \bigcup_{a \in T} Y_a \longrightarrow T$ by $\varphi(Y_a) = a$.

For any $w \in F$ $(|w|=m)$ and $x_1, \ldots, x_m \in A$ there exist $a_1, \ldots, a_m \in T$ such that $a_s \in Y_{a_s}$ i.e. $a_s \in X_{r_s}^{a_s}$ for some $1 \leq r_i \leq n$. So

$$\varphi(w(x_1,\ldots,x_m)) = \varphi(\phi^{(a_1^m)}_{(r_1^m),w}(x_1,\ldots,x_m)),$$

where

$$\phi^{(a_1^m)}_{(r_1^m),w}(x_1,\ldots,x_m) \in X_k^{w(a_1^m)} \subset Y_{w(a_1^m)}$$

for some $\max(r_1,\ldots,r_m)+1 \leq k \leq n$ if $\max(r_1^m)+1 \leq n$, and $\phi^{(a_1^m)}_{(r_1^m),w}(x_1,\ldots,x_m) = w(a_1,\ldots,a_m)$ if $\max(r_1^m)+1 > n$. Now by the definition of φ we have

$$\begin{aligned}\varphi(w(x_1,\ldots,x_m)) &= w(a_1,\ldots,a_m)\\ &= w(\varphi(x_1),\ldots,\varphi(x_m)).\end{aligned}$$

It is clear that $\varphi(x) = x$ for all $x \in T$. Therefore, A is retract extension of T.

Conversely, let n by the smalest positive integer such that $A^{n(|w|-1)+1} \subset T$ for all $w \in F$ and let φ be a retraction of A onto T. An arbitrary $a \in T$ is in one of the following sets

$$A \setminus \bigcup_{w\in F} A^{|w|},\ \bigcup_{w\in F} A^{|w|} \setminus \bigcup_{w\in F} A^{2|w|-1},\ \ldots,\ \bigcup_{w\in F} A^{(n-1)(|w|-1)+1} \setminus \bigcup_{w\in F} A^{n(|w|-1)+1},$$

$$\bigcup_{w\in F} A^{n(|w|-1)+1}.$$

For $a \in \bigcup_{w\in F} A^{(n-r)(|w|-1)+1} \setminus \bigcup_{w\in F} A^{(n-r+1)(|w|-1)+1}$ for some $1 \leq r \leq n$, we define sets: $Y_a = \varphi^{-1}(a)$,

$$\begin{aligned}X_1^a &= Y_a \cap (A \setminus \bigcup_{w\in F} A^{|w|})\\ X_2^a &= Y_a \cap (\bigcup_{w\in F} A^{|w|} \setminus \bigcup_{w\in F} A^{2|w|+1})\\ &\vdots\\ X_{n-r}^a &= Y_a \cap (\bigcup_{w\in F} A^{(n-r-1)(|w|-1)+1} \setminus \bigcup_{w\in F} A^{(n-r)(|w|-1)+1})\\ X_{n-r+1}^a &= Y_a \cap (\bigcup_{w\in F} A^{(n-r)(|w|-1)+1})\end{aligned}$$

$$X_{n-r+2}^a = X_{n-r+3}^a = \ldots = X_n^a = \emptyset.$$

It is clear that the conditions (1.1) hold for every X_i^a and X_j^b $(1 \leq i,j \leq n\ ;\ a,b \in T)$.

If $a \in T$ then $Y_a = \bigcup_{i=1}^{n} X_i^a$ and so $A = \bigcup_{a\in T} Y_a$. For $x_1,\ldots,x_m \in A$ and $w \in F$ $(|w|=m)$ there exist $a_1,\ldots,a_m \in T$ such that $x_k \in Y_{a_k}$. So by Proposition 0.2. we have that

$$w(Y_{a_1},Y_{a_2},\ldots,Y_{a_m}) \subset Y_{w(a_1,a_2,\ldots,a_m)}$$

Let $x_k \in X_{i_k}^{a_k}$ $(1 \leq k \leq m)$, $a_k \in \bigcup_{w\in F} A^{(n-r_k)(|w|-1)+1} - \bigcup_{w\in F} A^{(n-r_k+1)(|w|-1)+1}$ $(1 \leq r_k \leq n)$. Then

$$x_k \in X_{i_k}^{a_k} = Y_{a_k} \cap \left(\bigcup_{w\in F} A^{(i_k-1)(|w|-1)+1} - \bigcup_{w\in F} A^{i_k(|w|-1)+1} \right)$$

$(1 \leq i_k \leq n-r_k)$.

Then

$$w(x_1,\ldots,x_m) \in w\left(\bigcup_{w\in F} A^{(i_1-1)(|w|-1)+1}, \ldots, \bigcup_{w\in F} A^{(i_m-1)(|w|-1)+1} \right)$$

$$= \bigcup_{w\in F} A^{p}, \text{ here } p = \left(\sum_{s=1}^{m} i_s - m\right)(|w|-1)+m$$

and if $p \leq n$ we have $w(x_1,\ldots,x_m) \in \bigcup_{\nu=p}^{n} x_\nu^{w(a_1^m)}$. If $p > n$, then $w(x_1,\ldots,x_m) = w(a_1,\ldots,a_m) \in T$. For $a_k \in T$ we have that $w(x_1^{k-1}, a_k, x_{k+1}^m) = w(a_1^m)$, $(k=1,\ldots,m)$. In this way functions $\phi_{(i_1^m),w}^{(a_1^m)}$ from Lemma 1.1. are defined and the condition (1.3) holds.

Exemple. (a) The algebra $(A,+,.)$ given by the table

+	0	a	b	1	c	d
0	1	1	1	1	1	1
a	1	1	1	1	1	1
b	1	1	c	1	1	1
1	1	1	1	1	1	1
c	1	1	1	1	1	1
d	1	1	c	1	1	c

·	0	a	b	1	c	d
0	0	0	0	0	0	0
a	0	0	0	0	0	0
b	0	0	a	0	0	a
1	0	0	0	0	0	0
c	0	0	0	0	0	0
d	0	0	0	0	0	a

satisfying $\Sigma = \emptyset$ is a 2-inflation of the algebra $(T,+,.)$ given by the table

+	0	1
0	1	1
1	1	1

·	0	1
0	0	0
1	0	0

Here we have that $\varphi : A \longrightarrow T$, defined by $\varphi = \begin{pmatrix} 0 & a & b & 1 & c & d \\ 0 & 0 & 0 & 1 & 1 & 1 \end{pmatrix}$, is a homomorphism and $\varphi(x) = x$ for all $x \in T$. Therefore,

$$2A = \{1,c\}, \quad 3A = \{1\}, \quad A^2 = \{0,a\}, \quad A^3 = \{0\},$$

$$Y_0 = \varphi^{-1}(0) = \{0,a,b\}, \quad Y_1 = \varphi^{-1}(1) = \{1,c,d\}.$$

$$X_1^0 = Y_0 \cap (A - \bigcup_{w\in F} A^{|w|}) = Y_0 \cap (A \setminus (2A \cup A^2))$$

$$= \{0,a,b\} \cap (A \setminus \{1,c,0,a\}) = \{0,a,b\} \cap \{b,d\} = \{b\}.$$

$$X_2^0 = \{0,a\}, \quad X_1^1 = \{d\}, \quad X_2^1 = \{1,c\}.$$

4-inflation semigroup i.e. 4-inflation of the

algebra $(S,.)$ satisfying $\Sigma = \{ x.(y.z) = (x.y).z \}$ [1].

Problem. In [2] the definition of a Rees subalgebra was given:
DEFINITION 1.1. Let $M \subset A$ be a subalgebra of A, and for every n-ary operation $w \in F$ and every $(a,b) \in M^2$ and $x_1,\ldots,x_{n-1} \in A$ the following condition might hold:

$$w(a,x_1,\ldots,x_{n-1}),\ w(b,x_1,\ldots,x_{n-1}) \in M \text{ or } w(a,x_1,\ldots,x_{n-1}) = w(b,x_1,\ldots,x_{n-1})$$

$$w(x_1,a,\ldots,x_{n-1}),\ w(x_1,b,\ldots,x_{n-1}) \in M \text{ or } w(x_1,a,\ldots,x_{n-1}) = w(x_1,b,\ldots,x_{n-1})$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$w(x_1,\ldots,x_{n-1},a),\ w(x_1,\ldots,x_{n-1},b) \in M \text{ or } w(x_1,\ldots,x_{n-1},a) = w(x_1,\ldots,x_{n-1},b).$$

Then M is called a Rees subalgebra of (A,F).
In connection to definition give the Rees extension and n-inflation of algebras.

REFERENCES

[1] S.Bogdanović, S.Milić, Inflation of semigroups, Publ.Inst. Math. 41(55) 1987,63-73.

[2] Robert F. Tichy, The Rees congruence in universal algebras, Publ.Inst.Math. 29(43) 1981, 229-239.

Matematički institut
Knez Mihailova 35/I
11001 Beograd p.p. 367
Yugoslavija

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

ON CONTRACTIONS OF LIE ALGEBRAS*

Dušan Pagon

Abstract. Let L be a Lie algebra over the field of complex numbers and $A(t)$ a function from the set of real numbers to the set of linear mappings of algebra L, such that $\det A(t) \neq 0$ if $t \neq 0$. Than we'll call a Lie algebra L' the contraction of algebra L if it has the same vector space as algebra L but a new commutator defined as

$$[x, y]' = \lim_{t \to 0} A(t)^{-1} [A(t)x, A(t)y] .$$

We give the conditions for existence of this limit if $A(t)$ are derivations of algebra L and show some examples of Lie algebras obtained as contractions.

1. Introduction

Let L be an arbitrary Lie algebra over the field of complex numbers with n- dimensional vector space V and $A \in Lin(V)$. Than V is a direct sum of subspaces $V_1 = A^n V$ and $V_0 = \{ x \in V : A^n x = 0 \}$. For each $x \in V$ we'll denote by $x_1 \in V_1$ and $x_0 \in V_0$ elements such that $x = x_1 + x_0$ and call them the regular and the nilpotent part of x, corresponding to mapping A.

If f and g are two continuous real functions of a real variable t than F. Mimura has prooved [1] that a family of linear mappings $B(t) = f(t)A + g(t)I$ where I is the identical mapping of V gives us the same contractions of algebra L as the family $C(t) = t^n A + t^{n+1} I$ where n is an integer greater than -2. The case $n = 0$ was studied earlier by Saletan and the case of natural number n was discused by Levy-Nahas [2].

---

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

Author gratitudes Raziskovalna skupnost Slovenije for the support, contract number C1-0501-101-1988.

Further more it is possible to assume that $A|_{V_1} = I|_{V_1}$ because other linear mappings give us contracted algebras isomorphical to the ones obtained this way. The proof of this statement as well as the conditions for the existence of the contracted algebra were given by Mimura [1]. If $n = -1$ then L^2 must lay in V_1 and $(AL)^2$ must be equal to 0. For nonnegative n there are the following conditions: acting by A n times on each of the elements $[w, x]$, $[x, Ay] - A[x, y]$ and $[Ay, Az] - A(\delta A)(y, z)$, where $w, x \in V_1$, $y, z \in V_0$ and δ is a coboundary operator, acting on space $C^1(L, L)$ we must always recieve an element from V_1. When these conditions are satisfied we recieve contracted algebras with the following comutators (elements w, x, y, z as in conditions above):

$[w, x]^\wedge = 0$, $[x, y]^\wedge = [x, y]$, $[y, z]^\wedge = [Ay, z] + [y, Az]$ if $n = -1$,

$[w, x]^\wedge = [w, x]$, $[x, y]^\wedge = [x, y]_0 + [x, Ay]_1$, $[y, z]^\wedge = [Ay, Az]_1 + (\delta A)(y, z)_0$ if $n = 0$ and

$[w, x]^\wedge = (-A)^{n-1}[w, x]$, $[x, y]^\wedge = (-A)^{n-1}([x, Ay] - A[x, y])_0$,

$[y, z]^\wedge = (-A)^{n-1}([Ay, Az] - A(\delta A)(y, z))_0$ for all natural numbers n.

2. Examples

As an example of Lie algebra contraction we'll study the algebras obtained by this technics from the nilpotent part of a classical simple Lie algebra A_3. Denote the basis of this algebra as $e_1 = E_{1,2}$, $e_2 = E_{2,3}$, $e_3 = E_{1,3}$, $e_4 = E_{3,4}$, $e_6 = E_{2,4}$ and $e_7 = E_{1,4}$. Than the bracket operation in A_3^+ looks like this:

$$[e_i, e_j] = \begin{cases} e_{i+j}, \text{ if } i+j \in \{3, 6, 7\} \text{ and } i<j \\ -e_{i+j}, \text{ if } i+j \in \{3, 6, 7\} \text{ and } i>j \\ 0 \quad \text{for all other indexes } i \text{ and } j \end{cases}$$

a) Let e_3, e_6 and e_7 be the eigenvectors of operator A with eigenvalue 1 and $Ae_4 = e_2$, $Ae_2 = e_1$ and $Ae_1 = 0$. Then the Mimura's contraction conditions are satisfied for all integer $n>-2$ and we recieve the following nonisomorphical algebras

If $n = -1$: $[e_1, e_4]^\wedge = e_3$, $[e_1, e_6]^\wedge = [e_3, e_4]^\wedge = e_7$

If $n = 0$: $[e_2, e_4]^\wedge = e_3$, $[e_2, e_6]^\wedge = e_7$. Other commutators of basical elements are in both cases equal to 0. The bracket operation is extended to the whole algebra by bilinearity and anticommutativity laws.

Finaly for all natural numbers n the contracted algebra is abelian.

b) If we now define operator A so that the elements e_1, e_2 and e_6 will be its eigenvectors corresponding to the eigenvalue 1, while elements e_3, e_4 and e_7 will lay in the kernel of A the contracted algebra will exist only for natural numbers n and will be isomorphical to the second algebra from case a) if $n = 1$. For $n > 1$ the contracted algebra is abelian again.

3. Contractions generated by derivations

An interesting situation appears if we suppose that the operator A generating a contraction is itself a derivation of algebra L. That means that for each pair of elements $x, y \in L$ we have $A[x, y] = [Ax, y] + [x, Ay]$.

THEOREM 1. *If A is a derivation of algebra L than it will generate a contraction of this algebra if and only if it satisfies the following conditions:*

$L^2 \subset V_1$ *and* $(AL)^2 = 0$ *for* $n = -1$ *and*
V_1^2, $[V_0, AV_1]$, $(AV_0)^2$ *are translated into* V_1 *by n-th power of operator* A *for all nonnegative integers* n.

Proof. The prescribed conditions as well as the next corollary follow out from general conditions for operators generating contractions (see [1]) if we use the definition of the derivation as an 1-cocycle given above.

COROLLARY. *If A is a derivation of algebra L generating a contraction of this algebra then the new bracket operation looks as follows*

$[w, x]^{\wedge} = 0$, $[x, y]^{\wedge} = A^{-1}[Ax, y]$ *and* $[y, z]^{\wedge} = [y, z]$ *for* $n = -1$

$[w, x]^{\wedge} = A^{-1}[Aw, Ax]$, $[x, y]^{\wedge} = A^{-1}[Ax, Ay]_1 + [Ax, y]_0$ *and*
$[y, z]^{\wedge} = A^{-1}[Ay, Az]_1$ *for* $n = 0$

$[w, x]^{\wedge} = (-A)^{n-1}[Aw, Ax]_0$, $[x, y]^{\wedge} = -(-A)^{n-1}[A^2 x, y]_0$ *and*
$[y, z]^{\wedge} = (-A)^{n-1}[Ay, Az]_0$ *for positive* n.

Here $w, x \in V_1$ *and* $y, z \in V_0$.

If we apply to this expresions the definition of a derivation and the conditions of Theorem 1, we can get a more compact description for the new operation:

if $n = -1$ then V_1 becomes abelian other commutators are unchanged
if $n = 0$ then $[u, v]^{\wedge} = A^{-1}[Au, Av]_1$ for all $u, v \in V$, while for positive n and the same u, v we have $[u, v]^{\wedge} = (-A)^{n-1}[Au, Av]_0$.

4. Contractions of free nilpotent Lie algebras

Let L^* be a free Lie algebra with N generators $e_1, e_2, \ldots, e_N$. Then the factor algebras $L/(L^*)^{d+1}$, $d > 1$ we call free nilpotent Lie algebras with N generators of order d. We define a linear mapping A on the generators of this algebra so that the first k of them will lay in kernel of some power of operator A and the other will be its eigenvectors with eigenvalue 1. It is posssible to extend in unique way this operator to the whole algebra so that it will become a derivation and we'll denote this extension by A. What we are going to do now is to describe all contractions of free nilpotent Lie algebras that can be obtained by such operators.

THEOREM 2. If $n = -1$ (Mimura's contraction) than the only possibility is $N = d = 2$ and the contracted algebra is isomorphical to the initial.

Proof. In this case according to the conditions of Theorem 1 L^2 must be included in V_1, while the square of the last one must be 0. So $N = d = 2$ really is the only possibility.

THEOREM 3. If $n = 0$ (Saletan's contraction) then $AV_0 = 0$ or $d = 3$. In first case we recieve a free nilpotent Lie algebra of order d with $n-k$ generators.

Proof. From Theorem 1 we have $(AV_0)^2 = 0$, so the dimension of AV_0 must no be greater then 1. If it is 0, than the contracted algebra is obtained by simply throwing away the first k generators. In the second case $\dim V_0 = 2$ and d must be 3. The generator that is eigenvektor of operator A for eigenvalue 0 will lay in the center of contracted algebra L^*.

THEOREM 4. For positive n the contracted algebra always exists and its structure depends on the structure of the nilpotent part of operator A.

Proof. The first two conditions from Theorem 1 are satisfied autimatically but for the last one we must have $A^n(AV_0)^2 = 0$. We'll recieve nonabelian algebra only if $U = A^m V_0 \neq 0$ while $AU = 0$. If U is spanned by element e_1 and $A^{m-1}V_0$ by Ae_1 than $n = dm - 3$ and the only nonzero commutator in L^* is $[e, [e, \ldots [e, Ae]\ldots]]^* = [e_1, [e_1 \ldots [e_1, A^{m-1}e]\ldots]]$ where $A^m e = e_1$. If there exists such a linearly independent with Ae vector f that V_0 is a direct sum of $\operatorname{Ker} A^{m-1}$ and the subspace spannned with

Ae, f than we have as much nonzero commutators in contracted algebra as much such linearly independent vectors exist and n must be equal to dm - 2.

The last case that happens is when the dimenson of Ker A^m is dim V_k - k. In this case to recieve a nonabelian contracted algebra n must be dm - 1 and the number of nontrivial commutators in the new algebra is equal to

$$\sum_{l=1}^{\left[\frac{d-1}{2}\right]} r(l)\, r(d-l) + (d-1-2\left[\frac{d-1}{2}\right])\binom{v(\frac{d}{2})}{2}$$

where r(l) is the number of basical elements of lenght l generated by k generators.

REFERENCES

1 F. Mimura, Contractions of Lie algebras, Bull. of Kyushu Techn. Institute 19 (1972), 38 - 51.

2 M. Levy-Nahas, Deformation and Contraction of Lie algebras, J. of Math. Physics 8 (1967), 1211 - 1222.

PEDAGOŠKA FAKULTETA
62000 MARIBOR
Koroška c. 160
Yugoslavia

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

ON A GENERALIZATION OF TRANSITIVE QUASIGROUPS

Mirko Polonijo

Abstract. The present note shows that for every quasigroup $(Q,\cdot)$ possessing an element $0 \in Q$ such that the identity $ab\cdot c = a\cdot(c\cdot 0b)$ (resp. $a\cdot bc = (b0\cdot a)\cdot c$) holds, there is a group (Q,o) and its involutory antiautomorphism φ satisfying $xy=xo\varphi y$ (resp. $xy=yo\varphi x$). This is a generalization of a result for right (resp. left) transitive quasigroups, in which case there is a group (Q,o) such that $xy=xoy^{-1}$ (resp. $xy=yox^{-1}$).

J.M.Cardoso and C.P.da Silva defined in [1] the notion of Ward quasigroup as a quasigroup $(Q,\cdot)$ which satisfies the following constraits:

(W1) There is $0 \in Q$ such that $aa=0$ for all $a \in Q$

(W2) $ab\cdot c=a\cdot(c\cdot 0b)$, for the element 0 postulated in (W1) and all $a,b,c \in Q$.

They proved that if $(Q,\cdot)$ is a Ward quasigroup and o the binary operation on Q defined by $xoy=x\cdot 0y$ then (Q,o) is a group and $xy=xoy^{-1}$, where y^{-1} is the inverse of $y \in Q$

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

in the group (Q,o). Conversely, if (Q,o) is a group and the binary operation $\cdot$ on Q defined by $xy = xoy^{-1}$ then it is easy to check that $(Q,\cdot)$ is a Ward quasigroup.

The author proved in [3] that the axioms (W1) and (W2) in the definition of a Ward quasigroup could be replaced by one axiom, i.e. by the law of right transitivity, [2]:

(RT) $\qquad ac\cdot bc = ab$, for all $a,b,c \in Q$.

Since the law of right transitivity is the (13)-conjugate of the associativity, Cardoso-da Silva's result follows immediately.

Analogously, one can prove that the law of left transitivity

(LT) $\qquad ca\cdot cb = ab$, for all $a,b,c \in Q$

in a quasigroup $(Q,\cdot)$ is equivalent to (W1) and (W2'), where

(W2') $a\cdot bc = (b0\cdot a)\cdot c$, for the element 0 postulated in (W1) and all $a,b,c \in Q$.

The purpose of this note is to describe the structure of a quasigroup $(Q,\cdot)$ which satisfies only (W2), resp. (W2'), i.e. more precisely, for which the following condition is valid:

(W) There is $0 \in Q$ such that $ab\cdot c = a\cdot(c\cdot 0b)$ for all $a,b,c \in Q$,

respectively,

(W') There is $0 \in Q$ such that $a\cdot bc=(b0\cdot a)\cdot c$, for all $a,b,c \in Q$.

The following example shows that (W) does not imply (W1). Take the symmetric group (S_3,o) and define a new binary operation $\cdot$ on S_3 by the equality $xy=xoaoy^{-1}oa$, for $a=(23)$ and all $x,y \in S_3$. It is easy to check that $(S_3,\cdot)$ satisfies (W), taking the identity permutation for 0, but (W1) does not hold since $(12)\cdot(12)=(132)\neq(123)=$ $=(132)\cdot(132)$.

Let us suppose that $(Q,\cdot)$ is a quasigroup in which (W) holds. Putting $a=0$ in (W), it follows $0b\cdot c=0\cdot(c\cdot 0b)$, which implies

(A) $$xy = 0\cdot yx$$

for all $x,y \in Q$. Hence $0y=0\cdot y0$, i.e. $y0=y$ which means that $(Q,\cdot)$ is a right loop and 0 its right unit.

Therefore, if $(Q,\cdot)$ is a loop then 0 is its unit and $ab\cdot c=a\cdot cb$ for all $a,b,c \in Q$. Since $ab\cdot a=a\cdot ab$, $(Q,\cdot)$ is commutative and the associativity follows, i.e. $(Q,\cdot)$ is an abelian group.

Similarly, if (W') is valid for a quasigroup $(Q,\cdot)$ then it is a left loop with the left unit 0 and

(A') $$xy = yx\cdot 0$$

for $x,y \in Q$. It implies that a loop $(Q,\cdot)$ satisfying (W') is an abelian group too.

Obviously, for any abelian group the constraints (W) and (W') are fulfilled.

Now, we shall call our attention to the quasigroups satisfying (A), resp. (A').

PROPOSITION 1. Let $(Q,\cdot)$ be a quasigroup for which exists an element $0 \in Q$ such that (A) (resp. (A^1)) holds for all $x,y \in Q$. Then there is a loop (Q,o) and its involutory antiautomorphism φ such that

$$xy = xo\varphi y \quad (\text{resp. } xy = yo\varphi x).$$

Proof. If (A) is true, define the bijection $\varphi: Q \to Q$ by

$$\varphi x = \varphi(x) = 0x ,$$

and the binary operation o on Q by

$$xoy = x\cdot\varphi y .$$

Because of $0\cdot 0x = x$, we have $\varphi^2 = 1$, where 1 is the identity on Q, and therefore

$$xo\varphi y = x\cdot\varphi^2 y = xy .$$

Since

$$xo0 = x\cdot 00 = x0 = x ,$$

$$0ox = 0\cdot 0x = x ,$$

(Q,o) is a loop, and it remains to prove that φ is an antiautomorphism. Indeed, we get

$$\varphi(xoy) = \varphi(x\cdot\varphi y) = \varphi y\cdot x = \varphi y\cdot\varphi(\varphi x) = \varphi yo\varphi x .$$

The proof for the case (A^1) is similar and we omit it. We shall do the same in the sequel.

COROLLARY 1. If $(Q,\cdot)$ is a quasigroup and there is $0 \in Q$ for which $xx = 0$ and (A) (resp. (A^1)) are valid for all $x,y \in Q$, then there is a loop (Q,o) such that

$$xy = xoy^{-1} \quad (\text{resp. } xy = yox^{-1}),$$

where y^{-1} is the right inverse of y in (Q,o).

Proof. Let (Q,o) be the loop defined in the previous proposition. Then 0 is its unit and we have to prove $\varphi y = y^{-1}$. Since $yoy^{-1}=0$, i.e. $y\cdot 0y^{-1}=0$, it follows $0y^{-1}=y$ because of $yy=0$, and therefore $\varphi(y)=0y=0\cdot 0y^{-1}=y^{-1}$. Note that the left inverse ${}^{-1}y$ of y is equal to the right inverse y^{-1}, since $y^{-1}oy=0$, i.e. $y^{-1}\cdot 0y=0$ implies $y^{-1}=0y$.

PROPOSITION 2. If (Q,o) is a loop, φ its involutory anti-automorphism and $\cdot$ the binary operation on Q defined by

$$xy = xo\varphi y \quad (\text{resp. } xy = yo\varphi x)$$

then there is $0 \in Q$ such that (A) (resp. (A')) is fulfilled.

Proof. If 0 is the unit of (Q,o) then we get $\varphi x = 0x$ and hence

$$0\cdot yx = \varphi(yx) = \varphi(yo\varphi x) = \varphi^2 xo\varphi y = xo\varphi y = xy .$$

COROLLARY 2. Let (Q,o) be a loop in which the identities

$$(x^{-1})^{-1} = x , \quad (xoy)^{-1} = y^{-1}ox^{-1}$$

hold and define the binary operation $\cdot$ on Q by

$$xy = xoy^{-1} \quad (\text{resp. } xy = yox^{-1}).$$

Then there is $0 \in Q$ such that $xx=0$ and (A) (resp. (A')) are valid.

Since the condition (W) (resp. (W^1)) implies (A) (resp. (A^1)), we can apply Proposition 1 and its proof to a quasigroup $(Q,\cdot)$ satisfying (W) (resp. (W^1)), and prove that the loop (Q,o) defined by $xoy=x\cdot\varphi y$ (resp. $xoy=y\cdot\varphi x$), where $\varphi x=0x$, (resp. $\varphi x=x0$), is a group. Namely, the binary operation o is associative:

$$(aob)oc = (a\cdot\varphi b)\cdot\varphi c \overset{(W)}{=} a\cdot(\varphi c\cdot\varphi^2 b). =$$
$$= a\cdot(\varphi c\cdot b) \overset{(A)}{=} a\cdot\varphi(b\cdot\varphi c) = ao(boc) .$$

Therefore, taking into account Corollary 1, too, we have the following proposition.

PROPOSITION 3. *If $(Q,\cdot)$ is a quasigroup satisfying (W) (resp. (W^1)) then there is a group (Q,o) and its involutory antiautomorphism φ such that*

$$xy = xo\varphi y \quad (\text{resp. } xy=yo\varphi x) .$$

In addition, if $xx=0$ holds, which means that $(Q,\cdot)$ is a right (resp. left) transitive quasigroup, then φy is the inverse of y in (Q,o), i.e.

$$xy = xoy^{-1} \quad (\text{resp. } xy = yox^{-1}).$$

The converse holds too:

PROPOSITION 4. *Let (Q,o) be a group, φ its involutory antiautomorphism and $\cdot$ the binary operation on Q defined by*

$$xy = xo\varphi y \quad (\text{resp. } xy=yo\varphi x).$$

Then (W) (resp. (W^1)) is fulfilled in the quasigroup $(Q,\cdot)$.

Proof. If 0 is the unit of the group (Q,o), then we have $\varphi x = 0x$ and therefore

$$ab \cdot c = (ao\varphi b)o\varphi c = ao(\varphi bo\varphi c) =$$
$$= ao\varphi(cob) = a\cdot(co\varphi^2 b) = a\cdot(c\cdot\varphi b) =$$
$$= a\cdot(c\cdot 0b) .$$

If the group (Q,o) in the previous proposition is abelian, then we get

$$ab = ao\varphi b = \varphi boa = \varphi b\cdot\varphi a = 0b\cdot 0a ,$$

i.e. $ab = 0b\cdot 0a$ (resp. $ab = b0\cdot a0$) for all $a,b \in Q$. Conversely, let $(Q,\cdot)$ be a quasigroup satisfying the assumptions of Proposition 3 and the identity $ab = 0b\cdot 0a$ (resp. $ab = b0\cdot a0$). Then the group (Q,o) defined in the proof of Proposition 3 is abelian, since

$$aob = a\cdot\varphi b = \varphi^2 b\cdot\varphi a = b\cdot\varphi a = boa .$$

REFERENCES:

[1] Cardoso,J.M. and da Silva,C.P., On Ward quasigroups, An.st.Univ.Iasi, s.I a Math., 2461978), 231-233.

[2] Denes,J. and Keedwell, A.D., Latin squares and their applications, Akademiai Kiado, Budapest, 1974.

[3] Polonijo, M., A note on Ward quasigroups, An.st.Univ.Iasi, s.I a Math., 32 (1986), 5-10.

Mirko Polonijo
Department of Mathematics
University of Zagreb
p.o.box 187, 41001 Zagreb
Yugoslavia

PUTTING N LOOPS TOGETHER [1]

Slaviša B. Prešić

Abstract. We give a BASIC program by which one implements the following n-loop algorithm

(1)
```
For i_1 = A_1 to B_1
:
For i_n = A_n to B_n
C(i_1,...,i_n)
NEXT i_n,...,i_1
```

where $n, A_i, B_i, C(i_1,\ldots,i_n)$ are input-objects.

At first consider the following general equivalence

(2)
```
For i=A to B                    i=A
C(i)            <----->         (*) C(i)
Next i                          If i<B then i=i+1:goto (*)
```

Suppose now that $n, A_i, B_i, C(i_1,\ldots,i_n)$, the objects appearing i (1), are given. Then by means of (2) one can easily prove that the algorithm (1) is logically equivalent to the following one:

(3)
```
i_1=A_1
:
i_r=A_r
:
i_n=A_n
(*)     C(i_1,...,i_n)
If i_n<B_n then i_n=i_n+1:goto (*)
:
If i_r<B_r then i_r=i_r+1:i_(r+1)=A_(r+1):...:i_n=B_n:goto (*)
:
If i_1<B_1 then i_1=i_1+1:i_2=A_2:...:i_n=B_n:goto (*)
```

[1] This paper is in final form and no version of it will be submitted for publication elswhere.

To implement (3) in BASIC instead of $i_1,\ldots,i_n$ we shall employ the following array notations F(1),...,F(N). Accordingly a BASIC program for the algorithm (1) reads:

```
10 DIM F(1000),A(1000),B(1000)[2]
15 INPUT N
20 FOR I=1 TO N:INPUT A(I),B(I):NEXT
50 FOR I=1 TO N:F(I)=A(I):NEXT
60 C[3]
70 FOR J=N TO 1 STEP -1
80 IF F(J)<B(J) THEN F(J)=F(J)+1:GOSUB 200:GOTO 60
90 NEXT J
100 END
200 FOR I=J+1 TO N:F(I)=A(I):NEXT I
210 RETURN
```

EXAMPLE. Here we list a program for printing all functions F:(1,...,k) --> (1,...,n) with input-variables k,n.

```
10 DIM F(1000)
20 INPUT K,N
30 FOR I=1 TO K:F(I)=1:NEXT
35 CN=CN+1:PRINT CN;" function is:"
40 FOR S=1 TO K-1:PRINT "F(";S;")=";F(S);",";:NEXT S
45 PRINT "F(";S;")=";F(S)
50 PRINT
100 FOR R=K TO 1 STEP -1
120 IF F(R)<N THEN F(R)=F(R)+1:GOSUB 200:GOTO 35
150 NEXT R
180 END
200 FOR I=R+1 TO K:F(I)=1:NEXT I:RETURN
```

[2]The number 1000 is optional.

[3]C may be a condition (or a block) containing the parameters F(1),..., F(N).

RINGS AND MODULES, A CONSTRUCTIVE VIEW

Daniel A. Romano

Abstract. A coequality relation on the set was introduced and studied by the author in the papers [7],[8],[9] and [10]. Generalizing classical results on rings and modules and some constructive results of Richman ([6]) and Ruitenburg ([11]), general theory of rings and modules in Bishop's constructive mathematics in nondiscrete case was demonstrated in this paper. Using the technique of [7] we explained some results of modules and homomorphisms of modules, and finite and infinite sums of modules and their applications.

0. Introduction

For all notions of sets and functions in Bishop's constructive mathematics which we use here, the reader is referred to the papers [1],[2],[3],[9] and [10]. The papers [5] and [13] contain elementary definitions and basic facts about finite and infinite sets and the papers [4],[6],[7],[8],[11] and [12] contain algebraic structures which will be used here.

1. Preliminaries

In classical mathematics the identity relation is completely neutral, it does not influence, and it is not influenced by the proper mathematics. The situation is completely diferent in Bishop's constructive mathematics.

I am thankful to Professor Fred Richman (Las Cruces, New Mexico State University, USA) for his help and suggestions for this paper.

AMS Subject Classification (1980): Primary 03 F 65; Secondary 13 A 15, 13 C 99, 13 E 15.

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

This paper is a part of research work "Prsteni i moduli, konstruktivno shvatanje (opšta teorija)" supported by the Viša tehnička škola u Bihaću (NIR: 09-2174/85).

1.1. Equality. An equality relation "=" on the class X satisfies the folowing conditions:

(1) $(\forall x \in X)(x = x)$,

(2) $(\forall xy \in X)(x = y \longrightarrow y = x)$,

(3) $(\forall xyz \in X)(x = y \wedge y = z \longrightarrow x = z)$.

How should we understand an equality x = y? There seem to be two possible senses: (i) both x and y exist and are equal; and (ii) if either x or y exists, so does the other and they are equal.

Let X be a class, that is, let us describe what is the construction K_X of a class X. Often, the construction K_X of a class X and our intention at the selection of the K_X suggests a definition of the equality relation which is not appropriate for investigation or it has no property which we excepted from it. Therefore, we define an ordering relation on equality relations $=_1 \prec =_2$ as follows:

$$=_1 \prec =_2 \longleftrightarrow (\forall xy \in X)(x =_2 y \longrightarrow x =_1 y).$$

1.2. Sets. Bishop ([11]) describes the construction of a set as a three stage process. First, one must describe what must be done to construct an arbitrary element of X. The corresponding construction is denoted by K_X. Second, one must describe what must be done to prove that two arbitrary elements of X are equal. Third, the equality relation satisfies (1), (2) and (3). Therefore, a set is an ordered pair (X,R) comprising a class X and the equality relation R on X. We usually speak of "the set X with equality R", and write x = y instead $(x,y) \in R$.

Let (X,=) be a set and let Y and Z be subclasses of X. We say that Y is a subset of Z, writen $Y \subseteq Z$, iff

$$(\forall y \in Y)(\exists z \in Z)(x = y).$$

In the class N we define

$$(\forall nm \in N)(n =_N m \longleftrightarrow n = m).$$

The set $(N,=_N)$ is called the set of natural numbers.

If X and Y are classes, there is a class $X \times Y$ whose members are exactly the pairs (x,y) such that x belongs to X and y belongs to Y. If $(X,=_X)$ and $(Y,=_Y)$ are sets, then there is a natural equality relation on $X \times Y$ defined by

$$(x,y) =_d (u,v) \longleftrightarrow x =_X u \wedge y =_Y v ,$$

which turns $X \times Y$ into a set.

If $(X,=)$ is a set and if

$$(\forall xy \in X)(\neg\neg(x = y) \longrightarrow x = y),$$

then we say that the equality relation $=$ on the class X is stable. The equality relation on the set $(N,=_N)$ is stable.

1.3. Diversity. Let $(X,=)$ be a set and let x,y be arbitrary elements of X. Inequality on the set $(X,=)$ is defined by $\neg(x = y)$, where $x,y \in X$. The inequality relation on the set $(X,=)$ satisfies the folowing conditions:

$$(\forall x \in X)\neg\neg(x = x),$$

$$(\forall xy \in X)(\neg(x = y) \longrightarrow \neg(y = x)),$$

$$(\forall xyz \in X)(\neg(x = z) \wedge Ey \longrightarrow \neg(x = y \wedge y = z)),$$

where E is the existence predicate in Scott's sense ([11],[12]).

In Bishop's constructive mathematics there is a "positive" theory of inequalities. We decide to use a diversity relation "$\neq$", in Richman's sense ([4]), defined on $(X,=)$ by

$$(\forall x \in X)\neg(x \neq x),$$

$$(\forall xy \in X)(x \neq y \longrightarrow y \neq x),$$

$$(\forall xyz \in X)(x = y \wedge y \neq z \longrightarrow x \neq z).$$

Clearly

$$(\forall xy \in X)(x \neq y \longrightarrow \neg(x = y)),$$

but the converse, in general, is not valid. For the diversity relation, in Richman's sense,

$$(\forall xy \in X)(\neg(x \neq y) \longrightarrow x = y)$$

is not valid. How are these axioms obtained? If we go back to 1.1. the axioms for the equality relations, we note the obvious parallelism. The first axiom we understand as irreflexivity. The second axiom we understand as symmetry. The third axiom we understand as compatibility. In reading these axioms, "$\neq$" must be taken as a symbol in itself, and "$x \neq y$" must not be read as an abbrevation for $\neg(x = y)$. Therefore, we define the ordering relation on diversity relations $\neq_1 \prec \neq_2$ as follows:

$$\neq_1 \prec \neq_2 \longleftrightarrow (\forall xy \in X)(x \neq_2 y \longrightarrow x \neq_1 y).$$

1.4. Functions. Let $(X,=_X,\neq_X)$ and $(Y,=_Y,\neq_Y)$ be sets.

A mapping $f:X \longrightarrow Y$ is a function iff

(f) $(\forall x x' \in D(f))(x =_X x' \longrightarrow f(x) =_Y f(x'))$,

(swf) $(\forall x x' \in D(f))(f(x) \neq_X f(x') \longrightarrow x \neq_X x')$.

A weaker notion of a function is given by the condition (f) and

(wf) $(\forall x x' \in D(f))(\neg(f(x) =_Y f(x')) \longrightarrow \neg(x =_X x'))$.

If the domain of f is A, and the equality in A is stable, then this weaker notion of the function is given by (f). In general, the condition (swf) is not equal to the condition (f).

If $(X,=)$ is a set, a predicate on X is a function A from X to the set $(\Omega, \longleftrightarrow)$. Thus, for every element x in X, A(x) is a proposition, and if $x = x'$, then $A(x) \longleftrightarrow A(x')$.

Let $(X,=,\neq)$ be a set and let A be a predicate on a class X. Corresponding to A, we have the subset $S \equiv \{x \in X : A(x)\}$. To construct an element of S it is necessary first to construct an element x of X, and then to prove A(x). Two elements of S are equal as elements on $(X,=,\neq)$. Hence, it is not quite correct to say that an element of S is an element of X; it is more than an element of X, since it carries the additional structure of a proof of A(x). This construction describes a construction of the class 2^X which consists of all subsets of the set X. If Y and Z are subsets of X, we define

$$Y =_2 Z \longleftrightarrow Y \subseteq Z \wedge Z \subseteq Y.$$

Let $(X,=,\neq)$ be a set and Y one of its subsets. We define

$$(\forall x \in X)(x \# Y \longleftrightarrow (\forall y \in Y)(y \neq x)).$$

This notation is new in constructive mathematics and it makes us possible to determine the diversity relation in the set 2^X as follows:

$$Y \neq_2 Z \longleftrightarrow (\exists y \in Y)(y \# Z) \vee (\exists z \in Z)(z \# Y).$$

A description of a construction of a function $f:X \longrightarrow Y$ consists a class $F(X,Y)$ of all functions from X to Y. If $f,g \in F(X,Y)$, we define

$$f =_F g \longleftrightarrow D(f) =_2 D(g) \wedge Imf =_2 Img \wedge (\forall x \in D(f))(f(x) =_Y g(x)).$$

Remark. 2^X is just $F(X,\Omega)$. Note also that the power-set of a singleton is simply Ω.

1.5. The basic definitions. Let $(X,=_X,\neq_X)$ and $(Y,=_Y,\neq_Y)$

be sets and $f:X \longrightarrow Y$ a function. For a function f we say that is

- <u>total</u> iff
  $(\forall x \in X)(Ef(x) \wedge f(x) \in Y)$;
- <u>injective</u> iff
  $(\forall x x' \in D(f))(f(x) =_Y f(x') \longrightarrow x =_X x')$;
- an <u>embedding</u> iff ([11])
  $(\forall x x' \in D(f))(x \neq_X x' \longrightarrow f(x) \neq_Y f(x'))$;
- <u>surjective</u> iff
  $(\forall y \in Y)(Ex \wedge x \in D(f) \wedge y =_Y f(x))$;
- <u>bijective</u> iff a function f is total, injective and surjective.

Let $(X,=)$ be a set. For an element x of X we say that it is <u>discrete</u>, iff

$$(\forall y \in X)(y = x \vee \neg(y = x)).$$

For the set $(X,=)$ we say that it is <u>discrete</u> iff every element of X is discrete, i.e.

$$(\forall xy \in X)(x = y \vee \neg(x = y)).$$

Let X be a class and Y its subclass. Then Y is <u>detachable</u> in X iff ([1])

$$(\forall x \in X)(x \in Y \vee \neg(x \in Y)).$$

When used as notation for functional relations, " $\longrightarrow$ ", " $\longrightarrow\!\!\!\!\rightarrow$ " and " $\rightarrowtail$ " take their familiar meanings:

(i) $f:X \longrightarrow Y$ iff f is a mapping from X into Y;

(ii) $f:X \longrightarrow\!\!\!\!\rightarrow Y$ iff f is a mapping from X onto Y;

(iii) $f:X \rightarrowtail Y$ iff f is an injective mapping from X into Y.

Then

(a) The set X is <u>strictly finite</u> iff
$(\exists n \in N)(\exists f)(f:\bar{n} \rightarrowtail X)$;

(b) The set Y is <u>finite</u> iff
$(\exists n \in N)(\exists f)(f:\bar{n} \longrightarrow\!\!\!\!\rightarrow Y)$;

(c) The set Z is <u>subfinite</u> iff
$(\exists n \in N)(\exists A \subseteq \bar{n})(\exists f)(f:A \longrightarrow\!\!\!\!\rightarrow X)$.

<u>Remark.</u> For details about above see the papers by Troelstra, Grayson and McCarty ([14],[2],[5]).

2. Operation relations

DEFINITION 2.1. Let $(X,=_X,\neq_X)$, $(Y,=_Y,\neq_Y)$ and $(Z,=_Z,\neq_Z)$ be sets and let $f \in F(X \times Y,Z)$ be a total function.

a) If $Z = Y$, then we say that f is a left external operation on Y over X;

b) If $Z = X$, then we say that f is a right external operation on X over Y;

c) If $X = Y = Z$, then we say that f is an internal operation on X.

d) The structure $(X,=,\neq,f)$ is called a grupoid, where $(X,=,\neq)$ is a set and where f is an internal operation on X;

e) Let $(X,=,\neq,f)$ be a grupoid which has an element e. We say that X is a monoid iff it satisfies the following properties:

$$(\forall xyz \in X)(f(x,f(y,z)) = f(f(x,y),z)),$$
$$(\forall x \in X)(f(x,e) = x = f(e,x));$$

f) A grupoid $(X,=,\neq,f)$ is called a group iff it has an element e and satisfies the following conditions:

$$(\forall xyz \in X)(f(x,f(y,z)) = f(f(x,y),z)),$$
$$(\forall x \in X)(f(x,e) = x = f(e,x)),$$
$$(\forall x \in X)(\exists x'' \in X)(f(x,x'') = e = f(x'',x)).$$

The group $(X,=,\neq,f)$ is Abelian if it moreover satisfies

$$(\forall xy \in X)(f(x,y) = f(y,x)).$$

LEMMA 2.1. If any of the elements of an Abelian group $(G,=,\neq,+)$ is discrete, then the group G is discrete.

Proof. See [7], Lemma 2.1.

LEMMA 2.2. Let $(G,=,\neq,+)$ be an Abelian group. Then

$$(\forall xyz \in G)(x \neq z \longrightarrow x \neq y \vee y \neq z).$$

Proof. See [7], Lemma 2.2.

DEFINITION 2.2. A ring is a set $(A,=,\neq)$ which has an element o (zero) and two internal binary operations "+" and "." (total functions from $A \times A$ to A). These operations have the following properties (we write ab instead of a.b):

$$(\forall abc \in A)(a+(b+c) = (a+b)+c),$$
$$(\forall a \in A)(a+o = a),$$
$$(\forall a \in A)(\exists b \in A)(a+b = o),$$
$$(\forall ab \in A)(a+b = b+a),$$
$$(\forall abc \in A)(a(bc) = (ab)c),$$
$$(\forall abc \in A)(a(b+c) = ab+ac),$$
$$(\forall ab \in A)(ab = ba).$$

Since "+" and "." are total functions, we have

$$a = a' \wedge b = b' \longrightarrow a+b = a'+b',$$

$$a+b \neq a'+b' \longrightarrow a \neq a' \vee b \neq b'$$

and

$$a = a' \wedge b = b' \longrightarrow ab = a'b',$$

$$ab \neq a'b' \longrightarrow a \neq a' \vee b \neq b'.$$

A ring A has a unit of A iff

$$1 \in A,$$

$$o = 1 \vee o \neq 1,$$

If $o = 1$, then $A = (o)$.

If $o \neq 1$, then $(\forall a \in A)(a.1 = a)$.

LEMMA 2.3. Let $(A,=,\neq,+,.)$ be a ring. Then

$$(\forall ab \in A)(ab \neq o \longrightarrow a \neq o \wedge b \neq o).$$

Proof. See [12], Proposition 8.4.10.

Examples I: a) The sets Z, Q and R are rings.

b) The ring of formal sequences $A[[X]]$ over the ring A is the set $F(N,A)$ with equality and diversity relations given by

$$f =_F g \longleftrightarrow (\forall n \in N)(f(n) =_A g(n)),$$

$$f \neq_F g \longleftrightarrow (\exists n \in N)(f(n) \neq_A g(n))$$

and the operations given by

$$(\forall n \in N)((f+g)(n) =_A f(n)+g(n)),$$

$$(\forall n \in N)((fg)(n) =_A \sum_{i=1}^{n} f(i)g(n-i)).$$

c) The ring of polinomials $A[X]$ is the subset of $A[[X]]$ defined by

$$f \in A[X] \longleftrightarrow (\exists n \in N)(\forall j \in N)(f(n+j) =_A o).$$

DEFINITION 2.3. Let $(A,=,\neq,+,.)$ be a ring and let $(S,=,\neq)$ be its subset.

a) S is an ideal of A iff

$$o \in S,$$

$$a \in S \wedge b \in S \longrightarrow a+b \in S,$$

$$a \in S \longrightarrow -a \in S,$$

$$a \in S \vee b \in S \longrightarrow ab \in S.$$

$(A,=_A,\neq_A,+,\cdot)$. Then

1. The equality relation $=_M$ on M is a congruence on M and the set $(o) \equiv \{x\in M: x =_M o\}$ is a submodule of M.

2. The diversity relation $\neq_M$ on M is a cocongruence on M and the set $M_o \equiv \{x\in M: x \neq_M o\}$ is a cosubmodule of M.

Examples VI: 1. The set $\{k\in Z: k$ is not divisible by $n\}$ for $\neg(n =_N o)$ is a cosubmodule of Z.

2. The set $\{f\in \mathcal{C}(R,R): |f(o)| > o\}$ is a cosubmodule of the R-module of continuous functions from R to R.

3. $\emptyset$ is a cosubmodule of M.

Remarks. 1. If the cosubmodule of M is inhabited, then

$$((\exists x\in M)(x\in H) \longrightarrow) \; 1.x\in H \longrightarrow 1 \neq_A o.$$

2. Let C be a cocongruence on the A.module M. We have

$$(ax,by)\in C \longrightarrow a \neq_A b \vee (x,y)\in C.$$

First, we have

$$(x,y)\in C \longleftrightarrow (x-y+y,o+y)\in C \longrightarrow (x-y,o)\in C \vee (y,y)\in C \longrightarrow$$
$$\longrightarrow (x-y,o)\in C,$$

and

$$(x-y,o)\in C \longleftrightarrow (x-y,y-y)\in C \longrightarrow (x,y)\in C \vee (-y,-y)\in C \longrightarrow$$
$$\longrightarrow (x,y)\in C.$$

Second, we have

$$(ax,by)\in C \longleftrightarrow (ax-by,o)\in C \longrightarrow (ax-ay+ay-by,o)\in C \longleftrightarrow$$
$$(a(x-y)+(a-b)y,o)\in C \longrightarrow (a(x-y),o)\in C \vee ((a-b)y,o)\in C \longrightarrow$$
$$\longrightarrow (a \neq_A o \wedge (x,y)\in C) \vee (a \neq_A b \wedge (y,o)\in C) \longrightarrow$$
$$\longrightarrow (x,y)\in C \vee a \neq_A b .$$

PROPOSITION 3.1. If $(M,=,\neq,+)$ is an A-module and R a relation on M, then the R is a congruence on M iff the set $H \equiv \{x\in M:(x,o)\in R\}$ is a submodule of M and $(x,y)\in R \longleftrightarrow x-y\in H$.

Proof. Routine.

PROPOSITION 3.2. Let $(M,=_M,\neq_M,+)$ be an A-module and C a relation on M. Then C is a cocongruence on M iff the set

$P = \{x \in M : (x,o) \in C\}$ *is a cosubmodule of* M *and* $(x,y) \in C \iff x-y \in P$.

Proof.

a) Let P be a cosubmodule of M. We define a relation C on M by

$$(\forall xy \in M)((x,y) \in C \iff x-y \in P).$$

Then

(1) $(x,x) \# C$, because $P \# o = x-x$;

(2) $(x,y) \in C \iff x-y \in P \implies y-x \in P \iff (y,x) \in C$;

(3) $(x,z) \in C \iff x-z \in P \iff x-y+y-z \in P \implies x-y \in P \vee y-z \in P$
$\iff (x,y) \in C \vee (y,z) \in C$;

(4) $(x+u,y+v) \in C \iff x+u-y-v \in P \implies x-y \in P \vee u-v \in P \iff$
$\iff (x,y) \in C \vee (u,v) \in C$;

(5) $(ax,o) \in C \iff ax \in P \implies a \neq_A o \wedge x \in P \iff a \neq_A o \wedge (x,o) \in C$.

b) Let C be a cocongruence on the A-module M. Then

(6) $x \in P \iff (x,o) \in C \# (o,o) \implies (x,o) \neq_d (o,o) \implies x \neq_M o$;

(7) $-x \in P \iff (-x,o) \in C \iff (o-x,x-x) \in C \iff (x-x,o-x) \in C \implies$
$\implies (x,o) \in C \vee (-x,-x) \in C \implies (x,o) \in C \iff x \in P$;

(8) $x+y \in P \iff (x+y,o) \in C \implies (x,o) \in C \vee (y,o) \in C \iff$
$\iff x \in P \vee y \in P$;

(9) $ax \in P \iff (ax,o) \in C \implies a \neq_A o \wedge (x,o) \in C \iff a \neq_A o \wedge x \in P$.

PROPOSITION 3.3. *Let* $(M,=_M,\neq_M,+)$ *be a module over a ring* $(A,=_A,\neq_A,+,\cdot)$ *and let* C *be a cocongruence on* M. *Then a relation* $\neg C$, *defined by*

$$(\forall xy \in M)((x,y) \in \neg C \iff \neg((x,y) \in C),$$

is a congruence on M *such that* $\neg C \prec =_M$.

Proof.

(1) $(x,x) \# C \implies \neg((x,x) \in C) \iff (x,x) \in \neg C$;

(2) $(x,y) \in \neg C \iff \neg((x,y) \in C) \implies \neg((y,x) \in C) \iff (y,x) \in \neg C$;

(3) $(x,y) \in \neg C \wedge (y,z) \in \neg C \iff \neg((x,y) \in C) \wedge \neg((y,z) \in C) \implies$
$\implies \neg((x,y) \in C \vee (y,z) \in C) \implies \neg((x,z) \in C) \iff (x,z) \in \neg C$;

(4) $(x,y) \in \neg C \wedge (u,v) \in \neg C \iff \neg((x,y) \in C) \wedge \neg((u,v) \in C) \implies$
$\neg((x,y) \in C \vee (u,v) \in C) \implies \neg((x+u,y+v) \in C) \iff (x+u,y+v) \in \neg C$;

(5) $a\in A \wedge (x,y)\in \neg C \iff a\in A \wedge \neg((x,y)\in C) \longrightarrow \neg((ax,ay)\in C)$
$\longleftarrow (ax,ay)\in \neg C.$

COROLLARY 3.3.1. Let M be a module over a ring A and P its cosubmodule. Then the set $\neg P \equiv \{x\in M:\neg(x\in P)\}$ is a stable submodule of the module M.

COROLLARY 3.3.2. Let $(M,=_M,\neq_M,+)$ be an A-module. Then the relation $=_s$ on M, defined by

$$(\forall xy\in M)(x =_s y \longleftrightarrow \neg(x \neq_M y)),$$

is a congruence on M such that $=_s \prec =_M$.

COROLLARY 3.3.3. Let M be an A-module. Then the set $\neg M_o \equiv \{x\in M:x =_s o\}$ is a stable submodule of M and $(o)\subseteq \neg M_o$.

DEFINITION 3.3. Let M be an A-module, R a congruence on M, and C a cocongruence on M. We say that R and C are compatible iff

$$(\forall xyz\in M)((x,y)\in R \wedge (y,z)\in C \longrightarrow (x,z)\in C).$$

THEOREM 3.4. Let $(M,=_M,\neq_M,+)$ be a module over a ring $(A,=_A,\neq_A,+,\cdot)$, R a congruence on M, C a cocongruence on M, and let R and C be compatible. Then $(M,=_1,\neq_1,+')$ is a module over a ring A with equality and diversity relations defined by

$$(\forall xy\in M)(x =_1 y \longleftrightarrow (x,y)\in R),$$
$$(\forall xy\in M)(x \neq_1 y \longleftrightarrow (x,y)\in C)$$

and operations

$$+':M\times M\ni(x,y)\longmapsto x+'y\in M, \qquad \cdot':A\times M\ni(a,x)\longmapsto a\cdot'x\in M$$

by

$$x+'y\in\{z\in M:(z,x+y)\in R\}$$
$$a\cdot'x\in\{u\in M:(u,ax)\in R\}.$$

Proof.

(1) $x =_1 y \wedge u =_1 v \longleftrightarrow (x,y)\in R \wedge (u,v)\in R \longrightarrow (x+u,y+v)\in R$
$\longrightarrow (x+'u,x+u)\in R \wedge (x+u,y+v)\in R \wedge (y+v,y+'v)\in R \longrightarrow$
$\longrightarrow (x+'u,y+'v)\in R \longleftrightarrow x+'u =_1 y+'v$;

(2) $x+'u \neq_1 y+'v \longleftrightarrow (x+'u,y+'v)\in C \longrightarrow$

$\longrightarrow (x+u,x+'u)\in R \wedge (x+'u,y+'v)\in C \wedge (y+'v,y+v)\in R \longrightarrow$

$\longrightarrow (x+u,y+v)\in C \longrightarrow (x,y)\in C \vee (u,v)\in C \longleftrightarrow x \neq_1 y \vee u \neq_1 v$;

(3) $x =_1 y \wedge a =_A b \longleftrightarrow (x,y)\in R \wedge a =_A b \longrightarrow$

$\longrightarrow (ax,ay)\in R \wedge ay =_M by \longrightarrow (ax,ay)\in R \wedge (ay,by)\in R \longrightarrow$

$\longrightarrow (ax,by)\in R \longrightarrow (a.'x,ax)\in R \wedge (ax,by)\in R \wedge (by,b.'y)\in R$

$\longrightarrow (a.'x,b.'y)\in R \longleftrightarrow a.'x =_1 b.'y$;

(4) $a.'x \neq_1 b.'y \longleftrightarrow (a.'x,b.'y)\in C \longrightarrow$

$\longrightarrow (ax,a.'x)\in R \wedge (a.'x,b.'y)\in C \wedge (b.'y,by)\in R \longrightarrow$

$\longrightarrow (ax,by)\in C \longrightarrow a \neq_A b \vee (x,y)\in C \longleftrightarrow a \neq_A b \vee x \neq_1 y$;

(5) $x+(y+z) =_M (x+y)+z \longrightarrow (x+(y+z),(x+y)+z)\in R \longrightarrow$

$(x+'(y+'z),x+(y+z))\in R \wedge (x+(y+z),(x+y)+z)\in R \wedge ((x+y)+z,(x+'y)+'z)\in R$

$\longrightarrow (x+'(y+'z),(x+'y)+'z)\in R \longleftrightarrow x+'(y+'z) =_1 (x+'y)+'z$;

...

(13) $a.'x \neq_1 o \longleftrightarrow (a.'x,o)\in C \longrightarrow$

$\longrightarrow (ax,a.'x)\in R \wedge (a.'x,o)\in C \longrightarrow (ax,o)\in C \longrightarrow$

$\longrightarrow a \neq_A o \wedge (x,o)\in C \longleftrightarrow a \neq_A o \wedge x \neq_1 o$.

DEFINITION 3.4. A module $(M,=_1,\neq_1,+')$, defined in the Theorem 3.4., is called a quotient module and it is denoted by $M/(R,C)$.

Remark. If H is a submodule which corresponds to the congruence R and if P is a cosubmodule which corresponds to the cocongruence C such that

$$(\forall xy\in M)(x\in H \wedge y\in P \longrightarrow x+y\in P),$$

then we denote the A-module $M/(R,C)$ with $M/(H,P)$. In this case we say that H and P are compatible in M. In the A-module $M/(H,P)$ we have

$$x+H =_1 y+H \longleftrightarrow x-y\in H,$$

$$x+H =_1 y+H \longleftrightarrow x-y\in P,$$

$$(x+H)+'(y+H) =_1 x+y+H,$$

$$a.'(x+H) =_1 ax+H .$$

COROLLARY 3.4.1. Let M be an A-module and let P be a cosubmodule of M. Then we can construct a quotient module $M/(\neg P,P)$.

Proof. Combine Theorem 3.4. and Corollary 3.3.1.

PROPOSITION 3.5. Let $(M,=_M,\neq_M,+)$ be an A-module and P its cosubmodule. Then there exists a submodule $\overline{P}$ of M, compatible with P.

Proof. Let $\overline{P} = \{x\in M: x \neq P\}$. Then

(o) $o\in\overline{P}$.

(i) Let $x\in\overline{P}$ ($\Longleftrightarrow x \neq P$) and let $u\in P$ be taken arbitrary, i.e. $-(u)\in P$. Then $-u\in P$. Thus $-u \neq_M x$, i.e. $u \neq_M -x$. Therefore $-x \neq P$, i.e. $-x\in\overline{P}$.

(ii) Let $x\in\overline{P}$ and $y\in\overline{P}$ be taken arbitrarily i.e. $x \neq P$ and $y \neq P$. Surely $\neg(x+y\in P)$ holds. Let $u\in P$ be taken arbitrarily. Then

$$u\in P \Longleftrightarrow u-x-y+x+y\in P \Longrightarrow u-x-y\in P \vee x+y\in P \Longrightarrow$$

$$\Longrightarrow u-x-y\in P \neq o \Longrightarrow u-x-y \neq_M o \Longleftrightarrow u \neq_M x+y .$$

Thus $x+y \neq P$, i.e. $x+y\in\overline{P}$.

(iii) Let $x\in\overline{P}$ and $a\in A$. Then $a\in A$ and $x \neq P$. Surely $\neg(ax\in P)$ holds. Let $u\in P$ be taken arbitrarily. Then

$$u\in P \Longleftrightarrow u-ax+ax\in P \Longrightarrow u-ax\in P \vee ax\in P \Longrightarrow u-ax\in P$$

$$\Longrightarrow u-ax \neq_M o \Longleftrightarrow u \neq_M ax .$$

Thus $ax \neq P$, i.e. $ax\in\overline{P}$.

(iv) $x\in\overline{P} \wedge y\in P \Longleftrightarrow x \neq P \wedge y\in P \Longleftrightarrow x \neq P \wedge x+y-x\in P \Longrightarrow$

$\Longrightarrow x \neq P \wedge (x+y\in P \vee -x\in P) \Longrightarrow x+y\in P.$

COROLLARY 3.5.1. Let M be an A-module. Then the set

$$\overline{M}_o = \{z\in M:(\forall y\in M)(y \neq_M o)(y \neq_M z)\}$$

is a submodule of M and $(o)\subseteq\overline{M}_o\subseteq\neg M_o$.

DEFINITION 3.5. Let $(A,=_A,\neq_A,+,.)$ be a ring and let P be a coideal of A. P is minimal iff

$$1\in P,$$

$$(\forall a\in A)(a\in P \Longrightarrow (\exists b\in A)(ab-1 \neq P)).$$

COROLLARY 3.5.2. Let $(A,=_A,\neq_A,+,.)$ be a ring and let P

be the minimal coideal of A. Then the quotient ring $A/(\bar{P},P)$ is a Richman field.

Proof. Combine Theorem 3.4. and Proposition 3.5. and

$$a \neq_1 o \iff a \in P \longrightarrow (\exists b \in A)(ab-1 \neq P)$$
$$(\exists b \in A/(\bar{P},P))(a.'b =_1 1).$$

Remark. If P is the minimal coideal of the ring A, then the ideal $\bar{P}$ need not be maximal ideal of A, in classical sense, because $\bar{P} \subseteq \neg P$.

4. Homomorphisms of modules

DEFINITION 4.1. Let $(A,=_\Lambda,\neq_A,+,.)$ be a ring and let $(M,=_M,\neq_M,+)$ and $(H,=_H,\neq_H,+)$ be A-modules. Total function $f:M \longrightarrow H$ is called a homomorphism of modules iff

$$(\forall xy \in M)(f(x+y) =_H f(x)+f(y)),$$
$$(\forall a \in \Lambda)(\forall x \in M)(f(ax) =_H af(x)).$$

A homomorphism $f:M \longrightarrow H$ is a monomorphism iff f is injective, an epimorphism iff it is surjective, and an isomorphism iff it is a bijective embedding.

PROPOSITION 4.1. Let $f:M \longrightarrow H$ be a homomorphism of A-modules. Then

a) The set $Kerf \equiv \{x \in M : f(x) =_H o\}$ is a submodule of M and $(o) \subseteq Kerf$;

b) The set $M_f \equiv \{x \in M : f(x) \neq_H o\}$ is a cosubmodule of M and $M_f \subseteq M_o$;

c) The submodule Kerf and the cosubmodule M_f are compatible in M;

d) The set Imf is a submodule of H.

Proof.

b) $(x \in M_f \iff f(x) \neq_H o \longrightarrow x \neq_M o) \longrightarrow o \neq M_f$;

$x+y \in M_f \iff f(x+y) \neq_H o \iff f(x)+f(y) \neq_H o \longrightarrow$

$\longrightarrow f(x) \neq_H o \vee f(y) \neq_H o \iff x \in M_f \vee y \in M_f$;

$ax \in M_f \iff f(ax) \neq_H o \iff af(x) \neq_H o \longrightarrow$

$\longrightarrow a \neq_A o \wedge f(x) \neq_H o \iff x \neq_A o \wedge x \in M_f$;

$$x \in M_f \iff f(x) \neq_H o \longrightarrow x \neq_M o \iff x \in M_o .$$

c) $x \in \mathrm{Kerf} \wedge y \in M_f \iff f(x) =_H o \wedge f(y) \neq_H o \longrightarrow$

$\longrightarrow f(x)+f(y) \neq_H o \iff f(x+y) \neq_H o \iff x+y \in M_f$.

PROPOSITION 4.2. Let $f:M \longrightarrow H$ be a homomorphism of A-modules. Then Kerf is detachable in M iff Imf is discrete.

Proof.

$(x \in \mathrm{Kerf} \vee \neg(x \in \mathrm{Kerf})) \iff (f(x) =_H o \vee \neg(f(x) =_H o))$.

COROLLARY 4.2.1. Let M be an A-module and H its submodule. Then the A-module M/H is discrete iff H is detachable in M.

Proof. The canonical epimorphism $p:M \longrightarrow M/H$, defined by $p:M \ni x \longmapsto x+H \in M/H$, has a kernel H.

COROLLARY 4.2.2. An A-module is discrete iff the submodule (o) is detachable in M.

LEMMA 4.3. Let $f:M \longrightarrow H$ be a homomorphism of A-modules.

a) A homomorphism f is injective iff Kerf = (o).

b) A homomorphism f is an embedding iff $M_f = M_o$.

Proof.

$$x \in M_o \iff x \neq_M o \iff f(x) \neq_H o \iff x \in M_f .$$

THEOREM 4.4. Let $f:M \longrightarrow H$ be an A-homomorphism of A-modules. There exists the unique isomorphism $h:M/(\mathrm{Kerf},M_f)$ Imf with $f = h.p$.

Proof. We define the mapping h

$(\forall x+\mathrm{Kerf} \in M/(\mathrm{Kerf},M_f))(h(x+\mathrm{Kerf}) =_H f(x))$.

Then

$x+\mathrm{Kerf} =_1 y+\mathrm{Kerf} \iff x-y \in \mathrm{Kerf} \iff f(x-y) =_H o \iff$

$\iff f(x)-f(y) =_H o \iff f(x) =_H f(y) \iff h(x+\mathrm{Kerf}) =_H h(y+\mathrm{Kerf})$;

$h(x+\mathrm{Kerf}) \neq_H h(y+\mathrm{Kerf}) \iff f(x) \neq_H f(y) \iff$

$\iff f(x)-f(y) \neq_H o \iff f(x-y) \neq_H o \iff x-y \in M_f \iff$

$\iff x+\mathrm{Keff} \neq_1 y+\mathrm{Kerf}$.

LEMMA 4.5. Let M be an A-module and let (H_1,P_1) and

(H_2,P_2) be two pairs of compatible submodules and cosubmodules of the module M. If $H_2 \subseteq H_1$, then $P_2 \cap H_1$ is a cosubmodule of the module H_1 and H_2 and $P_2 \cap H_1$ are compatible in H_1.

Proof.

$o \not= P_2 \longrightarrow o \not= P_2 \cap H_1$;

$x+y \in P_2 \cap H_1$ $(x,y \in H_1) \longrightarrow x+y \in P_2$ $(x,y \in H_1) \longrightarrow$

$\longrightarrow x \in P_2 \vee y \in P_2$ $(x,y \in H_1) \longrightarrow x \in P_2 \cap H_1 \vee y \in P_2 \cap H_1$;

$ax \in P_2 \cap H_1$ $(x \in H_1) \longrightarrow ax \in P_2$ $(x \in H_1) \longrightarrow$

$\longrightarrow a \not=_A o \wedge x \in P_2$ $(x \in H_1) \longrightarrow a \not=_A o \wedge x \in P_2 \cap H_1$.

$x \in H_2 \wedge y \in P_2 \cap H_1 \longrightarrow x \in H_2 \subseteq H_1 \wedge y \in P_2 \wedge y \in H_1 \longrightarrow$

$\longrightarrow x+y \in P_2 \wedge x+y \in H_1 \longrightarrow x+y \in P_2 \cap H_1$.

LEMMA 4.6. Let M be an A-module and let (H_1,P_1) and (H_2,P_2) be two pairs of compatible submodules and cosubmodules of the module M. Then $H_1 \subseteq H_2$ and $P_1 \subseteq P_2$ are the compatible submodule and cosubmodule of the module M.

Proof.

$o \not= P_1 \wedge o \not= P_2 \longrightarrow o \not= P_1 \cup P_2$;

$x+y \in P_1 \cup P_2 \longleftrightarrow x+y \in P_1 \vee x+y \in P_2 \longrightarrow$

$x \in P_1 \vee y \in P_1 \vee x \in P_2 \vee y \in P_2 \longrightarrow x \in P_1 \cup P_2 \vee y \in P_1 \cup P_2$;

$ax \in P_1 \cup P_2 \longleftrightarrow ax \in P_1 \vee ax \in P_2 \longrightarrow$

$(a \not=_A o \wedge x \in P_1) \vee (a \not=_A o \wedge x \in P_2) \longrightarrow a \not=_A o \wedge (x \in P_1 \vee x \in P_2)$

$\longrightarrow a \not=_A o \wedge x \in P_1 \cup P_2$.

THEOREM 4.7. Let M be an A-module and let (H_1,P_1) and (H_2,P_2) be two pairs of compatible submodules and cosubmodules of the module M such that $H_2 \subseteq H_1$ and $P_1 \subseteq P_2$. Then there exists the isomorphism

$$M/(H_1,P_1) \cong (M/(H_2,P_2))/(H_1/(H_2,P_2 \cap H_1),P_1/(H_2,P_2 \cap H_1)).$$

Proof.

1. We define $H_1/(H_2,P_2 \cap H_1) = \{x+H_2 \in M/(H_2,P_2) : x \in H_1\}$ and $P_1/(H_2,P_2 \cap H_1) = \{x+H_2 \in M/(H_2,P_2) : x \in P_1\}$ and we prove

that they are a submodule and cosubmodule of the module $M/(H_2,P_2)$ which are compatible.

$$x+H_2\in P_1/(H_2,P_2\cap H_1) \longleftrightarrow x\in P_1\subseteq P_2 \longrightarrow x+H_2 \neq_1' H_2;$$

$$(x+H_2)+'(y+H_2)\in P_1/(H_2,P_2\cap H_1) \longleftrightarrow$$

$$\longleftrightarrow x+y+H_2\in P_1/(H_2,P_2\cap H_1) \longleftrightarrow x+y\in P_1 \longrightarrow x\in P_1 \vee y\in P_1$$

$$\longleftrightarrow x+H_2\in P_1/(H_2,P_2\cap H_1) \vee y+H_2\in P_1/(H_2,P_2\cap H_1);$$

$$a\cdot'(x+H_2)\in P_1/(H_2,P_2\cap H_1) \longleftrightarrow ax+H_2\in P_1/(H_2,P_2\cap H_1)$$

$$\longleftrightarrow ax\in P_1 \longrightarrow a\neq_A 0 \wedge x\in P_1 \longleftrightarrow a\neq_A 0 \wedge x+H_2\in P_1/(H_2,P_2\cap H_1);$$

$$x+H_2\in H_1/(H_2,P_2\cap H_1) \wedge y+H_2\in P_1/(H_2,P_2\cap H_1) \longleftrightarrow$$

$$\longleftrightarrow x\in H_1 \wedge y\in P_1 \longrightarrow x+y\in P_1 \longleftrightarrow x+y+H_2\in P_1/(H_2,P_2\cap H_1).$$

2. Define a mapping from $M/(H_2,P_2)$ into $M/(H_1,P_1)$ with

$$(\forall x+H_2\in M/(H_2,P_2))(f(x+H_2) =_1 x+H_1).$$

Then f is a well-defined surjective homomorphism. Thus, by Theorem 4.4.,

$$(M/(H_2,P_2))/(\mathrm{Ker}f,(M/(H_2,P_2))_f) \cong M/(H_1,P_1).$$

However

$$f(x+H_2) =_1 x+H_1 =_1 H_1 \longleftrightarrow x\in H_1$$

and

$$f(x+H_2) =_1 x+H_1 \neq_1 H_1 \longleftrightarrow x\in P_1 .$$

Thus

$$\mathrm{Ker}f = H_1/(H_2,P_2\cap H_1) \text{ and } (M/(H_2,P_2))_f = P_1/(H_2,P_2\cap H_1).$$

THEOREM 4.8. Let M be an A-module and let (H_1,P_1) and (H_2,P_2) be two pairs of compatible submodules and cosubmodules of the module M. Then there exists the isomorphism

$$H_1/(H_1\cap H_2,H_1\cap(P_1\cup P_2)) \cong (H_1+H_2)/(H_2,P_2\cap(H_1+H_2)).$$

Proof.

Define a mapping f from H_1 into $(H_1+H_2)/(H_2,P_2\cap(H_1+H_2))$ with

$$(\forall x\in H_1)(f(x) =_1' x+H_2\in (H_1+H_2)/(H_2,P_2\cap(H_1+H_2))).$$

It is clear that f is a homomorphism. To show that f is surjective we note that if $(x+y)+H_2$ is a typical element of $(H_1+H_2)/(H_2,P_2\cap(H_1+H_2))$, with $x\in H_1$ and $y\in H_2$, then

$$(x+y)+H_2 =_1' x+H_2 =_1' f(x) .$$

Thus, by Theorem 4.4.,

$$H_1/(\mathrm{Ker}f,(H_1)_f) \cong (H_1+H_2)/(H_2,P_2\cap(H_1+H_2)).$$

However

$$f(x) =_1' x+H_2 =_1' H_2 \longleftrightarrow x\in H_2 \longrightarrow x\in H_2\cap H_1$$

and

$$f(x) =_1' x+H_2 \neq_1' H_2 \longleftrightarrow x\in P_2 \longrightarrow x\in P_2\cap H_1 .$$

Hence

$$\mathrm{Ker}f = H_1\cap H_2$$

and

$$(H_1)_f = P_2\cap H_1 = (P_2\cup P_1)\cap H_1 .$$

5. Sums of modules

Let M be an A-module and let S and T be its submodules. The sum of them, denoted by S+T, is defined by

$$S+T = \{s+t : s\in S \wedge t\in T\}.$$

It is easily seen that S+T is a submodule of M. If $(S_i)_{i=1}^n$ are submodules of M, then

$$S_1+\ldots+S_n = \{s_1+\ldots+s_n : (\forall i\in\bar{n})(s_i\in S_i)\}$$

is a submodule of M. We denoted this submodule with $\sum_{i=1}^{n} S_i$; it is called the sum of $S_1,\ldots,S_n$. The notion of the sum of submodules of M can be extended to an arbitrarily inhabited family $(S_i)_{i\in I}$ of submodules of M. For each subfinite subset $J\subseteq I$, $\sum_{i\in J} S_i$ is a submodule of M. In general, the union of submodules of M is not a submodule of M. However, $\bigcup_{J\subseteq I}\sum_{i\in J} S_j$, where J is a subfinite subset of the set I, is a submodule of M. It is this submodule that we call the sum of the family $(S_i)_{i\in I}$ and denote with $\sum_{i\in I} S_i$.

5.1. Finitely generated modules. Let M be an A-module and let $x\in M$. Then $Ax = \{ax : a\in A\}$ is a submodule of M. Since M is unital, Ax containes x. If S is an inhabited subset of M, the $\sum_{x\in S} Ax$ is called a submodule generated by S. If S is a strictly finite subset $\{x_1,\ldots,x_n\}$ such that $(\forall ij\in n)(x_i \neq_M x_j)$ and

$M = \sum_{i=1}^{m} Ax_i$, then we say that M is strictly finitely generated.

PROPOSITION 5.1. If an A-module M is strictly finitely generated, then there are $n \in N$ and compatible submodule H and cosubmodule P of the A-module A^n such that $M \cong A^n/(H,P)$.

Proof. Let $M = Ax_1 + \ldots Ax_n$. Define a mapping $f: A^n \longrightarrow M$ with

$$f: A^n \ni (a_1,\ldots,a_n) \longmapsto \sum_{i=1}^{m} a_i x_i \in M .$$

For arbitrary $\sum a_i x_i \in M$ we can get $(a_1,\ldots,a_n) \in A^n$ such that $f(a_1,\ldots,a_n) =_M \sum a_i x_i$. So, if we take

$$\mathrm{Ker} f = \{(a_1,\ldots,a_n) \in A^n : \sum_{i=1}^{m} a_i x_i =_M o\},$$

and

$$(A^n)_f = \{(a_1,\ldots,a_n) \in A^n : \sum_{i=1}^{m} a_i x_i \neq_M o\},$$

then

$$M \cong A^n/\mathrm{Ker} f, (A^n)_f .$$

PROPOSITION 5.2. Let

$$(\exists n \in N)(\exists H,P \subseteq A^n)(h: M \cong A^n/(H,P))$$

for an A-module M, where H and P are a compatible submodule and cosubmodule of A^n. Then the A-module M is subfinitely generated.

Proof. Let

$$f: A^n \xrightarrow{\ p\ } A^n/(H,P) \xrightarrow{\ h\ } M .$$

Then f is the epimorphism of A-modules. Let

$$L = \{i \in \bar{n} : (d_{i1},\ldots,d_{in}) \in H\}$$

where d_{ij} $(ij \in \bar{n})$ is Cronecer simbol and let $x \in M$ be taken arbitrarily Then we can find $(a_1,\ldots,a_n)+H \in A^n/(H,P)$ such that $h((a_1,\ldots,a_n)+H) =_M x$. If $(d_{i1},\ldots,d_{in}) = e_i$ $(i \in \bar{n})$, then

$$h(a_1e_1+\ldots+a_ne_n+H) =_M x .$$

So, the set $(f(e_i))_{i \in \bar{n} \setminus L}$ generated the A-module M.

COROLLARY 5.2.1. Let M be a discrete module over a discrete ring A and let H be a detachable submodule of A^n such that $M \cong A^n/H$, then the A-module M is (strictly) finitely generated.

DEFINITION 5.1. A sequence of A-modules and homomorphisms

$$\ldots \longrightarrow M_{n-1} \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \longrightarrow \ldots$$

is an exact sequence iff

$$(\forall n)(\mathrm{Im} f_{n-1} = \mathrm{Ker} f_n) .$$

LEMMA 5.3. Let M', M and M'' be A-modules.

(a) A sequence

$$(o) \longrightarrow M' \xrightarrow{f} M$$

is exact iff f is injective.

(b) A sequence

$$M \xrightarrow{g} M'' \longrightarrow (o)$$

is exact iff g is surjective.

(c) A sequence

$$(*) \qquad (o) \longrightarrow M' \xrightarrow{f} M \xrightarrow{g} M'' \longrightarrow (o)$$

is exact iff f is injective, $\mathrm{Im} f = \mathrm{Ker} f$ and g surjective.

PROPOSITION 5.4. Let the sequence $(*)$ be exact. If M' and M'' strictly finitely generated the A-modules, then A-module M is finitely generated.

Proof. Let $S' \equiv \{x'_1,\ldots,x'_n\}$ be a generator of an A-module M' and let $S'' \equiv \{x''_1,\ldots,x''_m\}$ be a generator of an A-module M''. Following $\mathrm{Im} g = M''$, we have

$$(\forall i \in \overline{m})(\exists x_i \in M)(x''_i =_{M''} g(x_i))$$

with

$$(\forall ij \in \overline{m})(x''_i \neq_{M''} x''_j \longrightarrow g(x_i) \neq_{M''} g(x_j) \longrightarrow x_i \neq_M x_j)$$

and

$$u \in \mathrm{Ker} g \longrightarrow g(u) =_{M''} o \neq_{M''} x''_i \Longrightarrow g(u) \neq_{M''} g(x_i) \longrightarrow$$
$$\Longrightarrow u \neq_M x_i \quad (i \in \overline{m}).$$

So

$$(\forall i \in \overline{m})(x_i \neq \mathrm{Ker} g = \mathrm{Im} f),$$

i.e.

$$(\forall i \in \overline{m})(\forall j \in \overline{n})(x_i \neq_M f(x'_j)).$$

Further, we have

$$(\forall ij \in \overline{n})(x'_i =_{M'} x'_j \longrightarrow f(x'_i) =_M f(x'_j))$$

and

$$(\forall ij \in \overline{n})(x'_i \neq_{M'} x'_j \longrightarrow \neg(f(x'_i) =_M f(x'_j)))$$

because the homomorphism f is injective. So, the set

$$S = \{f(x'_1),\dots,f(x'_n),x_1,\dots,x_m\}$$

generated the A-module M.

COROLLARY 5.4.1. If the homomorphism f in the Proposition 5.4 is an embedding, then the A-module M is strictly finitely generated by the set $S = \{f(x'_1),\dots,f(x'_n),x_1,\dots,x_m\}$.

COROLLARY 5.4.2.([6]), Lemma 2.) Let M be an A-module and let H and P be its compatible submodule and cosubmodule. If the A-module H and M/(H,P) are strictly finitely generated, then so is the A-module M.

Proof. We have the exact sequence

$$(o) \longrightarrow H \xrightarrow{u} M \xrightarrow{p} M/(H,P) \longrightarrow (o)$$

where the homomorphism u is the inclusion (injective and embedding).

5.2. Strictly finite direct sum of submodules.

DEFINITION 5.2. The A-module M is the (internal) direct sum of submodules S and T, denoted by $M = S \oplus T$, iff

$$(\forall x\in M)(\exists s\in S)(\exists t\in T)(x =_M s+t),$$

$$(\forall s\in S)(\forall t\in T)(s+t =_M o \longrightarrow s =_M o \wedge t =_M o),$$

$$(\forall s\in S)(\forall t\in T)(s \neq_M o \vee t \neq_M o \longrightarrow s+t \neq_M o).$$

DEFINITION 5.3. Let S and T be A-submodules of an A-module M. We denote

$$C_S = \{s+t : t \neq_M o\}, \qquad C_T = \{s+t : s \neq_M o\}.$$

PROPOSITION 5.5. Let $M = S \oplus T$. Then

a) The set C_S is a cosubmodule of M compatible with S;

b) The set C_T is a cosubmodule of M compatible with T;

c) $C_S = \{x\in M : x \nmid S\}$, $\quad C_T = \{x\in M : x \nmid T\}$;

d) $S \cong M/(T,C_T)$, $\quad T \cong M/(S,C_S)$.

Proof.

a) $(t \neq_M o \longrightarrow s+t \neq_M o) \longrightarrow o \nmid C_S$;

$ax \in C_S \longleftrightarrow a(s+t) \in C_S \longleftrightarrow as+at \in C_S \longleftrightarrow at \not=_M o \longrightarrow$

$\longrightarrow a \not=_A o \wedge t \not=_M o \longleftrightarrow x \not=_M s+t \in C_S \wedge a \not=_A o$;

$x+y \in C_S \longleftrightarrow s_x+t_x+s_y+t_y \in C_S \longleftrightarrow t_x+t_y \not=_M o \longrightarrow$

$\longrightarrow t_x \not=_M o \vee t_y \not=_M o \longleftrightarrow x \not=_M s_x+t_x \in C_S \vee y \not=_M s_y+t_y \in C_S$;

$x \in S \wedge y \in C_S \longleftrightarrow x \in S \wedge y \not=_M s_y+t_y \ (t_y \not=_M o) \longrightarrow$

$\longrightarrow x+y \not=_M (x+s_y)+t_y \ (t_y \not=_M o) \longrightarrow x+y \in C_S$.

c) $x \not=_M s_x+t_x \in C_S \longleftrightarrow t_x \not=_M o \longrightarrow (s_x-u)+t_x \not=_M o \ (u \in S) \longrightarrow$

$\longrightarrow s_x+t_x \not=_M u \ (u \in S) \longrightarrow x \not=+ S$;

$x \not=+ S \longleftrightarrow x \not=_M s_x+t_x \not=_M u \ (u \in S) \longrightarrow s_x+t_x \not=_M s_x \longleftrightarrow$

$\longleftrightarrow t_x \not=_M o \longleftrightarrow x \not=_M s_x+t_x \in C_S$.

d) If we define $f: M = S \oplus T \ni s+t \longmapsto s \in S$, then we have

$\mathrm{Ker} f = T, \quad M_f = C_T, \quad S \cong M/(T, C_T)$.

THEOREM 5.6. Let M be an A-module and let S and T be its submodules. Then $M = S \oplus T$, iff

$M = S + T, \quad S \cap T = (o) \quad C_S \cup C_T = M_o$.

Proof.

(a) Let $M = S \oplus T$. Then

i) Obviously, $M = S + T$.

ii) $x \in S \cap T \longleftrightarrow x \not=_M s+t \begin{cases} \in S \\ \in T \end{cases} \longleftrightarrow \begin{cases} (-x+s)+t \not=_M o \\ s+(-x+t) \not=_M o \end{cases} \longrightarrow$

$\longrightarrow s \not=_M x \wedge t \not=_M o \wedge s \not=_M o \wedge t \not=_M x \longrightarrow x \not=_M o$.

iii) $M_o \ni x \not=_M s+t \not=_M o \longrightarrow s \not=_M o \vee t \not=_M o \longleftrightarrow$

$\longleftrightarrow x \in C_S \vee x \in C_T \longleftrightarrow x \in C_S \cup C_T$.

(b)

iv) $(\forall x \in M)(\exists s \in S)(\exists t \in T)(x \not=_M s+t)$.

v) $(\forall s \in S)(\forall t \in T)(s+t \not=_M o \longrightarrow s \not=_M -t \in S \cap T = (o) \longrightarrow$

$\longrightarrow s \not=_M o \wedge t \not=_M o)$.

vi) $(\forall s \in S)(\forall t \in T)(s \not=_M o \vee t \not=_M o \longrightarrow s+t \in C_T \vee s+t \in C_S \longrightarrow$

$\longrightarrow s+t \in C_T \cup C_S = M_o \longrightarrow s+t \not=_M o)$.

5.3. Infinite direct sum of modules. Let $\langle\langle (M_t, =_t, \neq_t, +_t)\rangle\rangle_{t\in T}$ be a family of A-modules indexed by an infinite set $(T, =_T, \neq_T)$.

DEFINITION 5.4. ([9],[10])

a) For a family J of subsets of the set T we say that it is an a-ideal of T, iff

$$\emptyset \in J,$$

$$Y_1 \subseteq Y_2 \wedge Y_2 \in J \longrightarrow Y_1 \in J,$$

$$Y_1 \in J \wedge Y_2 \in J \longrightarrow Y_1 \cup Y_2 \in J.$$

The ideal J is strong, iff $T \neq J$.

b) We say that a family K of subsets of the set T is a b-coideal of T, iff

$$T \in K,$$

$$Z_1 \subseteq Z_2 \wedge Z_1 \in K \longrightarrow Z_2 \in K,$$

$$Z_1 \in K \wedge Z_2 \in K \longrightarrow Z_1 \cap Z_2 \in K.$$

The coideal K is strong, iff $\emptyset \neq K$.

Example VII: a) The family $J_o = \{Y \subseteq T : Y \text{ is subfinite}\}$ is a strong ideal of T.

b) The family

$$K_o = \{Z \subseteq T : (\exists Y \subseteq T)(T = Y \cup Z)(Y \text{ is subfinite})\}$$

is a strong coideal of T.

The Cartesian product of the family $\langle\langle (M_t, =_t, \neq_t, +_t)\rangle\rangle_{t\in T}$ is denoted by

$$F = \prod_{t\in T} M_t = \{f : T \longrightarrow \bigcup_{t\in T} M_t : (\forall t \in T)(f(t) \in M_t)\}.$$

In the class F we define compatible equality and diversity relations with

$$f =_F g \longleftrightarrow (\forall t \in T)(f(t) =_t g(t)),$$

$$f \neq_F g \longleftrightarrow (\exists s \in T)(f(s) \neq_s g(s)).$$

Therefore, $(\prod_{t\in T} M_t, =_F, \neq_F)$ is a set. We define algebraic operations on $\prod_{t\in T} M_t$ with

$$(f+g)(t) =_t f(t) +_t g(t) \quad (t \in T),$$

$$O(t) =_t o \quad (t \in T),$$

$$(-f)(t) =_t -f(t) \quad (t \in T),$$

$$(af)(t) =_t af(t) \quad (t \in T).$$

Then $(\prod_{t\in T} M_t, =_F, \neq_F, +)$ is an A-module.

PROPOSITION 5.7. Let $\langle (M_t, =_t, \neq_t, +_t) \rangle_{t\in T}$ be a family of A-modules. Then

i) If J is an ideal of the set T, then the set

$$S_2 = \{ f \in \prod_{t\in T} M_t : \{ t \in T : f(t) \neq_t o \} \in J \}$$

is a submodule of the A-module $\prod_{t\in T} M_t$.

ii) Let K be a coideal of the set T. Then the set

$$S_1 = \{ f \in \prod_{t\in T} M_t : \{ t \in T : f(t) =_t o \} \in K \}$$

is a submodule of the A-module $\prod_{t\in T} M_t$.

Proof.

i) Let $Z(f,g) = \{ t \in T : f(t) \neq_t g(t) \}$. Then

$$Z(0,0) =_2 \emptyset \in J \longrightarrow 0 \in S_2;$$

$$f \in S_2 \longleftrightarrow Z(f,0) \in J \longrightarrow | Z(f,0) =_2 Z(-f,0) | \longrightarrow$$

$$\longrightarrow Z(-f,0) \in J \longleftrightarrow -f \in S_2;$$

$$f \in S_2 \wedge g \in S_2 \longleftrightarrow Z(f,0) \in J \wedge Z(g,0) \in J \longrightarrow$$

$$\longrightarrow Z(f,0) \cup Z(g,0) \in J \longrightarrow | Z(f+g,0) \subseteq Z(f,0) \cup Z(g,0) | \longrightarrow$$

$$\longrightarrow Z(f+g,0) \in J \longleftrightarrow f+g \in S_2;$$

$$a \in A \wedge f \in S_2 \longleftrightarrow a \in A \wedge Z(f,0) \in J \longrightarrow | Z(af,0) \subseteq Z(f,0) |$$

$$\Longrightarrow Z(af,0) \in J \longleftrightarrow af \in S_2.$$

ii) Let $Y(f,g) = \{ t \in T : f(t) =_t g(t) \}$. Then

$$Y(0,0) =_2 T \in K \longrightarrow 0 \in S_1;$$

$$g \in S_1 \Longrightarrow -g \in S_1;$$

$$f \in S_1 \wedge g \in S_1 \longleftrightarrow Y(f,0) \in K \wedge Y(g,0) \in K \longrightarrow$$

$$\longrightarrow Y(f,0) \cap Y(g,0) \in K \longrightarrow | Y(f,0) \cap Y(g,0) \subseteq Y(f+g,0) | \longrightarrow$$

$$\Longrightarrow Y(f+g,0) \in K \longleftrightarrow f+g \in S_1;$$

$$a \in A \wedge g \in S_1 \longleftrightarrow a \in A \wedge Y(g,0) \in K \longrightarrow | Y(g,o) \subseteq Y(ag,0) |$$

$$\longrightarrow Y(ag,0) \in K \longleftrightarrow ag \in S_1.$$

Let T be an infinite set and let $\langle\langle (M_t,=_t,\neq_t,+_t)\rangle\rangle_{t\in T}$ be a family of A-modules. Then the set

$$S = \{f \in \bigsqcap_{t\in T} M_t : Z(f,0)\in J_o \wedge Y(f,0)\in K_o\} = S_1 \cap S_2$$

is a submodule of the A-module $\bigsqcap_{t\in T} M_t$. The submodule S is called the (external) direct sum of the family $\langle\langle (M_t,=_t,\neq_t,+_t)\rangle\rangle_{t\in T}$ and we write

$$S = \bigoplus_{t\in T} M_t .$$

It is easily seen that M_t is a submodule of S for each $t\in T$.

PROPOSITION 5.8. Let $\langle\langle (M_t,=_t,\neq_t,+_t)\rangle\rangle_{t\in T}$ and $\langle\langle (H_t,=_t,\neq_t,+_t)\rangle\rangle_{t\in T}$ be families of A-modules and let $M = \bigoplus_{t\in T} M_t$ and $H = \bigoplus_{t\in T} H_t$. For each $t\in T$, let $f_t : M_t \longrightarrow H_t$ be a homomorphism. Define $f : M \longrightarrow H$ with

$$(\forall t\in T)((f(x))(t) =_t f_t(x(t))).$$

Then

$$\mathrm{Ker}f \cong \bigoplus_{t\in T} \mathrm{Ker}f_t \qquad \mathrm{Im}f \cong \bigoplus_{t\in T} \mathrm{Im}f_t$$

$$(M)_f = \bigcup_{j\in T} \{x \in \bigoplus M_t : j\in Z(x,0) \wedge x(j)\in (M_t)_{f_t}\}$$

and

$$(\bigoplus_{t\in T} M_t)/(\bigoplus_{t\in T} \mathrm{Ker}f_t,\ M_f) = \bigoplus_{t\in T} (M_t/(\mathrm{Ker}f_t,(M_t)_{f_t}))$$

Proof.

1. i) $x \in \bigoplus_{t\in T} \mathrm{Ker}f_t \longleftrightarrow Z(x,0)\in J_o \wedge Y(x,0)\in K_o \wedge$

$\wedge (\forall i\in Z(x,0))(x(i)\in \mathrm{Ker}f_i) \longrightarrow (\forall i\in Z(x,0))(f_i(x(i)) =_i o)$

$\longrightarrow (\forall i\in Z(x,0))(f(x)(i) =_i o) \longrightarrow f(x) =_H o \longleftrightarrow x\in \mathrm{Ker}f.$

ii) Let $x\in \mathrm{Ker}f \subseteq \bigoplus_{t\in T} M_t$. Then $Z(x,0)\in J_o \wedge Y(x,0)\in K_o$ and $f(x) =_H o$. Then

$$(\forall i\in Z(x,0))(f(x)(i) =_i o) \longleftrightarrow (\forall i\in Z(x,0))(f_i(x(i)) =_i o)$$

$$\longleftrightarrow (\forall i\in Z(x,0))(x(i)\in \mathrm{Ker}f_i).$$

So, $x\in \bigoplus_{t\in T} \mathrm{Ker}f_t$.

2. Let $y\in \bigoplus_{t\in T} \mathrm{Im}f_t$. Then $Z(y,0)\in J_o \wedge Y(y,0)\in K_o$ and

$$(\forall j\in Z(y,0))(y(j)\in \mathrm{Im}f_j).$$

Then

$$(\forall j \in Z(y,0))(\exists x_j \in M_j)(y(j) =_j f_j(x_j)).$$

Let us define $x \in \bigoplus M_t$ with

$$Z(x,0) =_2 Z(y,o) \wedge Y(y,0) =_2 Y(x,0) \wedge (\forall j \in Z(x,0))(x(j) =_j x_j)$$

Then $x \in \bigoplus M_t$ and $(\forall j \in Z(x,0))(y(j) =_j f(x(j)))$. Thus $y =_H f(x)$, i.e. $y \in \mathrm{Im}f$.

Let $y \in \mathrm{Im}f \subseteq \bigoplus H_t$. Then $Z(y,0) \in J_o \wedge Y(y,0) \in K_o$ and $(\exists x \in \bigoplus M_t)(y =_H f(x))$. Further,

$$(\forall j \in Z(y,0))(y(j) =_j f(x)(j) =_j f_j(x(j)))$$

and $(\forall j \in Z(y,0))(y_j =_j f_j(x(j)))$, where $x(j) \in M_j$. Therefore $y \in \bigoplus \mathrm{Im}f_t$.

$$x \in M_f \longleftrightarrow f(x) =_H 0 \longrightarrow (\exists s \in T)(f(x)(s) \neq_s o) \longleftrightarrow$$

$$\longrightarrow (\exists s \in T)(f_s(x(s)) \neq_s o) \longrightarrow (\exists s \in T)(x(s) \in (M_s)_{f_s}) \longrightarrow$$

$$\longrightarrow x \in \bigcup \{x \in \bigoplus M_t : j \in Z(x,0) \wedge x(j) \in (M_j)_{f_j}\}$$

It is clear that

$$(\bigoplus_{t\in T} M_t)/(\bigoplus_{t\in T} \mathrm{Ker}f_t, M_f) \cong \bigoplus_{t\in T}(M_t/(\mathrm{Ker}f_t, (M_t)_{f_t})).$$

COROLLARY 5.8.1. Let $\langle (M_t, =_t, \neq_t, +_t)\rangle_{t\in T}$ be a family of A-modules and let (L_t, P_t) be a pair of compatible submodules and cosubmodules of M_t $(t \in T)$. Then

$$(\bigoplus_{t\in T} M_t)/(\bigoplus_{t\in T} L_t, C) = \bigoplus_{t\in T}(M_t/(L_t, P_t))$$

where

$$C = \bigcup_{j\in T}\{x \in \bigoplus_{t\in T} M_t : j \in Z(x,0) \wedge x(j) \in P_j\}.$$

REFERENCES

[1] E.Bishop, Foundations of Constructive Analysis; McGraw-Hill, New York 1967.

[2] R.J.Grayson, Intuitionistic Set Theory; Ph.D.Tesis. Oxford University, 1978.

[3] N.Greenleaf, Liberal Constructive Set Theory; Lecture No-

tes in Mathematics, Springer-Verlag, Berlin, 873(1981),213-240.

[4] W.Julian, R.Mines and F.Richman, Algebraic Numbers, a Constructive Development; Pacific Journal of Mathematics,(74)1(1978),91-102.

[5] D.G.McCarty, Realizability and Recurzive Mathematics; Ph. D.Tesis. Carnegie-Mellon University, 1984.

[6] F.Richman, Constructive Aspect of Noetherian Rings; Proceedings of the American Mathematical Society, (44)2(1974),436-441.

[7] D.A.Romano, Rings and Fields, a Constructive View; Zeitschrift für Mathematische Logik und Grundlegen der Mathematik, (34)1(1988),25-40.

[8] ----------, Constructive Aspect of Abelian Groups; Proceedings of 5th Conference "Algebra and Logic", Cetinje 1986. Institute of Mathematics, University of Novi Sad, 1987., 167-174.

[9] ----------, Construction of Compatible Relations on the Cartesian Product of Sets; Radovi Matematički, (3)1(1987),85-92.

[10] ----------, Equality and Coequality Relations on the Cartesian Product of Sets; Zeitschrift für Mathematische Logik und Grundlegen der Mathematik, (34)5(1988),471-480.

[11] W.B.G.Ruitenburg, Intuitionistic Algebra; Ph.D.Tesis. Utrecht University, 1982.

[12] A.S.Troelstra and D.van Dalen, Constructivism in Mathematics, An Introduction;(Preliminary draft of Chapter VIII: Algebra).

[13] A.S.Troelstra, Finite and Infinite in Intuitionistic Mathematics; Compositio Mathematica, 18(1967),94-116.

Daniel A. Romano
77000 BIHAĆ
Viša tehnička škola u Bihaću
Omladinska 2
Yugoslavia

Bihać, September 21, 1987.

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

ON A CLASS OF CYCLIC VECTOR VALUED GROUPOIDS

Zoran Stojaković

Abstract. Cyclic vector valued groupoids represent a generalization of cyclic n-ary quasigroups and semisymmetric quasigroups. In this paper a class of cyclic vector valued groupoids which are closely related to Mendelsohn quadruple systems (MQS) is considered. Some properties of such vector valued groupoids are determined, their relation to MQS described and a construction of some vector valued groupoids from this class is given.

1. Itroduction and preliminaries

Vector valued groupoids represent a convenient generalization of n-ary groupoids. Various classes of vector valued groupoids which generalize n-ary quasigroups, semigroups and other structures were considered in [2], [3], [4], [6]. Some of them have combinatorial applications and one such class of vector valued groupoids will be considered here.

We shall use the following notation. The sequence $x_p,x_{p+1},\ldots,x_q$ we denote by x_p^q. If $p>q$, then x_p^q will be considered empty.

Let S be a nonempty set, m, n positive integers and F a mapping of S^n into S^m. Then (S,F) is said to be an (n,m)-groupoid (or vector valued groupoid when it is not necessary to emphasize n and m). $|S|$ is called the order of (S,F). The n-ary operations $f_1,\ldots,f_m$ defined by

$$f_i(x_1^n) = y_i \Leftrightarrow (\exists y_1^{i-1}, y_{i+1}^m)\ F(x_1^n) = (y_1^m),\ i=1,\ldots,m,$$

are called the component operations (or components) of F.

Although every (n,m)-groupoid (S,F) can be interpreted as an algebra $(S,f_1,\ldots,f_m)$ with m n-ary operations, it is often more convenient

---

This paper is in final form and no version of it will be submitted

to consider (n,m)-groupoids in the compact form as an algebra with one (n,m)-operation.

Definition 1. An (n,m)-groupoid (S,F) is called cyclic iff for every $x_1^{n+m} \in S$

$$F(x_1^n) = (x_{n+1}^{n+m}) \Rightarrow F(x_2^{n+1}) = (x_{n+2}^{n+m}, x_1) .$$

Cyclic (n,m)-groupoids represent a generalization of cyclic n-ary quasigroups and semisymmetric binary quasigroups. If m=1, then a cyclic n-ary quasigroup is obtained (every cyclic n-ary groupoid is necessarily an n-ary quasigroup) and if n=2, m=1, then we get a well known semisymmetric quasigroup (a quasigroup satisfying the identity $y(xy) = x$ is called semisymmetric). Cyclic n-ary quasigroups were considered in [7] and their combinatorial applications in [8], [10].

Definition 1 implies the following:

An (n,m)-groupoid (S,F) is cyclic iff for all $x_1^{n+m} \in S$ and every $i \in \{1,...,n+m\}$

$$F(x_1^n) = (x_{n+1}^{n+m}) \Leftrightarrow F(x_1^{n+i-1}) = (x_{n+i}^{n+m}, x_1^{i-1}) .$$

Some questions concerning general theory of cyclic (n,m)-groupoids were considered in [9].

A groupoid $(S, \cdot)$ is called idempotent iff for all $x \in S$, $x^2 = x$, and an (n,m)-groupoid (S,F) is idempotent iff for all $x \in S$, $F(x,...,x) = (x,...,x)$.

2. Co-ordinatizing Mendelsohn quadruple systems

Let S be a finite set of v elements. A cyclic quadruple $\langle abcd \rangle$, where a, b, c, d are distinct elements of S, is the following set of ordered pairs

$$\langle abcd \rangle = \{ (a,b), (b,c), (c,d), (d,a) \} .$$

A Mendelsohn quadruple system (MQS) of order v is a pair (S,T), where T is a collection of cyclic quadruples of elements of S, such that every ordered pair of distinct elements of S belongs to exactly one cyclic quadruple from T.

The necessary condition for the existence of a MQS of order v is

$$v(v-1) = 4|T| ,$$

which imply that if v is a positive integer such that $v \equiv 2,3 \pmod 4$, then there does not exist a MQS of order v.

Every MQS of order v is equivalent to a partition of the complet directed graph K_v^* into pairwise arc-disjoint 4-circuits. By a 4-circuit we mean a directed elementary circuit of length 4. Hence from the results of Schönheim [5] and Bermond, Faber [1] who proved independently that K_v^* is decomposable into 4-circuits iff $v(v-1) \equiv 0 \pmod 4$ and $v>4$, we get the spectrum of MQSs:

There exists a MQS of order v iff $v(v-1) \equiv 0 \pmod 4$ and $v>4$.

Now we shall show that a class of cyclic vector valued groupoids is equivalent to MQSs.

Theorem 1. Let (S,T) be a MQS. If on S we define a (2,2)-operation F such that for every $a \in S$ $F(a,a) = (a,a)$ and for all $a,b \in S$, $a \neq b$,

$$F(a,b) = (c,d) \Leftrightarrow \langle abcd \rangle \in T,$$

then (S,F) is an idempotent cyclic (2,2)-groupoid.

Proof. It is easy to see that F is well defined and since $\langle abcd \rangle = \langle bcda \rangle$, it follows that $F(a,b) = (c,d) \Rightarrow F(b,c) = (d,a)$.

The converse of the preceding theorem is not valid. Namely, if (S,F) is an idempotent cyclic (2,2)-groupoid and $F(a,b) = (c,d)$, then $\langle abcd \rangle$ need not be a cyclic quadruple. For example, if S is a set and F the identity mapping of S^2, then (S,F) is an idempotent cyclic (2,2)-groupoid which does not define a MQS. This example also shows that there exist idempotent cyclic (2,2)-groupoids of every order. We give also another example of an idempotent cyclic (2,2)-groupoid which does not define a MQS:

$$S = \{1, 2, 3, 4\}, \quad F(a,a) = (a,a) \text{ for all } a \in S,$$
$$F(1,2) = (1,3), \quad F(1,4) = (2,4), \quad F(2,3) = (4,3),$$
$$F(2,1) = (3,1), \quad F(4,1) = (4,2), \quad F(3,2) = (3,4).$$

The remaining values of F can be obtained from $F = F^{-1}$, where F^{-1} is the inverse mapping of F (since in every cyclic (n,n)-groupoid (S,F) F is a bijection and $F = F^{-1}$).

Definition 2. An idempotent cyclic (2,2)-groupoid (S,F) such that $a,b \in S$, $a \neq b$, $F(a,b) = (c,d)$ implies that the elements a,b,c,d are distinct, is called an M-(2,2)-groupoid.

The (2,2)-groupoid defined in Theorem 1 is obviously an M-(2,2)-groupoid.

Theorem 2. Let (S,F) be an M-(2,2)-groupoid of order v. If a family T of cyclic quadruples is defined by

$$\langle abcd\rangle \in T \Leftrightarrow F(a,b) = (c,d),$$

then (S,T) is a MQS of order v.

Hence from Theorems 1 and 2 it follows that there is an equivalence between MQSs and finite M-(2,2)-groupoids: every MQS defines and is defined by a finite M-(2,2)-groupoid.

3. Idempotent cyclic (2,2)-groupoids

We shall use the following notation. If (S,F) is a (2,2)-groupoid, then its component binary operations will be denoted by f and g, and in some cases (when we consider identities satisfied by f and g), we shall use $(\cdot)$ and $(*)$ instead of f and g respectively.

A groupoid (S,F) is called a left quasigroup iff for every $a,b \in S$ the equation $f(x,a) = b$ has a unique solution and iff $f(a,y) = b$ has a unique solution then (S,F) is called a right quasigroup.

Let (S,f) be a groupoid and σ a permutation of the set {1, 2, 3}. Then by

$$f^{\sigma}(x_{\sigma(1)}, x_{\sigma(2)}) = x_{\sigma(3)} \Leftrightarrow f(x_1, x_2) = x_3,$$

a groupoid (S,f^{σ}) is defined:

- if $\sigma(3) = 1$ and f is a left quasigroup,
- if $\sigma(3) = 2$ and f is a right quasigroup,
- if $\sigma(3) = 3$.

f^{σ} is called a σ-parastrophe of f or simply parastrophe.

Two operations f and g defined on the same set S are said to be orthogonal iff for every $a,b \in S$ the system $f(x,y) = a$, $g(x,y) = b$ has a unique solution.

Theorem 3. Let (S,F) be an idempotent cyclic (2,2)-groupoid. Then its components f and g satisfy the following conditions:

(i) f and g are idempotent,

(ii) f is a left and g is a right quasigroup,

(iii) f and g are orthogonal operations,

(iv) $f^{(123)} = g$, that is, g is a (123)-parastrophe of f,

(v) f and g satisfy the following identities (where $f = (\cdot)$, $g = (*)$)

$$(y(xy))x = y,$$
$$y*((x*y)*x) = x,$$
$$x*y = y(xy).$$

Proof. (ii) Let $a,b \in S$. Then there exist unique $x,y \in S$ such that $F(a,b) = (x,y)$, hence $F(y,a) = (b,x)$ and $F(b,x) = (y,a)$. So, for every $a,b \in S$ the equations $f(y,a) = b$ and $g(b,x) = a$ have unique solutions x and y.

(iii) For every $a,b \in S$ the system $f(x,y) = a$, $g(x,y) = b$, is equivalent to the equation $F(x,y) = (a,b)$, but the last equation has a unique solution $(x,y) \in S^2$ since $F(a,b) = (x,y)$.

(iv) Let $x,y \in S$. Then $f(x,y) = z$, $g(x,y) = u$ and $F(x,y) = (z,u)$, hence

$$F(u,x) = (y,z) = (f(u,x), g(u,x))$$
$$F(y,z) = (u,x) = (f(y,z), g(y,z)),$$

that is,

$$y = f(u,x),\ z = g(u,x),\ u = f(y,z),\ x = g(y,z).$$

We obtained that $f(x,y) = z$ implies $g(y,z) = x$, and $g(x,y) = u$ implies $f(u,x) = y$, which means that for every $x,y,z \in S$

$$f(x,y) = z \Leftrightarrow g(y,z) = x,$$

that is, $f^{(123)} = g$.

(v) Since for every $x,y \in S$

$$F(x,y) = (xy,\ x*y)$$

and

$$F(y,\ xy) = (x*y,\ x) = (y(xy),\ y*(xy)),$$
$$F(x*y,\ x) = (y,\ xy) = ((x*y)x,\ (x*y)*x),$$

we get

$$x*y = y(xy),\quad x = y*(xy),\quad y = (x*y)x,\quad xy = (x*y)*x.$$

From the first and the third of the preceding equalities it follows that

$$(y(xy))x = y$$

and from the second and the fourth

$$y*((x*y)*x)) = x.$$

Theorem 4. Let $(S,\cdot)$ be a groupoid. Then the identity

$$(y(xy))x = y \qquad (1)$$

is equivalent to the identity

$$(xy)(y(xy)) = x. \qquad (2)$$

Proof. If (1) is valid and we put in (1) as the variables y(xy) and x we get (2).

If (2) is valid and we put in (2) as the variables x and yx we get (1).

If $(S,\cdot)$ satisfies identities (1) and (2) and $a,b \in S$, then the equation

$$xa = b \qquad (3)$$

has a solution x = b(ab). If we suppose that (3) has another solution $y \neq x$, ya = b, then

$$a(ya) = ab$$

and

$$(ya)(a(ya)) = (ya)(ab),$$

hence y = b(ab).

So, $(S,\cdot)$ is a left quasigroup.

Theorem 5. If (S,F) is an idempotent cyclic (2,2)-groupoid and $F(x_1^2) = (x_3^4)$, where x_1^4 are not all equal, then $x_i \neq x_{i+1}$, $i = 1, 2, 3$ and $x_1 \neq x_4$.

Proof. If F(a,a) = (b,c), since F(a,a) = (a,a) it follows a = b = c. From F(a,b) = (b,c) it follows F(b,b) = (c,a) and as before we get a = b = c and analogously in other cases.

Theorem 6. If $(S,\cdot)$ is an idempotent cyclic (2,2)-groupoid such that its components f and g are quasigroups, then (S,F) is an M-(2,2)-groupoid.

Proof. If we suppose that F(a,b) = (a,c), $a \neq b$, then f(a,b) = a and since f is an idempotent quasigroup it follows that a = b. Similarly from F(a,b) = (c,b), $a \neq b$, we get g(a,b) = b, hence a = b.

The natural question whether the inverse of the preceding theorem is true, that is, are the components of an M-(2,2)-groupoid always quasigroups has a negative answer which follows from the next example.

Example. The MQS (S,T) where S = (1,...,8) and

T = { ‹1245›, ‹1356›, ‹1482›, ‹1523›, ‹1678›, ‹1754›, ‹1857›, ‹2584›, ‹2653›, ‹2746› ‹2837›, ‹3476›, ‹3687›, ‹3864› }

defines an M-(2,2)-groupoid (S,F) whose components f and g are not

quasigroups because

$$f(1,3) = 5,\ f(1,7) = 5 \quad \text{and} \quad g(6,1) = 5,\ g(4,1) = 5.$$

In the preceding example none of the component operations was a quasigroup. That component operations are both quasigroups or both are not quasigroups follows from the next theorem.

Theorem 7. Let $(S,\cdot)$ be an idempotent cyclic (2,2)-groupoid. Then one of its components is a quasigroup iff the other component is a quasigroup.

Proof. We suppose that g is a quasigroup and f is not. But f is a left quasigroup, hence there exist $a,b,c,d \in S$, $b \neq c$, such that

$$f(a,b) = f(a,c) = d,$$

or the equation $f(a,x) = b$ for some $a,b \in S$ does not have a solution at all. In the first case it follows that $F(a,b) = (d,x)$ and $F(a,c) = (d,y)$ for some $x,y \in S$. The cyclicity of F implies that $g(b,d) = a$ and $g(c,d) = a$, which contradicts the assumption that g is a quasigroup.

In the second case, which might be possible only if $|S| = \infty$, it follows that the equation $g(x,b) = a$ has no solution, which is a contradiction.

If we suppose that f is a quasigroup and g is not the proof is analogous.

Theorem 8. Let $(S,\cdot)$ be a groupoid. S is an idempotent groupoid satisfying the identity

$$(y(xy))x = y, \tag{4}$$

iff the (2,2)-groupoid (S,F) defined by

$$F(x,y) = (xy,\ y(xy))$$

is an idempotent cyclic (2,2)-groupoid.

Proof. Let $(S,\cdot)$ be an idempotent groupoid satisfying (4). (S,F) is obviously an idempotent (2,2)-groupoid. If $x,y \in S$, then

$$F(x,y) = (xy,\ y(xy))$$

and

$$F(y(xy),x) = ((y(xy))x,\ x((y(xy))x)) = F(y,\ xy),$$

hence (S,F) is a cyclic (2,2)-groupoid.

Conversely, let (S,F) be an idempotent cyclic (2,2)-groupoid. Then $(S,\cdot)$ is obviously idempotent and for all $x,y \in S$

$$F(x,y) = (xy,\ y(xy)),$$

hence

$$F(y(xy),x) = ((y(xy))x,\ x((y(xy))x)),$$

which by the cyclicity of F implies that $(y(xy))x = y$.

From Theorems 6,7 and 8 we get the following corollary.

Corollary. If $(S,\cdot)$ is an idempotent quasigroup satisfying the identity $(y(xy))x = y$, then the (2,2)-groupoid (S,F) defined by

$$F(x,y) = (xy,\ y(xy))$$

is an M-(2,2)-groupoid.

4. A construction of M-quasigroups

A groupoid (quasigroup) $(S,\cdot)$ satisfying the identities $(y(xy))x = y$ and $x^2 = x$ we shall call an M-groupoid (M-quasigroup). Now we shall give a construction of M-quasigroups which by the Corollary is also a construction of M-(2,2)-groupoids.

Let $F = GF(v)$ be a Galois field of order v. If $a,b \in F$, $a \neq 0$, $b \neq 0$, then by

$$x \circ y = ax + by \tag{5}$$

a quasigroup $(F,\circ)$ of order v is defined. We shall determine a,b such that $(F,\circ)$ be an M-quasigroup. Putting (5) in $(y\circ(x\circ y))\circ x = y$ and $x\circ x = x$ we get

$$\begin{cases} a^2 + 1 = 0, \\ a(a+b^2) = 1, \\ a + b = 1, \end{cases}$$

which is equivalent to

$$\begin{cases} a^2 = -1, \\ b = 1 - a. \end{cases} \tag{6}$$

Hence $(F,\circ)$ is an M-quasigroup iff a and b are nonzero elements of F satisfying (6).

We shall find all prime powers v for which system (6) has nonzero solutions a, b. The necessary condition for the existence of an M-quasigroup of order v is that $v(v-1) \equiv 0 \pmod 4$. Hence such v should be searched for among the numbers 4k and 4k+1, $k \in \mathbb{N}$.

If $v = 2^t$, $t \in \mathbb{N}$, then $1 = -1$, the multiplicative group G of the field is cyclic of odd order and the only element $a \in G$ such that $a^2 = 1$ is $a = 1$, but then $b = 0$. Hence system (6) does not have nonzero solutions in $GF(2^t)$.

If $v = p^t$, p prime $\neq 2$, and $v = 4k + 1$, $k \in \mathbb{N}$, then the multiplicative

group G of the field GF(v) is cyclic of order v-1 = 4k. Consequently, G has an element of order 4. Since a^2 is of order 2 and -1 is the only element of order 2 in G, it follows that $a^2 = -1$ and $1-a \neq 0$. Hence in this case system (6) has nonzero solutions.

Since the direct product of M-quasigroups is an M-quasigroup, by the described construction we can obtain M-quasigroups of order

$$v = p_1^{\alpha_1} \dots p_s^{\alpha_s},$$

where $p_1,\dots,p_s$ are primes and $\alpha_1,\dots,\alpha_s$ positive integers such that $p_i^{\alpha_i} \equiv 1 \pmod 4$ for all $i \in \{1,\dots,s\}$.

REFERENCES

1. J.C. Bermond, V. Faber, *Decomposition of the complete directed graph into k-circuits*, J. Combinatorial Theory, Ser. B, 21 (1976), 146-155.
2. G. Čupona, J. Ušan, Z. Stojaković, *Multiquasigroups and some related structures*, Maced. Acad. Sci. and Arts, Contributions, Sect. Math. Techn. Sci. I 2, 1980, 5-12.
3. G. Čupona, Z. Stojaković, J. Ušan, *On finite multiquasigroups*, Publ. Inst. Math. Belgrade, 29 (43), 1981, 53-59.
4. G. Čupona, *Vector valued semigroups*, Semigroup Forum, 26, 1983, 65-74.
5. J. Schönheim, *Partitions of the edges of the directed complete graph into 4-cycles*, Discrete Math., 11 (1975), 67-70.
6. Z. Stojaković, *On bisymmetric [n,m]-groupoids*, Univ. u Novom Sadu, Zb. rad. Prir.-mat. fak., 12, 1982, 399-405.
7. Z. Stojaković, *On cyclic n-quasigroups*, Univ u Novom Sadu, Zb. rad. Prir.-mat. fak., 12, 1982, 407-415.
8. Z. Stojaković, *A generalization of Mendelsohn triple systems*, Ars Combinatoria, 18, 1984, 131-138.
9. Z. Stojaković, *Cyclic vector valued groupoids* (to appear).
10. Z. Stojaković, Đ. Paunić, *Self-orthogonal cyclic n-quasigroups*, Aequationes Math., 30, 1986, 252-257.

Institute of Mathematics
University of Novi Sad
21000 Novi Sad
Yugoslavia

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

CLOSURE OPERATORS AND CONSEQUENCE RELATIONS

Z. Šikić, Zagreb

I We consider the multiple consequence relation as defined in [S]. The definition is there prompted by the following line of argument: To say that a set of conclusions follows from a given set of premisses is to say that at least one of the conclusions must be true if the premisses are all true. That means that each possible state of affairs in which all the premisses are true is one in which some of the conclusions are true. Assuming the formulae of our language $\mathcal{L}$ to be capable of truth and untruth, each relevant state of affairs is represented by the partition (T,U) of formulae of $\mathcal{L}$ such that the formulae of T are true in this state of affairs, while the formulae of U are untrue in it. If $\mathcal{M}$ is the set of all partitions which correspond to the possible states of affairs, it is plausible to define the consequence relation with regard to $\mathcal{M}$ as follows.

Definition 1. Let X and Y be sets of formulae of $\mathcal{L}$ i.e. $X \subset \mathcal{L}$ and $Y \subset \mathcal{L}$. Y is a consequence of X with regard to $\mathcal{M}$ i.e.

$$X \models_{\mathcal{M}} Y$$

iff there is no $(T,U) \in \mathcal{M}$ such that $X \subset T$ and $Y \subset U$. It is also said that the set of partitions $\mathcal{M}$ generates the consequence relation $\models_{\mathcal{M}}$.

If we presuppose nothing about the internal structure of the formulae of $\mathcal{L}$, and about their semantical interconnections, we have to be prepared to allow any set of partitions of formulae

to play the role of $\mathcal{M}$. So, we are led to the general definition of the multiple consequence relation proposed in [S].

Definition 2. A relation $\models$ on $\mathcal{P}(\mathcal{L})$ is a consequence relation iff there is a set of partitions $\mathcal{M}$ such that $\models = \models_{\mathcal{M}}$.

Remark: Each set of partitions $\mathcal{M}$ determines, and is completely determined, by $\mathcal{T} = \{T:(\exists U)(T,U)\in\mathcal{M}\}$ which will be called its true set, or by $\mathcal{U} = \{U:(\exists T)(T,U)\in\mathcal{M}\}$ which will be called its untrue set. So, we will talk about consequence with regard to $\mathcal{M}$, or with regard to $\mathcal{T}$, or with regard to $\mathcal{U}$, synonymously and we will use the notations $\models_{\mathcal{M}}$, $\models_{\mathcal{T}}$, $\models_{\mathcal{U}}$ interchangeably.

We consider the three special cases (i.e. restrictions) of the consequence relation $\models$.

(i) The most common single-conclusion relation which permits only one conclusion and which accordingly has instances of the form

$$X \models B \qquad X\subset\mathcal{L},\ B\in\mathcal{L}.$$

(ii) The single-premiss relation which permits only one premiss and which accordingly has instances of the form

$$A \models Y \qquad A\in\mathcal{L},\ Y\subset\mathcal{L}.$$

(iii) The singular relation which permits only one premiss and only one conclusion, and which accordingly has instances of the form

$$A \models B \qquad A\in\mathcal{L},\ B\in\mathcal{L}.$$

It is evident that these restrictions satisfy

(1) $\vdash \;=\; \Vdash \cap \models$

The characterization theorem, proved in [S] p.16, states that a single-conclusion relation is a consequence relation iff it is closed under

overlap	$B \in X \longrightarrow X \Vdash B$
dilution	$X' \Vdash B \;\&\; X' \subset X \longrightarrow X \Vdash B$, and
cut for sets	$X,Z \Vdash B \;\&\; (\forall A \subseteq Z) X \Vdash A \longrightarrow X \Vdash B.$

Results on counterparts, in ch. 5 of [S] (p.72-74.), may be understand as proving that different sets of partitions may generate one and the same single-conclusion consequence relation.

Considering single-conclusion (single-premiss) consequence relations as closure operators, in a Tarskian way, we will find simple conditions that must be satisfied by different sets of partitions in order to generate the same consequence relation. Incidentally the characterization theorem for single-conclusion (single-premiss) consequence relations will turn out to be an immediate corollary to the characterization theorem for closure operators.

II A single-conclusion relation $\Vdash$, with instances of the form $X \Vdash B$ ($X \subset \mathcal{L}$, $B \in \mathcal{L}$), determines and is completely determined by the corresponding consequence-operator

$\Vdash : \wp(\mathcal{L}) \longrightarrow \wp(\mathcal{L})$ defined by $^{\Vdash}\overline{X} = \{B : X \Vdash B\}$.

A consequence-operator $\Vdash^{\mathcal{T}}$, which corresponds to $\Vdash_{\mathcal{T}}$, may be characterized refering directly to the true set $\mathcal{T}$. This is the content of the following lemma.

Lemma 1. A consequence-operator $\vdash_{\mathcal{T}}$ corresponds to the single-conclusion consequence relation $\|\!\sim_{\mathcal{T}}$ iff $\vdash_{\mathcal{T}} X = \bigcap \{T : X \subset T \ \& \ T \in \mathcal{T}\}$.

Proof: $A \in \vdash_{\mathcal{T}} X$ iff $X \|\!\sim_{\mathcal{T}} A$ iff $(\forall T)(X \subset T \ \& \ T \in \mathcal{T} \longrightarrow A \in \mathcal{T})$ iff $A \in \bigcap \{T : X \subset T \ \& \ T \in \mathcal{T}\}$.

Hence, the consequence-operator $\vdash_{\mathcal{T}} : \mathcal{P}(\mathcal{L}) \longrightarrow \mathcal{P}(\mathcal{L})$ is a closure operator on $\mathcal{L}$, in the sense of the following definition.

Definition 3. Let $\mathcal{L}$ be any set and let $\mathcal{T}$ be any set of subsets of $\mathcal{L}$, i.e. $\mathcal{T} \subset \mathcal{P}(\mathcal{L})$. The closure operator generated by $\mathcal{T}$ is a function $^{-\mathcal{T}} : \mathcal{P}(\mathcal{L}) \longrightarrow \mathcal{P}(\mathcal{L})$, such that $\overline{X}^{\mathcal{T}} = \bigcap \{T : X \subset T \ \& \ T \in \mathcal{T}\}$.
A function $^- : \mathcal{P}(\mathcal{L}) \longrightarrow \mathcal{P}(\mathcal{L})$ is a closure operator on $\mathcal{L}$ iff there exists $\mathcal{T} \subset \mathcal{P}(\mathcal{L})$ such that $^- = {}^{-\mathcal{T}}$.

Note that we impose no condition on $\mathcal{T}$ (such as the intersection property or something else). $\mathcal{T}$ may be any subset of $\mathcal{P}(\mathcal{L})$.

It is quite easy to prove the following lemmas on closure operators.

Lemma 2. Any closure operator $^-$ has the following properties:
1. $X \subset \overline{X}$, 2. $Y \subset X \longrightarrow \overline{Y} \subset \overline{X}$ and 3. $\overline{X} = \overline{\overline{X}}$.

Lemma 3. A function $^- : \mathcal{P}(\mathcal{L}) \longrightarrow \mathcal{P}(\mathcal{L})$ with properties 1, 2. and 3. (from lemma 2.) is a closure operator on $\mathcal{L}$.

Proof: It is easy to check that $^- = {}^{-\mathcal{T}}$ for $\mathcal{T} = \{T : T \subset \mathcal{L} \ \& \ T = \overline{T}\}$.

Definition 4. The canonical extension of $\mathcal{T} \subset \mathcal{L}$ is the set $\overline{\mathcal{T}} = \{T : T \subset \mathcal{L} \ \& \ T = \overline{T}^{\mathcal{T}}\}$.

Lemma 4.

(i) $\mathcal{T} \subset \overline{\mathcal{T}}$ and $\overline{\overline{\mathcal{T}}} = \overline{\mathcal{T}}$.

(ii) $-^{\mathcal{T}} = -^{\overline{\mathcal{T}}}$ (cf. lemma 3.).

(iii) $-^{\mathcal{T}_1} = -^{\mathcal{T}_2}$ iff $\overline{\mathcal{T}}_1 = \overline{\mathcal{T}}_2$ (cf. lemma 3.).

Lemma 5. $\overline{\mathcal{T}}$ is the largest generator of $-^{\mathcal{T}}$.

Lemma 6. The canonical extension of $\mathcal{T} \subset \mathcal{L}$ is the intersection extension i.e. $\overline{\mathcal{T}} = \{X : (\exists \mathcal{A})(\mathcal{A} \subset \mathcal{T} \ \& \ X = \cap \mathcal{A})\}$.

Proof: If $\mathcal{A} \subset \mathcal{T}$ & $X = \cap \mathcal{A}$ then

$$\overline{X}^{\mathcal{T}} = \cap \{T : X \subset T \ \& \ T \in \mathcal{T}\} \subset \cap \{T : X \subset T \ \& \ T \in \mathcal{A}\} = \cap \{T : T \in \mathcal{A}\} = X$$

i.e. $\overline{X}^{\mathcal{T}} \subset X$. Hence, $\overline{X}^{\mathcal{T}} = X$. So we have proved that $\{X : (\exists \mathcal{A})(\mathcal{A} \subset \mathcal{T} \ \& \ X = \cap \mathcal{A})\} \subset \overline{\mathcal{T}}$. On the other hand from $\overline{X}^{\mathcal{T}} = X$ it follows that $X = \cap \{T : X \subset T \ \& \ T \in \mathcal{T}\}$ i.e. $X = \cap \mathcal{A}$ for $\mathcal{A} = \{T : X \subset T \ \& \ T \in \mathcal{T}\} \subset \mathcal{T}$. Hence,

$$\overline{\mathcal{T}} = \{X : X \subset \mathcal{L} \ \& \ X = \overline{X}^{\mathcal{T}}\} \subset \{X : (\exists \mathcal{A})(\mathcal{A} \subset \mathcal{T} \ \& \ X = \cap \mathcal{A})\}.$$

Taking into account that a consequence-operator is a closure operator, the characterization theorem and the equivalent generators theorem follow at once.

Characterization theorem 1. An operator $\overline{\ } : \mathfrak{P}(\mathcal{L}) \longrightarrow \mathfrak{P}(\mathcal{L})$ is a consequence-operator iff 1. $X \subset \overline{X}$, 2. $Y \subset X \rightarrow \overline{Y} \subset \overline{X}$ and 3. $\overline{X} = \overline{\overline{X}}$.

Equivalent generators theorem 1. True (untrue) sets generate one and the same consequence-operator iff their intersection (union)

extension is the same. The completion is the largest generator of the consequence-operator.

Taking into account the simple and natural connection between consequence-operators and single-conclusion consequence relations, we derive the characterization theorem of [S], and the sought for characterization of equivalent generators, as simple corrolaries.

Corrolary 1. A single-conclusion relation is a consequence relation iff it is closed under overlap, dilution and cut for sets.

Proof: It is quite easy to see that 1, 2. and 3. of the characterization theorem are equivalent to overlap, dilution and cut for sets. Namely, $B \in X \longrightarrow X \vdash B$ i.e. $(\forall B \in X) X \vdash B$ iff $(\forall B \in X) B \in \overline{X}$ i.e. $X \subset \overline{X}$. Hence, overlap is equivalent to 1. Similarly, $X' \vdash B \;\&\; X' \subset X \longrightarrow X \vdash B$ iff $X' \subset X \longrightarrow (B \in \overline{X}' \longrightarrow B \in \overline{X})$ i.e. $X' \subset X \longrightarrow \overline{X}' \subset \overline{X}$. Hence, dilution is equivalent to 2. Finally, $X, Z \vdash B \;\&\; (\forall A \in Z) X \vdash A \longrightarrow X \vdash B$ iff $Z \subset X \longrightarrow (B \in \overline{X \cup Z} \longrightarrow B \in \overline{X})$ i.e. $Z \subset \overline{X} \longrightarrow \overline{X \cup Z} \subset \overline{X}$. Hence, cut is equivalent to $Z \subset \overline{X} \longrightarrow \overline{X \cup Z} \subset \overline{X}$. Substituting $\overline{X}$ for Z we see that 3. follows from overlap, dilution and cut. On the other hand, presupposing $Z \subset \overline{X}$ it follows from 1. that $X \cup Z \subset \overline{X}$, and then from 2. that $\overline{X \cup Z} \subset \overline{X}$, and then from 3. that $\overline{X \cup Z} \subset \overline{X}$. Hence, cut follows from 1, 2. and 3.

Corrolary 2. True (untrue) sets generate one and the same single-conclusion consequence relation iff their intersection (union) extension is the same. The extension is the largest generator of the single-conclusion consequence relation.

III A single-premiss relation $\models$, with instances of the form $A \models Y$ ($A \in \mathcal{L}$, $Y \subset \mathcal{L}$), determines and is completely determined by the corresponding assumption-operator $\vdash : \mathcal{P}(\mathcal{L}) \longrightarrow \mathcal{P}(\mathcal{L})$ defined by

$$\vdash Y = \{A : A \models Y\}.$$

An assumption operator $\vdash_{\mathcal{U}}$, which corresponds to $\models_{\mathcal{U}}$, may be characterized refering directly to the untrue set $\mathcal{U}$.

Lemma 7. An assumption-operator $\vdash_{\mathcal{U}}$ corresponds to the single-premiss consequence relation $\models_{\mathcal{U}}$ iff $\vdash_{\mathcal{U}} Y = \bigcap \{U : Y \subset U \& U \in \mathcal{U}\}$.

Proof: Analogous to that of lemma 1.

Hence, the assumption-operator $\vdash_{\mathcal{U}} : \mathcal{P}(\mathcal{L}) \longrightarrow \mathcal{P}(\mathcal{L})$ is a closure operator on $\mathcal{L}$, and the characterization theorem, as well as the equivalent generators theorem, are as before.

Characterization theorem 2. An operator $\overline{} : \mathcal{P}(\mathcal{L}) \longrightarrow \mathcal{P}(\mathcal{L})$ is an assumption-operator iff 1. $X \subset \overline{X}$, 2. $Y \subset X \longrightarrow \overline{Y} \subset \overline{X}$ and 3. $\overline{X} = \overline{\overline{X}}$.

Equivalent generators theorem 2. Untrue (true) sets generate one and the same assumption-operator iff their intersection (union) extension is the same. The extension is the greatest generator of the assumption-operator.

Taking into account the simple and natural connection between assumption-operators and single-premiss consequence relations we easily derive the corrolaries:

Corrolary 3. A single-premiss relation is a consequence relation iff it is closed under

overlap $\quad A \in Y \longrightarrow A \models Y,$

dilution $\quad A \models Y' \ \& \ Y' \subset Y \longrightarrow A \models Y$ and

cut for sets $\quad A \models Y,Z \ \& \ (\forall B \in Z) B \models Y \longrightarrow A \models Y.$

Corrolary 4. Untrue (true) sets generate one and the same single-premiss consequence relation iff their intersection (union) extension is the same. The extension is the largest generator of the single-premiss consequence relation.

Let $\mathcal{M}$ be a set of partitions of $\mathcal{L}$, $\mathcal{T} = \{T:(\exists U)(T,U) \in \mathcal{M}\}$ its true set and $\mathcal{U} = \{U:(\exists T)(T,U) \in \mathcal{M}\}$ its untrue set. From (1) follows

(2) $$\vdash_{\mathcal{M}} = \models_{\mathcal{T}} \cap \models_{\mathcal{U}}.$$

Taking into account (2), corrolaries 1. and 3. imply

Corrolary 5. A singular relation $\vdash$ is a consequence relation iff it is closed under

overlap $\quad A \vdash A$ and

dilution $\quad A \vdash B \ \& \ B \vdash C \longrightarrow A \vdash C.$

Corrolary 6. is a simple consequence of corrolaries 2. and 4.

Corrolary 6. True (untrue) sets generate one and the same singular consequence relation iff their intersection-union extension is the same. The extension is the largest generator of the singular consequence relation (i.e. the largest generator, true and untrue, is closed under unions and intersections).

Remark: Corrolaries 5. and 6. may be seen as abstract algebraic results on pre- ordered sets. Corrolary 5. asserts

that each $\mathcal{T} \subset \mathcal{P}(S)$ induces a pre- order on S defined by $a \leq b :=: \neg(\exists T \in \mathcal{T})(a \in T \& b \notin T)$, and conversely, that each pre- order on S is induced by such a subset of $\mathcal{P}(S)$. Corrolary 6. asserts that subsets of $\mathcal{P}(S)$ induce the same pre- order on S iff they have the same intersection-union completion and that this completion is the largest generator of the pre- order.

[S] Shoesmith, D.J. & Smiley, T.J, Multiple-conclusion Logic, Cambridge University Press, 1978.

FAKULTET STROJARSTVA
I BRODOGRADNJE
SVEUČILIŠTA U ZAGREBU
41000 ZAGREB, ĐURE SALAJA 5

Yugoslavia

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

О НЕКОТОРЫХ ПОСТРОЕНИЯХ ПОЧТИ-РЕШЕТОК

Янез Ушан

Резюме

В [1] определены почти-решетки как одно обобщение решеток и рассмотрены некоторые построения почти-решеток одноэлементными продолжениеями решеток или почти-решеток. В настоящей работе рассматриваются новые построения почти-решеток.

ОПРЕДЕЛЕНИЕ 1. [1] Пусть (Q,∇) и (Q,Δ) коммутативные полугруппы. Объект (Q,∇,Δ) называется почти-решеткой тогда и только тогда, когда имеет место:

ПР1 $\quad x\nabla x = x$ и $x\Delta x = x$; и

ПР2 $\quad x\Delta(y\nabla z\nabla x) = (x\Delta y)\nabla(x\Delta z)\nabla(x\Delta x)$ [1)] для любых $x,y,z \in Q$.

УТВЕРЖДЕНИЕ 1. [1] Пусть $(\hat{Q},\nabla,\Delta)$ любая почти-решетка. Пусть, далее,

(1) $\quad Q \overset{\text{деф}}{=} \hat{Q}\cup\{e\}, \quad e \notin \hat{Q},$

и имеет место

---

1) обессиленная дистрибутивность.

This paper is in final form and no version of it will be submited for publication elsewhere.
AMS Mathematics Subject Classification (1980): 20N99
Key words and phrases: semigroups, lattices, near-lattices, weak-distributivity.

$$(2)\qquad x\textcircled{\scriptsize$\nabla$}y \overset{\text{деф}}{=} \begin{cases} x\nabla y, & (x,y) \in \hat{Q}^2 \\ x,y = e,x \in Q \\ y,x = e,y \in Q \end{cases};$$

$$(3)\qquad x\textcircled{\scriptsize$\Delta$}y \overset{\text{деф}}{=} \begin{cases} x\ y, & (x,y) \in \hat{Q}^2 \\ x,y = e,x \in Q \\ y,x = e,y \in Q. \end{cases}$$

Тогда $(Q,\textcircled{\scriptsize$\nabla$},\textcircled{\scriptsize$\Delta$})$ почти-решетка неявляющаяся решеткой.

Каждая решетка является почти-решеткой; утверждение 1 из [1]. Таким образом, следствием утверждения 1 является следующее утверждение:

УТВЕРЖДЕНИЕ 1′. [1] Пусть $(\hat{Q},\cup,\cap)$ любая решетка. Пусть, далее,

$$(\bar{1})\qquad Q \overset{\text{деф}}{=} \hat{Q} \cup \{e\},\quad e \notin \hat{Q},$$

и имеет место

$$(\bar{2})\qquad x \nabla y \overset{\text{деф}}{=} \begin{cases} x\cup y, & (x,y) \in \hat{Q}^2 \\ x,y = e,x \in Q \\ y,x = e,x \in Q \end{cases};$$

$$(\bar{3})\qquad x \nabla y \overset{\text{деф}}{=} \begin{cases} x\cap y, & (x,y) \in \hat{Q}^2 \\ x,y = e,x \in Q \\ y,x = e,y \in Q. \end{cases}$$

Тогда (Q,∇,Δ) почти-решетка неявляющаяся решеткой.

ТЕОРЕМА 2. Пустя $(\hat{Q},\nabla,\Delta)$ и $(E,\bar{\nabla},\bar{\Delta})$ любые почти-решетки такие, что $\hat{Q} \cap E = \emptyset$. Пусть, далее,

$$(\bar{\bar{1}})\qquad Q \overset{\text{деф}}{=} \hat{Q} \cup E,\ \hat{Q} \cap E = \emptyset;$$

и имеет место

$$(\bar{\bar{2}})\qquad x\textcircled{\scriptsize$\nabla$}y \overset{\text{деф}}{=} \begin{cases} x \nabla y, & (x,y) \in \hat{Q}^2 \\ x,y \in E, x \in \hat{Q} \\ y,x \in E, y \in \hat{Q} \\ x\ \bar{\nabla}\ y, & (x,y) \in E^2 \end{cases}$$

$$(\bar{\bar{3}})\qquad x\textcircled{\scriptsize$\Delta$}y \overset{\text{деф}}{=} \begin{cases} x\Delta y, & (x,y) \in \hat{Q}^2 \\ x,y \in E, x \in \hat{Q} \\ y,x \in E, y \in \hat{Q} \\ x\Delta y, & (x,y) \in E^2. \end{cases}$$

Тогда $(Q,\overset{\vee}{\vee},\overset{\wedge}{\wedge})$ почти-решетка неявляющаяся решеткой.

Доказательство

а) Из определения $(\bar{1})$-$(\bar{3})$ непосредственно следует, что каждый $e \in E$, $e \notin \hat{Q}$, является единицей группоидов $(\hat{Q} \cup \{e\},\overset{\vee}{\vee})$ и $(\hat{Q} \cup \{e\},\overset{\wedge}{\wedge})$.

б) Учитывая предположение, что $(\hat{Q},\vee,\wedge)$ и $(E,\bar{\vee},\underline{\wedge})$ почти-решетки, т.е., что в $(\hat{Q},\vee,\wedge)$ и $(E,\bar{\vee},\underline{\wedge})$ имеет метсо ПР1, ввиду (2) и (3), находим, что в $(Q,\overset{\vee}{\vee},\overset{\wedge}{\wedge})$, также, имеет место ПР1.

в) Ввиду а) и предположения, что $(\hat{Q},\vee,\wedge)$ и $(E,\bar{\vee},\underline{\wedge})$ почти-решетки, находим, что $(Q,\overset{\vee}{\vee})$ и $(Q,\overset{\wedge}{\wedge})$ коммутативные полугруппы.

г) Учитывая предположение, что $(Q,\vee,\wedge)$ и $(E,\bar{\vee},\underline{\wedge})$ почти-решетки, т.е., что в почти-решетке $(S,\smile,\frown)$ имеет место

ПР3 $\quad x \frown (y \smile x) = x \smile (y \frown x)$[1] для любых $x,y \in S$[2];

и, ввиду а), имеют место равенства

$$x \overset{\wedge}{\wedge} (e \overset{\vee}{\vee} x) = x \overset{\vee}{\vee} (e \overset{\wedge}{\wedge} x) = x \quad \text{и}$$

(e) $\quad e \overset{\wedge}{\wedge} (x \overset{\vee}{\vee} e) = e \overset{\vee}{\vee} (x \overset{\wedge}{\wedge} e) = x$

для любого $x \in \hat{Q}$ и любого $e \in E$, находим, что в $(Q,\overset{\vee}{\vee},\overset{\wedge}{\wedge})$, также, имеет место ПР3. Притом, так как равенства под (e) имеют место для любого $x \in \hat{Q}$ и любого $e \in E$, где $\hat{Q} \cap E = \emptyset$, находим что в $(Q,\overset{\vee}{\vee},\overset{\wedge}{\wedge})$ не имеют место законы поглощения. В самом делее, отсюда получаем, что $(Q,\overset{\vee}{\vee},\overset{\wedge}{\wedge})$ не является решеткой.

д) Так как ПР2 имеет место в $(Q,\vee,\wedge)$ и в $(E,\bar{\vee},\underline{\wedge})$, то ПР2 имеет место для всех $x,y,z \in Q$ и для всех $x,y,z \in E$.

Ввиду а) и в), имеют место равенства

$$e \overset{\wedge}{\wedge} (y \overset{\vee}{\vee} z \overset{\vee}{\vee} e) = y \overset{\vee}{\vee} z \quad \text{и}$$

$$(e \overset{\wedge}{\wedge} y) \overset{\vee}{\vee} (e \overset{\wedge}{\wedge} z) \overset{\vee}{\vee} (e \overset{\wedge}{\wedge} e) = y \overset{\vee}{\vee} z$$

для любых $y,z \in Q$ и любого $e \in E$. Отсюда находим, что ПР2 имеет место в $(Q,\overset{\vee}{\vee},\overset{\wedge}{\wedge})$ для всех $y,z \in Q$ и любого $x = e \in E$.

---

[1] обессилнное поглощение.

[2] утверждение 2 из [1].

Ввиду а), б) и в), находим, что имеют место равенства

$$x \textcircled{\Delta} (e \textcircled{\nabla} z \textcircled{\nabla} x) = x \textcircled{\Delta} (z \textcircled{\nabla} x) \quad \text{и}$$

$$(x \textcircled{\Delta} e) \textcircled{\nabla} (x \textcircled{\Delta} z) \textcircled{\nabla} (x \textcircled{\Delta} x) = x \textcircled{\nabla} (z \textcircled{\Delta} x)$$

для любых $x, z \in Q$ и любого $e \in E$. Отсюда, ввиду г), находим, что ПР2 имеет место в $(Q, \textcircled{\nabla}, \textcircled{\Delta})$ для всех $x, z \in Q$ и любого $y = e \in E$. Одновременно, ввиду в), мы получили, что ПР2 имеет место в $(Q, \textcircled{\nabla}, \textcircled{\Delta})$ для всех $x, y \in Q$ и любого $z = e \in E$.

Ввиду а) и в) находим, что имеют место равенства

$$x \textcircled{\Delta} (e_1 \textcircled{\nabla} e_2 \textcircled{\nabla} x) = x \textcircled{\Delta} x \quad \text{и}$$

$$(x \textcircled{\Delta} e_1) \textcircled{\nabla} (x \textcircled{\Delta} e_2) \textcircled{\nabla} (x \textcircled{\Delta} x) = x \textcircled{\nabla} x \textcircled{\nabla} (x \textcircled{\Delta} x)$$

для любого $x \in Q$ и любых $e_1, e_2 \in E$. Отсюда, ввиду б) и в) находим, что ПР2 имеет место для любого $x \in Q$ и любых $y, z \in E$.

Теорема доказана.

Каждая решетка является почти-решеткой; утверждение 1 из [1]. Таким образом, следствием теоремы 2 является следующее утверждение:

ТЕОРЕМА 3. Пусть $(\hat{Q}, \cup, \cap)$ и $(E, \vee, \wedge)$ любые решетки, такие, что $\hat{Q} \cap E = \emptyset$. Пусть, далее,

$$(\hat{1}) \qquad Q \overset{\text{деф}}{=} \hat{Q} \cup E, \quad \hat{Q} \cap E = \emptyset,$$

и имеет место

$$(\hat{2}) \qquad x \nabla y \overset{\text{деф}}{=} \begin{cases} x \cup y, & (x,y) \in \hat{Q}^2 \\ x, y \in E, x \in \hat{Q} \\ y, x \in E, y \in \hat{Q} \\ x \vee y, & (x,y) \in E^2 \end{cases}$$

$$(\hat{3}) \qquad x \Delta y \overset{\text{деф}}{=} \begin{cases} x \cap y, & (x,y) \in \hat{Q}^2 \\ x, y \in E, x \in \hat{Q} \\ y, x \in E, y \in E \\ x \wedge y, & (x,y) \in E^2. \end{cases}$$

Тогда (Q, ∇, Δ) почти-решетка неявляющаяся решеткой.

ПРИМЕЧАНИЕ

Если $|E| = 1$ теорема 2 станет утверждением 1. Таким же образом, теорема 3 при $|E| = 1$ станет утверждением 1'.

Обобщением утверждения 5 из [1], имеющие одно и то же доказательство, является следующее утверждение:

УТВЕРЖДЕНИЕ 4. Пусть $(\hat{Q},\cup,\cap)$ и $(E,\vee,\wedge)$ любые решетки, такие, что $\hat{Q} \cap E = \emptyset$. Притом, пусть решетка $(\hat{Q},\cup,\cap)$ обладающая по меньшей мере двумя элементами $a,b \in \hat{Q}$ удовлетворяющими условию $a \leq b$ и $a \neq b$. Пусть далее, объект (Q,∇,Δ) определен через $(\hat{1})$-$(\hat{3})$ из теоремы 3. Тогда в (Q,∇,Δ) не имеют место закон дистрибутивности и закон модулярности.

Обобщением утверждения 6 из [1], имеющие подобные доказательства, является следующее утверждение:

УТВЕРЖДЕНИЕ 5. Пусть $(\hat{Q},\cup,\cap)$ и $(E,\vee,\wedge)$ любые решетки такие что $Q \cap E = \emptyset$. Пусть, далее, объект (Q,∇,Δ) определен через $(\hat{1})$-$(\hat{3})$ из теоремы 3. Тогда в (Q,∇,Δ) имеет место

ПР2' $\quad x \nabla (y \Delta z \Delta x) = (x \nabla y) \Delta (x \nabla z) \Delta (x \nabla x)$ [1)]

для всех $x,y,z \in Q$.

ТЕОРЕМА 6. Пусть $(\hat{Q},\nabla,\Delta)$ и $(\emptyset,\bar{\nabla},\underline{\Delta})$ любые почти-решетки такие, что $\hat{Q} \cap \emptyset = \emptyset$. Пусть, далее,

(1') $\quad Q \overset{\text{деф}}{=} \hat{Q} \cup \emptyset,\ \hat{Q} \cap \emptyset = \emptyset,$

и имеет место

(2') $$x \textcircled{\nabla} y = \begin{cases} x \nabla y, & (x,y) \in \hat{Q}^2 \\ x,y \in \hat{Q},\ x \in \emptyset \\ y,x \in \hat{Q},\ y \in \emptyset & ; \\ x \bar{\nabla} y, & (x,y) \in \emptyset^2 \end{cases}$$

---

1) Дуал от ПР2.

$$(3') \qquad x \textcircled{\Delta} y = \begin{cases} x \Delta y, & (x,y) \in \hat{Q}^2 \\ x,y \in \hat{Q}, & x \in 0 \\ y,x \in \hat{Q}, & y \in 0 \\ x \underline{\Delta} y, & (x,y) \in 0^2 \end{cases}$$

Тогда $(Q, \textcircled{\nabla}, \textcircled{\Delta})$ почти-решетка неявляющаяся решеткой.

Доказательство

а) Из определения (1')-(3') непосредственно следует, что каждый $0 \in 0$, $0 \notin \hat{Q}$, является нулем группоидов $(\hat{Q} \cup \{0\}, \textcircled{\nabla})$ и $(\hat{Q} \cup \{0\}, \textcircled{\Delta})$, т.е., что имеют место формулы

$$(\forall x \in \hat{Q} \cup \{0\})(\forall y \in \hat{Q} \cup \{0\})(x = 0 \vee y = 0 \Rightarrow x \textcircled{\nabla} y = 0)$$

и

$$(\forall x \in \hat{Q} \cup \{0\})(\forall y \in \hat{Q} \cup \{0\})(x = 0 \vee y = 0 \Rightarrow x \textcircled{\Delta} y = 0).$$

б) Учитывая предположение, что $(\hat{Q}, \nabla, \Delta)$ и $(0, \bar{\nabla}, \underline{\Delta})$ почти-решетки, т.е., что в $(\hat{Q}, \nabla, \Delta)$ и $(0, \bar{\nabla}, \underline{\Delta})$ имеет место ПР1, ввиду (2') и (3'), находим, что в $(Q, \textcircled{\nabla}, \textcircled{\Delta})$, также, имеет место ПР1.

в) Ввиду а) и предположения, что $(\hat{Q}, \nabla, \Delta)$ и $(0, \bar{\nabla}, \underline{\Delta})$ почти-решетки, находим, что $(Q, \textcircled{\nabla})$ и $(Q, \textcircled{\Delta})$ коммутативные полугруппы.

г) Учитывая предположение, что $(\hat{Q}, \nabla, \Delta)$ и $(0, \bar{\nabla}, \underline{\Delta})$ почти-решетки, т.е., что в почти-решетке $(S, \cup, \cap)$ имеет место

ПР3 $\quad x \cap (y \cup x) = x \cup (y \cap x)$[1] для любых $x,y \in S$[2];

и, ввиду а), имеют место равенства

$$(0) \qquad x \textcircled{\Delta} (0 \textcircled{\nabla} x) = x \textcircled{\nabla} (0 \textcircled{\Delta} x) = 0 \text{ и}$$

$$0 \textcircled{\Delta} (x \textcircled{\nabla} 0) = 0 \textcircled{\nabla} (x \textcircled{\Delta} 0) = 0$$

для любого $x \in \hat{Q}$ и любого $0 \in 0$, находим, что в $(Q, \textcircled{\nabla}, \textcircled{\Delta})$, также, имеет место ПР3. Притом, так как равенства под (0) имеют ме-

---

[1] обессиленное поглощение.
[2] утверждение 2 из [1].

сто для каждого $x \in \hat{Q}$ и каждого $0 \in \mathbb{0}$, где $\hat{Q} \cap \mathbb{0} = \emptyset$, находим, что в $(Q, \textcircled{\nabla}, \textcircled{\Delta})$ не имеют место законы поглощения. В Самом делее, отсюда получаем, что $(Q, \textcircled{\nabla}, \textcircled{\Delta})$ не является решеткой.

д) Так как ПР2 имеет место в $(\hat{Q}, \nabla, \Delta)$ и в $(\mathbb{0}, \bar{\nabla}, \underline{\Delta})$, то ПР2 имеет место для всех $x,y,z \in \hat{Q}$ и для всех $x,y,z \in \mathbb{0}$.

Ввиду а) и в), имеют место равенства

$$0 \textcircled{\Delta} (y \textcircled{\nabla} z \textcircled{\nabla} 0) = 0$$

$$(0 \textcircled{\Delta} y) \textcircled{\nabla} (0 \textcircled{\Delta} z) \textcircled{\nabla} (0 \textcircled{\Delta} 0) = 0$$

для любых $y,z \in Q$ и любого $0 \in \mathbb{0}$. Отсюда находим, что ПР2 имеет место в $(Q, \textcircled{\nabla}, \textcircled{\Delta})$ для всех $y,z \in Q$ и любого $x \in \mathbb{0}$.

Подобним способом, ввиду а), в) и факта, что $\textcircled{\nabla}$ и $\textcircled{\Delta}$ бинарные операции в $\mathbb{0}$, непосредственно находим, что ПР2 имеет место в $(Q, \textcircled{\nabla}, \textcircled{\Delta})$ для всех $x,y,z \in Q$.

Теорема доказана.

Учитывая факт, что в почти-решетках (Q, ∇, Δ) имеет место

ПР3 $\quad x \Delta (y \nabla x) = x \nabla (y \Delta x)$ [1] для всех $x,y \in Q$ [2];

непосредственно находим, что имеет место следующее утверждение:

ТЕОРЕМА 7. Почти-решетка (Q, ∇, Δ) является решеткой тогда и только тогда, когда в (Q, ∇, Δ) по меньшей мере имеет место один из законов поглощения.

ЛИТЕРАТУРА

[1] Ушан Я., Об одном обобщению решеток, Review of Research Faculty of Scienece - University of Novi Sad, Vol. 17-2, 1987.

Јанез Ушан
21000 Нови Сад
Балзакова 25
Југославија

---

[1] обесселенное поглощение.
[2] утверждение 2 из [1].

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

SUBALGEBRAS AND CONGRUENCES VIA DIAGONAL RELATION

Gradimir Vojvodić, Branimir Šešelja
Institute of Mathematics
University of Novi Sad
Dr Ilije Djuričića 4, Novi Sad
Yugoslavia

ABSTRACT. Algebras whose congruence or subalgebra lattices satisfy some conditions were recently discussed by many authors. For a given algebra A we here consider both $\mathrm{Con}A$ and $\mathrm{Sub}A$ as sublattices of a lattice C_wA of weak congruences on A (i.e. of all congruences on all subalgebras of A). It turns out that the main connections (homomorphism, embedding, isomorphism) between $\mathrm{Sub}A$ and $\mathrm{Con}A$ depend mostly on the lattice properties of a diagonal relation Δ in C_wA.

We prove that Δ is a neutral element in C_wA if and only if for every subalgebra B, the congruence lattice $\mathrm{Con}B$ is isomorphic with the suitable ideal in $\mathrm{Con}A$, and the set of all such ideals is closed under intersections. Moreover, Δ is exceptional in C_wA if and only if those ideals form a sublattice of the lattice of all ideals on $\mathrm{Con}A$. Finally, for algebras having no infinite chain of subalgebras and congruences, $\mathrm{Con}A \cong \mathrm{Sub}A$ if and only if Δ is exceptional in C_wA, and the lattice of squares $(B^2,\ B \in \mathrm{Sub}A)$ is isomorphic with $\mathrm{Con}A$.

AMS Subject class.: 08A30
Key words: Congruence and subalgebra lattices

* * *

For an algebra A, $C_w A$ is its lattice of weak congruences, i.e. of all the congruences on all the subalgebras of A. The following properties of a weak congruence lattice were proved in [2] and [3].

1. $\mathrm{Con}A$ is a sublattice of $C_w A$, namely it is the filter $[\Delta)$ generated by a diagonal relation $\Delta = \{(x,x) \mid x \in A\}$.

2. $\mathrm{Sub}A$ is a retract of $C_w A$. Indeed, it is isomorphic with the ideal $(\Delta]$, under $B \to B^2 \wedge \Delta$, and moreover, the mapping $m: \rho \to \rho \wedge \Delta$ is an endomorphism on $C_w A$.

A is said to have the congruence intersection property (CIP) if for $\rho, \theta \in C_w A$

$$(\rho \wedge \theta) \vee \Delta = (\rho \vee \Delta) \wedge (\theta \vee \Delta).$$

Recall that A is said to have the congruence extension property (CEP) if every congruence on a subalgebra of A is a restriction of a congruence on A.

3. A has the CIP if and only if $n : \rho \to \rho \vee \Delta$ is a homomorphism from $C_w A$ into $\mathrm{Con}A$.

4. A has the CEP if and only if the restriction of n to $B \in \mathrm{Sub}A$ $n|_B : \rho \to \rho \vee \Delta$ is an injection from $\mathrm{Con}B$ into $\mathrm{Con}A$.

An element a of a bounded lattice L is neutral if

$m_a : x \to x \wedge a$ and $n_a : x \to x \vee a$ are homomorphisms, and

$f_a : x \to (x \wedge a, x \vee a)$ is an embedding of L into $(a] \times [a)$.

An element a of a bounded lattice L is exceptional if it is neutral, and the classes of the congruence induced by m_a have maximum elements which form a sublattice M_a of L ([1]).

5. The diagonal relation Δ of an algebra A is neutral in $C_w A$ if and only if A satisfies both the CIP and the CEP.

6. The classes of the congruence induced on $C_w A$ by the mapping m have maximum elements, collection of which $(M_\Delta = \{B^2 \mid B \in \mathrm{Sub}A\})$ is not necessarily a sublattice of $C_w A$.

* * *

Starting with the congruence intersection property, we induce two weaker conditions.

An algebra A is said to have the weak congruence intersection property (wCIP), if for $\rho, \theta \in C_w A$

$$\Delta \leq \theta \quad \text{implies} \quad \Delta \vee (\rho \wedge \theta) = (\Delta \vee \rho) \wedge \theta.$$

(Obviously, $\Delta \leq \theta$ means that $\theta \in \mathrm{Con} A$.)

A is said to have the subalgebra congruence intersection proprrty (sCIP), if for $\rho, \theta \in C_w A$

$$\rho \wedge \Delta = \theta \wedge \Delta \quad \text{implies} \quad \Delta \vee (\rho \wedge \theta) = (\Delta \vee \rho) \wedge (\Delta \vee \theta).$$

(obviously, ρ and θ are congruences on the same subalgebra of A.)

Clearly, the CIP implies both the wCIP and the sCIP.

LEMMA 1. If A satisfies the CEP and the wCIP, then A has the sCIP.

Proof. Let $\rho \wedge \Delta = \theta \wedge \Delta$, and suppose that A satisfies the wCIP and the CEP. Then

$(\rho \vee \Delta) \wedge (\theta \vee \Delta) = (\rho \wedge (\theta \vee \Delta)) \vee \Delta \leq \theta \vee \Delta$. Now, since $\rho \wedge (\theta \vee \Delta)$ and θ are congruences on the same subalgebra of A, then by the CEP and by 4.,

$$\rho \wedge (\theta \vee \Delta) \leq \theta.$$

Since

$$\rho \wedge (\theta \vee \Delta) \leq \rho,$$

it follows that

$$\rho \wedge (\theta \vee \Delta) \leq \rho \wedge \theta,$$

and thus

$$(\rho \wedge (\theta \vee \Delta)) \vee \Delta \leq (\rho \wedge \theta) \vee \Delta.$$

Since the inequality

$$(\rho \wedge \theta) \vee \Delta \leq (\rho \wedge (\theta \vee \Delta)) \vee \Delta$$

is always satisfied, the proof is complete. □

LEMMA 2. *If A has the wCIP, then the restriction $n|_B : \rho \to \rho \vee \Delta$ $(B \in \mathrm{Sub}A)$ is an onto homomorphism of $\mathrm{Con}B$ to the ideal $(B^2 \vee \Delta]$ in $\mathrm{Con}A$ (i.e. to $(B^2 \vee \Delta]_{\mathrm{Con}A}$).*

Proof. Let A has the wCIP and let $\theta \in (B^2 \vee \Delta]$, $B \in \mathrm{Sub}A$. The congruence we need is $B^2 \wedge \Delta$. Indeed, by the wCIP.

$$(B^2 \wedge \theta) \vee \Delta = (B^2 \vee \Delta) \wedge \theta = \theta, \text{ i.e.}$$

$$n|_B(B^2 \wedge \theta) = \theta. \quad \square$$

LEMMA 3. *A has the sCIP if and only if $n|_B$ is a homomorphism from $\mathrm{Con}B$ to $(B^2 \vee \Delta]_{\mathrm{Con}A}$, for every $B \in \mathrm{Sub}A$.*

Proof. Simple reformulation of the definition of the sCIP. $\square$

LEMMA 4. *A satisfies both the wCIP and the sCIP if and only if $n|_B$ is an "onto" homomorphism from $\mathrm{Con}A$ to $(B^2 \vee \Delta]_{\mathrm{Con}A}$ for every subalgebra B of A.*

Proof. The "only if" part follows from Lemmas 2 and 3.

For the "if" part, all we have to prove is that the sCIP and the fact that $n|_B$ is "onto" imply the wCIP.

Let $\rho \in \mathrm{Con}B$, $\theta \in (B^2 \vee \Delta]$. Then, since $n|_B$ is "onto", and by sCIP, $\theta = \alpha \vee \Delta$, for some $\alpha \in \mathrm{Con}B$. Hence,

$$(\rho \vee \Delta) \wedge \theta = (\rho \vee \Delta) \wedge (\alpha \vee \Delta) = (\rho \wedge \alpha) \vee \Delta \leq (\rho \wedge (\alpha \vee \Delta)) \vee \Delta =$$

$$= (\rho \wedge \theta) \vee \Delta,$$

and we are done, since the converse inequality always holds.

If $\theta \in \mathrm{Con}B$, but $\theta \notin (B^2 \vee \Delta]$, then $\theta_1 = (\Delta \vee \rho) \wedge \theta \in (B^2 \vee \Delta]$, and by the previous consideration

$$\Delta \vee (\rho \wedge \theta_1) = (\Delta \vee \rho) \wedge \theta_1 .$$

Hence,

$$\Delta \vee (\rho \wedge \theta) = \theta_1 = (\Delta \vee \rho) \wedge \theta_1 = \Delta \vee (\rho \wedge \theta_1) = \Delta \vee (\rho \wedge (\Delta \vee \rho) \wedge \theta) = \Delta \vee (\rho \wedge \theta),$$

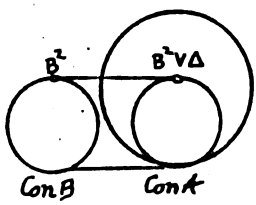
and the wCIP holds. $\square$

THEOREM 5. The following are equivalent for an algebra A:

(i) A has the CEP and the wCIP;

(ii) For $B \in \mathrm{Sub}A$, $\mathrm{Con}B \cong (B^2 \vee \Delta]_{\mathrm{Con}A}$, under $n|_B : \rho \to \rho \vee \Delta$.

($(B^2 \vee \Delta]_{\mathrm{Con}A}$ is an ideal in $\mathrm{Con}A$, as before.)



Proof. (i) ⇒ (ii):

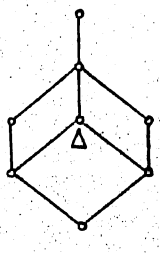
$n|_B$ is an injection by 4., and it is "onto" by Lemma 2. By Lemma 1 it is a homomorphism.

(ii) ⇒ (i):

The CEP follows by 4., and the wCIP by Lemma 4. □

EXAMPLE 1. We give here the four-element groupoid which satisfies the conditions of Theorem 5.

G	a	b	c	d
a	b	b	d	c
b	b	a	c	d
c	b	b	d	d
d	a	b	d	c



THEOREM 6. The following are equivalent for an algebra A:

(i) Δ is neutral in $C_w A$;

(ii) for all B, $C \in \mathrm{Sub}A$

a) $\mathrm{Con}B \cong (B^2 \vee \Delta]_{\mathrm{Con}A}$ under $n|_B$, and

b) $(B^2 \wedge C^2) \vee \Delta = (B^2 \vee \Delta) \wedge (C^2 \vee \Delta)$.

Proof. (i) ⇒ (ii):

a) holds by Theorem 5, and b) by 5. (in the introduction), namely by the CIP.

(ii) ⇒ (i): All we have to prove is that A satisfies the CIP.

Let $\rho \in \mathrm{Con}B$, $\theta \in \mathrm{Con}C$, $B, C \in \mathrm{Sub}A$, and put $\rho_A = \rho \vee \Delta$. Now,

$\rho_A \geq \rho_A \wedge \theta_A$ implies $\rho_A \geq (n|_B)^{-1}(\rho_A \wedge \theta_A)$,

$\theta_A \geq \rho_A \wedge \theta_A$ implies $\theta_A \geq (n|_C)^{-1}(\rho_A \wedge \theta_A)$. Hence,

$$\left.\begin{aligned} \rho &\geq (n|_B)^{-1}(\rho_A \wedge \theta_A) \geq (n|_{B\wedge C})^{-1}(\rho_A \wedge \theta_A) \\ \theta &\geq (n|_C)^{-1}(\rho_A \wedge \theta_A) \geq (n|_{B\wedge C})^{-1}(\rho_A \wedge \theta_A) \end{aligned}\right\} \quad (1)$$

We have used the fact that for $\rho \in \mathrm{Con}\mathcal{V}$, $\mathcal{V} \leq E \leq A$, $\rho_A = (\rho_E)_A$. Also, by a), inverse images exist, and by b) they belong to $\mathrm{Con}(B^2 \wedge C^2)$. Indeed

$$\rho_A \leq B_A^2 \quad \text{and} \quad \theta_A \leq C_A^2 \quad \text{imply}$$

$$\rho_A \wedge \theta_A \leq B_A^2 \wedge C_A^2 = (B^2 \wedge C^2)_A .$$

Now, 1) implies

$$\rho \wedge \theta \geq (n|_{B\wedge C})^{-1}(\rho_A \wedge \theta_A) \ , \quad \text{and hence}$$

$$(\rho\wedge\theta)_A \geq (\rho_A \wedge \theta_A)_A = \rho_A \wedge \theta_A \ ,$$

and the CIP is satisfied. □

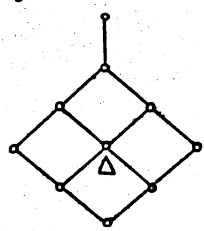
EXAMPLE 2. The following unary algebra ilustrates the situation in Theorem 6.

A	a	b	c	d
f_1	a	a	d	c
f_2	b	a	d	c

$A = (A, f_1, f_2)$

$B = \{a,b\}$

$C = \{c,d\}$



THEOREM 7. The following are equivalent for an algebra A:

(i) Δ is exceptional in $C_w A$;

(ii) For every $B \in \mathrm{Sub}A$;

a) $\mathrm{Con}B \cong (B^2 \vee \Delta]_{\mathrm{Con}A}$ and

b) $p|_{\mathrm{Sub}A} : B \to B^2 \vee \Delta$ is a homomorphism from SubA into ConA ($p : C_w A \to \mathrm{Con}A$, $p(\rho) = (\rho \wedge \Delta)^2 \vee \Delta$).

Proof. (i) ⇒ (ii):
a) follows by Theorem 6, and b) by the definition of the exceptional element, since in this case the squares form a sublattice of $C_w A$.

(ii) ⇒ (i): Δ is neutral by Theorem 6, and it is exceptional by b). □

LEMMA 8. Under the conditions of Theorem 7, $p|_{Sub A}$ is an embedding (ii), if and only if (in (i)) $B^2 \vee \Delta = C^2 \vee \Delta$ implies $B = C$ $(B, C \in Sub A)$.

Proof. Obvious. □

LEMMA 9. Let A be an algebra for which $C_w A$ has a finite length[1]. Then, under the conditions of Theorem 7, $p|_{Sub A}$ is "onto" (ii), if and only if (in (i)) the least congruence in the class $[\theta]_{\ker n}$ (for $\theta \in Con A$) is a square.

Proof. $p|_{Sub A}$ is "onto" if and only if there is at least one square B^2 in $[\theta]_{\ker n}$, for every $\theta \in Con A$ (since in that case $p|_{Sub A}(B) = B^2 \vee \Delta = \theta$). Now, if the least congruence in $[\theta]_{\ker n}$ is a square, then obviously there is a square in the class, and $p|_{Sub A}$ is "onto". Conversely, if ρ is a minimal congruence in the class $[\theta]_{\ker n}$ (which exists since $C_w A$ has a finite length), and if B^2 belongs to the same class, then $\rho \leq B^2$, and $(\rho \wedge \Delta)^2 = C^2 \leq B^2$. Thus, we have

$$\rho \wedge \Delta = C^2 \wedge \Delta, \quad \text{and} \quad \rho \vee \Delta = C^2 \vee \Delta.$$

Since by (i) in Theorem 7 A has the CEP, by 4., $\rho = C^2$, and the least congruence in the class is a square. □

---

1) I.e. all chains in this lattice are finite.

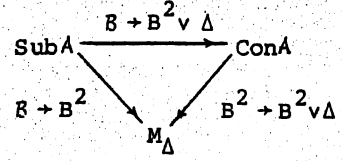
We shall characterize the algebras having isomorphic lattices of subalgebras and congruences, using, as before, a diagonal relation in the lattice of weak congruences. Recall that the set of all square $M_\Delta = \{B^2 \mid B \in \mathrm{Sub}A\}$ is a sublattice of C_wA, if Δ is an exceptional element in this lattice.

THEOREM 10. *The following are equivalent for an algebra A for which C_wA has a finite lenght:*

(i) $\begin{cases} \text{a) } \mathrm{Sub}A \cong \mathrm{Con}A \text{ under } p|_{\mathrm{Sub}A}: \mathcal{B} \to B^2 \vee \Delta \text{ ;} \\ \text{b) for every } \mathcal{B} \in \mathrm{Sub}A,\ \mathrm{Con}\mathcal{B} \cong (B^2 \vee \Delta]_{\mathrm{Con}A} \text{ under } n|_B: \rho \to \rho \vee \Delta; \end{cases}$

(ii) Δ *is an exceptional element in* C_wA *and* $M_\Delta \cong \mathrm{Con}A$ *under* $n|_{M_\Delta}: B^2 \to B^2 \vee \Delta$.

Theorem 10 can be represented by a commutative diagram:



Proof. (i) $\Rightarrow$ (ii):

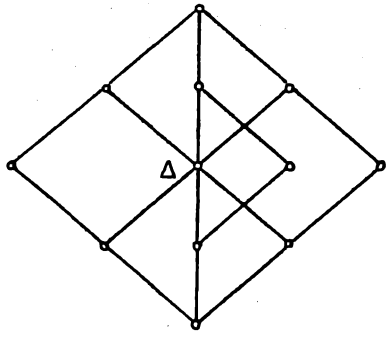
By Theorem 7, all we have to prove is that $M_\Delta = \mathrm{Con}A$. This is obvious since M_Δ is a sublattice of C_wA isomorphic with $\mathrm{Sub}A$, under $\mathcal{B} \to B^2$, and since $\mathcal{B} \to B^2 \vee \Delta$ is again an isomorphism from $\mathrm{Sub}A$ onto $\mathrm{Con}A$.

(ii) $\Rightarrow$ (i):

This part follows by Theorem 7 and by the fact that in every class $[\theta]_{\ker n}$ $(\theta \in \mathrm{Con}A)$ there is exactly one square (since $M_\Delta \cong \mathrm{Con}A$). □

EXAMPLE 3.

Any affine algebra satisfies the conditions of Theorem 10. Here we give a diagram of the weak congruence lattice for Klein's group G.



$\mathrm{Sub}G \cong M_\Delta G \cong \mathrm{Con}G$.

R E F E R E N C E S

[1] Reilly, N.R., Representation of lattices via neutral elements, Algebra Universalis, 19(1984), 341-354

[2] Vojvodić,G., Šešelja,B., On the lattice of weak congruence relations, Algebra Universalis, 25(1988), 121-130.

[3] Vojvodić,G., Šešelja,B., On CEP and CIP in the lattice of weak congruences, Proceedings of the Conference "Algebra and Logic", Cetinje, 1986, 221-227.

INSTITUTE OF MATHEMATICS
UNIVERSITY OF NOVI SAD
21000 Novi Sad, dr Ilije Đuričića 4
Yugoslavia

PROCEEDINGS OF THE CONFERECE
"ALGEBRA AND LOGIC", SARAJEVO 1987

ON SOME GENERALIZATIONS OF ORDERING RELATIONS

Mališa R. Žižović

Abstract In this paper we give some new connections of generalized ordering with binary ordering and total binary ordering.

I Main definitions

1. An (n+1)-ary relation R on S is (n+1)-reflexive iff $(a^{n+1})\in R$ for each $a\in S$. [1]

2. An (n+1)-ary relation R on S is 2-antisymmetric iff for each $a,b\in S$ the following is satisfied: If all permutations of $a,b\in S$ are included in (n+1)-tuples of R, then a=b. [1]

3. An (n+1)-ary relation R on S is iA_1-transitive, $i\in N_n$ iff for each $a_0,\dots,a_{n+1}\in S$

$$((a_0^{i-1},a_i,a_{i+1}^{n})\in R \wedge (a_1^{i-1},a_i,a_{i+1}^{n+1})\in R) \Rightarrow (a_0^{i-1},a_{i+1}^{n+1})\in R.$$ [2]

4. An (n+1)-ary relation R on S is compressible iff the following is satisfied for all $a_1,\dots,a_k\in S$:
If $(a_1^{i_1},\dots,a_k^{i_k})\in R$, $i_1+\dots+i_k=n+1$, $i_1,\dots,i_k\in N$, then
$(a_1^{j_1},\dots,a_k^{j_k})\in R$, for all $j_1,\dots,j_k\in N\cup\{0\}$, $j_1+\dots+j_k=n+1$. [1]

5. An (n+1)-ary relation R on S is weakly compressible iff the following is satisfied for all $a,b\in S$:

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

AMS Mathematics Subject Clasification (1980): 06A15.
Key words and phrases: n-ary relations.

If $(a,b)^{r\,s}\in R$, $r+s=n+1$, $r,s\in N$, then $(a,b)^{i\,j}\in R$ for all $i,j\in N\cup\{0\}$, $i+j=n+1$.

6. An $(n+1)$-ary relation R on S is 2-complete iff for all $a,b\in S$ the following is satisfied: $((\exists\, a_1,\ldots,a_{n+1}\in S)$ such that $(a_1^{n+1})\in R$ and $a_i=a$, $a_j=b$, $1\leq i<j\leq n+1)$ or $((\exists\, b_1,\ldots,b_{n+1}\in S)$ such that $(b_1^{n+1})\in R$ and $b_k=b$, $b_m=a$, $1\leq k<m\leq n+1)$.

7. An $(n+1)$-ary relation R on S is strongly 2-complete iff for all $a,b\in S$ the following is satisfied:

$(\exists\, r,s\in N,\ r+s=n+1$ such that $(a,b)^{r\,s}\in R)$ or

$(\exists\, k,m\in N,\ k+m=n+1$ such that $(a,b)^{k\,m}\in R)$.

II Some notes on generalizations of ordering relations

PROPOSITION 1. *If $(n+1)$-ary relation R on S is compressible and $i\Lambda_1$-transitive then it is $j\Lambda_1$-transitive for each $i,j\in N_n$.*

Proof: Let the $a_0,\ldots,a_{n+1}\in S$ be arbitrary elements, and let i,j, $i<j$ (for $i>j$ proof is analogous) be such that:

$$(a_o^{i-1},a_i,a_{i+1}^{j-1},a_j,a_{j+1}^{n})\in R \text{ and}$$
$$(a_1^{i-1},a_i,a_{i+1}^{j-1},a_j,a_{j+1}^{n+1})\in R.$$

From compressibility of relation R we also have

$$(a_o^{i-1},a_i,a_i,a_{i+1}^{j-1},a_{j+1}^{n})\in R \text{ and}$$
$$(a_1^{i-1},a_i,a_i,a_{i+1}^{j-1},a_{j+1}^{n+1})\in R.$$

From $i\Lambda_1$-transitivity we have

$$(a_o^{j-1},a_{j+1}^{n+1})\in R,$$

and it follows that the relation R is $j\Lambda_1$-transitive.

Remark. In Theorem 12 [1] instead of $n\Lambda_1$-transitivity $i\Lambda_1$-transitivity for some $i\in N_n$ can be required.

THEOREM 2. *Let R be an $(n+1,2,n\Lambda_1)$-RAT, weakly compressible relation on S. If $\leqslant$ is binary relation on S defined by $a\leqslant b$ iff $(a,b)^{k\,m}\in R$ for some $k,m\in N$, $k+m=n+1$ then $\leqslant$ is RAT-relation on S.*

Proof: Reflexivity and antisymmetry of relation $\leqslant$ can be proved as in Theorem 12 [1].

Relation $\leqslant$ is transitive:

Let $a\leqslant b$ and $b\leqslant c$. Then, by the definition of relation $\leqslant$ and by weak compressibility of relation R

$(a,\overset{n}{b})\in R$ and $(\overset{n}{b},c)\in R$.

It follows that $(a,\overset{n-1}{b},c)\in R$. From $(a,\overset{n-1}{b},c)\in R$ and $(a,\overset{2\ n-1}{b})\in R$ by $n\Lambda_1$-transitivity it follows that $(a,\overset{2\ n-1}{b},c)$ R,..., from $(\overset{n-1}{a},b,c)\in R$, $(a,\overset{n}{b})\in R$ it follows that $(a,c)\in R$ or $a\leqslant c$.

The next example shows that weak compressibility is not a consequence of others axioms for generalized order.

Example 1. $S=\{a,b,c,d\}$, n=2.

$R=\{\overset{3}{(x)}\mid x\in S\}\cup\{(a,b.c),(b,c,d),(a,b,d),(a,a,b),(a,a,c),(a,a,d)\}$

R is $(3,2,2\Lambda_1)$-RAT relation on S, but it is not weakly compressible, and thus it is not possible to reduce it to the binary order.

Relation R in the next example is $(3,2,2\Lambda_1)$-RAT, weakly compressible relation but it is not compressible.

Example 2. $S=\{a,b,c,d\}$, n=2.

$R=\{\overset{3}{(x)}\mid x\in S\}\cup\{(a,a,b),(a,b,b),(a,a,c),(a,c,c),(a,a,d),(a,d,d),(a,b,c),(a,b,d),(b,c,d)\}$.

It is reduced to binary order relation:

$\leqslant\ =\{(x,x)\mid x\in S\}\cup\{(a,b),(a,c),(a,d)\}$.

III Generalizations of total ordering relations

THEOREM 3. Let $\leqslant$ be a binary relation of total order on S. Then the (n+1)-ary relation R defined by:

$$(a_1^{n+1})\in R \text{ iff } a_1\leqslant a_2\leqslant\ldots\leqslant a_n\leqslant a_{n+1},$$

is (n+1)-reflexive, 2-antisymmetric, $i\Lambda_1$-transitive, compressible and 2-complete relation on S.

Proof: Total ordering of $\leqslant$ directly implies 2-completeness of R. Other properties are valid by theorem 11 [1].

The converse is also true:

THEOREM 4. Let R be an $(n+1,2,i\Lambda_1)$-RAT, compressible and 2-complete relation on S. If $\leqslant$ is binary relation on S defined by

$$a\leqslant b \text{ iff } (\overset{j}{a},\overset{k}{b})\in R \text{ for some } j,k\in N,\ j+k=n+1,$$

then $\leqslant$ is total ordering on S.

Proof: Relation $\leqslant$ is RAT-relation by theorem 12 [1]. Let $a,b\in S$, $a\neq b$. Because of 2-completeness and 2-antisymmetry of relation R, only one way in definition of 2-completeness is valid. Thus, $(\exists\, a_1,\ldots,a_{n-1}\in S)$, $(\exists\, j,k\in N)$ $1\leqslant j<k\leqslant n-1$, so that

$$(a_1^{j-1},a,a_j^{k-1},b,a_k^{n-1})\in R.$$

By compressibility of the relation R it follows that there are $r;s\in N$, $r+s=n+1$, such that $(a,b)\in R^{r\,s}$ i.e. $a\leqslant b$ and $\leqslant$ is total ordering on S.

If, instead of compressibility in Theorem 4. we take weak compressibility, then, instead of 2-completeness, we must use strong 2-completeness, and we come to the next theorem the proof of which is straightforward.

THEOREM 5. Let R be 2-antisymmetric, $n\Lambda_1$-transitive, strongly 2-complete and weakly compressible (n+1)-ary relation on S. If $\leqslant$ is binary relation on S defined by

$a\leqslant b$ iff $(a,b)\in R^{i\,j}$ for some $i,j\in N$, $i+j=n+1$,

then $\leqslant$ is total ordering on S.

Since the compressible and 2-complete (n+1)-ary relation is obviously strongly 2-complete and weakly compressible relation, it follows that Theorem 5. is extension of Theorem 4. in the way shown by the next example:

Example 3. $S=\{a,b,c\}$, $n=3$.

$R=\{(a,a,a,a),(b,b,b,b),(c,c,c,c),(a,a,a,b),(a,a,a,c),$
$(a,a,b,b),(a,a,c,c),(a,b,b,b),(a,c,c,c),(b,b,b,c),$
$(b,b,c,c),(b,c,c,c),(a,b,b,c)\}$.

R is $(4,2,3\Lambda_1)$-RAT, weakly compressible and strongly 2-complete, but it is not compressible.

Remark Compressible and 2-complete (n+1)-ary relation is (n+1)-reflexive.

Weakly compressible and strongly 2-complete (n+1)--ary relation is (n+1)-reflexive.

REFERENCES

[1] Ušan, J., Šešelja, B., On some generalizations of reflexive antisymmetric and transitive relations, Proceeding of the Simposium on n-ary Structures, Skopje 1982., 175-184.

[2] Ušan, J., Šešelja, B., Transitive n-ary relations and characterizations of generalized equivalences, Zbornik radova PMF-a u Novom Sadu, Ser. Mat. 11 (1981), 231-245.

[3] Ušan, J., Šešelja, B., On some operations on the set $I(S^{n+1})$, Prilozi MANU, Skopje, 1983., 77-84.