INSTITUTE OF MATHEMATICS
UNIVERSITY OF NOVI SAD

PROCEEDINGS OF THE CONFERENCE „ALGEBRA AND LOGIC", ZAGREB 1984

Novi Sad
1985

PROCEEDINGS OF THE CONFERENCE
"ALGEBRA AND LOGIC", ZAGREB 1984
published by
INSTITUTE OF MATHEMATICS
FACULTY OF SCIENCE
UNIVERSITY OF NOVI SAD
DR ILIJE DJURIČIĆA 4
21000 NOVI SAD, YUGOSLAVIA

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

Printed by: FTN OOUR Štamparija za grafičku delatnost
Novi Sad, Veljka Vlahovića 3
Tiraž: 4oo primeraka

P R E F A C E

The Fourth Yugoslav Algebraic Conference "Algebra and Logic" organized by the Faculty of Science, Zagreb, was held in Zagreb, June 7-9, 1984. This book contains most of the papers presented during the Conference.

The next Yugoslav Algebraic Conference is scheduled to be organized by the Faculty of Science, Sarajevo, in 1986.

Editor

CONTENTS

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", ZAGREB 1984

SOME CONGRUENCES ON GENERALIZED INVERSE SEMIGROUP

Branka P. Alimpić

Abstract. A regular semigroup S is called generalized inverse if the set E(S) of all idempotents of S forms a normal band [6]. A band B is normal if efgh = egfh, for every e,f,g,h of B. In this paper inverse and $\mathcal{L}$-unipotent congruences on S are characterized, analogous to the caracterization of congruences on inverse semigroups given by M.Petrich [4]. We mention that for $\mathcal{L}$-unipotent semigroups a similar characterization has been given by Sh.Shimokawa [5]. Finally, if ρ is a congruence on S, the smallest $\mathcal{L}$-unipotent and the smallest inverse congruence on S containing ρ are described.

Firstly we give some definitions and results. We adopt the notation and terminology of J.M.Howie [2]. If $\mathcal{C}$ is a class of semigroups, then a congruence ρ on a semigroup S is a $\mathcal{C}$-congruence if $S/\rho \in \mathcal{C}$. A regular semigroup S is $\mathcal{L}$-unipotent (inverse) if the set E(S) forms a right regular band (semilattice). A band B is right regular if ef=fef, for any e,f of B, and right normal if efg=feg, for any e,f,g of B. Obviously, a normal band is right regular if and only if it is right normal.

RESULT 1 [6]. Let S be a generalized inverse semigroup. Then

(1) xefy = xfey,

(2) xa'y = xa"y,

for every x,y,a $\in$ S, a',a" $\in$ V(a), e,f $\in$ E(S).

RESULT 2 [5]. Let S be an $\mathcal{L}$-unipotent semigroup. Then

(1) a'a = a"a,

(2) a'ea = a"ea,

(3) aa'ea = ea,

for every a $\in$ S, a',a" $\in$ V(a), e $\in$ E(S).

Let S be a generalized inverse semigroup. A congruence τ on the set E(S) is called normal if

$$e\tau f \Rightarrow (\forall s \in S)(\forall s' \in V(s))s'es\,\tau\, s'fs.$$

A regular subsemigroup K of S is called normal if it is full ($E(S) \subseteq S$) and selfconjugate ($((\forall s \in S)(\forall s' \in V(s))s'Ks \subseteq K)$.

For a congruence τ on E(S) we introduce the following relations:

(1) $e\,\tau_0\, f \overset{def}{\Longleftrightarrow} (\forall s \in S)(\forall s' \in V(s))s'es\,\tau\, s'fs$

(2) $e\,\tau_r\, f \overset{def}{\Longleftrightarrow} (\forall h \in E(S))he\,\tau\, hf.$

LEMMA 1. <u>If τ is a normal congruence on E(S), then the relations τ_0 and τ_r are normal congruences on E(S). τ_0 is the smallest semilattice congruence on E(S) containing τ, τ_r is the smallest right regular band congruence on E(S) containing τ, and $\tau_r \le \tau_0$.</u>

<u>Proof</u>. Obviously, the relations τ_0 and τ_r are equivalences. For any $g \in E(S)$ we have

$e\,\tau_0 f \Rightarrow (\forall s \in S)(\forall s' \in V(s))s'gegs\,\tau\, s'gfgs$ (Since $s'g \in V(gs)$)

$\Rightarrow (\forall s \in S)(\forall s' \in V(s))(s'ges\,\tau\, s'gfs \wedge s'egs\,\tau\, s'fgs)$ (By Result 1)

$\Rightarrow ge\,\tau_0 gf \wedge eg\,\tau_0 fg,$

$e\,\tau_r f \Rightarrow (\forall h \in E(S))(hge\,\tau\, hgf \wedge heg\,\tau\, hfg)$ (Since $hg \in E(S)$)

$\Rightarrow ge\,\tau_r gf \wedge eg\,\tau_r fg.$

Hence, τ_0 and τ_r are congruences.

Since τ is normal in S, we have $\tau \le \tau_0$, and since τ is a congruence, we have $\tau \le \tau_r$.

Let $s \in S$, $s' \in V(s)$, then we have

$e\,\tau_0 f \Leftrightarrow (\forall t \in S)(\forall t' \in V(t))t'et\,\tau\, t'ft$

$\Rightarrow (\forall t \in S)(\forall t' \in V(t))t's'est\,\tau\, t's'fst$ (Since $t's' \in V(st)$)

$\Rightarrow s'es\,\tau_0 s'fs$.

$e\,\tau_r f \Rightarrow ss'e\,\tau\, ss'f$ (Since $ss' \in E(S)$)

$\Rightarrow s'es\,\tau\, s'fs$ (Since τ is normal)

$\Rightarrow s'es\,\tau_r s'fs$ (Since $\tau \le \tau_r$).

Hence, τ_0 and τ_r are normal in S.

For τ_0 we have

$ef\,\tau_0 ef \Leftrightarrow (\forall s \in S)(\forall s' \in V(s))s'efs\,\tau\, s'efs$

$\Leftrightarrow (\forall s \in S)(\forall s' \in V(s))s'efs\,\tau\, s'fes$ (By Result 1)

$\Leftrightarrow ef\,\tau_0 fe,$

which yields that τ_o is a semilattice congruence.

Similarly, for τ_r we have

$$\begin{aligned} ef\ \tau_r\ ef &\Leftrightarrow (\forall h\in E(S))hef\,\tau\,hef \\ &\Leftrightarrow (\forall h\in E(S))hef\,\tau\,hfef \qquad \text{(By definition of S)} \\ &\Leftrightarrow ef\ \tau_r\ fef \end{aligned}$$

which yields that τ_r is a right regular band congruence.

Let σ be any semilattice congruence on E(S) containing τ. Then we obtain

$$\begin{aligned} e\ \sigma_o\ f &\Rightarrow e\ \sigma\ efe \wedge fef\,\sigma\, f \qquad \text{(For } s=s'=e, \text{ and } s=s'=f) \\ &\Rightarrow e\ \sigma\ f \qquad \text{(Since } efe\ \sigma\, fef) \end{aligned}$$

which implies $\sigma_o \leq \sigma$, and

$$\tau\leq\sigma \Rightarrow \tau_o \leq \sigma_o \Rightarrow \tau_o\leq\sigma.$$

Hence, τ_o is the smallest semilattice congruence on E(S) containing τ.

Similarly, if σ is a right regular band congruence on E(S) containing τ , we obtain

$$\begin{aligned} e\ \sigma_r f &\Rightarrow e\ \sigma\ ef \wedge fe\ \sigma\ f \qquad \text{(For } h=e \text{ and } h=f) \\ &\Rightarrow e\ \sigma\ f \qquad \text{(Since } ef\,\sigma\, fef,\ fef\,\sigma\, f) \end{aligned}$$

which implies that $\sigma_r\leq\sigma$, and $\tau_r\leq\sigma$.

Hence, τ_r is the smallest right regular band congruence on E(S) containing τ .

Finally, since every semilattice congruence is a right regular band congruence, it follows that $\tau_r\leq\tau_o$.

Now we describe $\mathcal{L}$-unipotent congruences on S.

LEMMA 2. _Let_ τ _be a normal congruence on_ E(S) _and let_ K _be a normal subsemigroup of_ S _such that_

(i) $ae\in K\wedge e\,\tau\,a'a \Rightarrow a\in K$,

(ii) $a\in K \Rightarrow a'ea\,\tau\, ea'a$

for every $a\in S$, $a'\in V(a)$ _and_ $e\in E(S)$, _then_

(1) $aeb\in K\wedge e\,\tau\, a'a \Rightarrow ab\in K$,

(2) $ab\in K \Rightarrow aeb\in K$,

(3) $ab'\in K \wedge a'a\,\tau\, b'b \Rightarrow a'ea\,\tau\, b'eb$,

(4) $ef\,\tau\, fef$ (τ _is a right regular band congruence_)

for every $a,b\in S$, $a'\in V(a)$, $b'\in V(b)$ _and_ $e,f\in E(S)$.

Proof. (1) By Result 1, $ab(b'eb)=aeb\in K$. Since τ is normal, from $e\,\tau\, a'a$ we obtain that $b'eb\,\tau\, b'a'ab$. Since $b'a'\in V(ab)$, it follows from (2) that $ab \in K$.

(2) Since K is normal, $ab \in K \Rightarrow aeb = ab(b'eb) \in K$.

(3) Assume that $ab' \in K$ and $a'a \,\tau\, b'b$. Then

$$\begin{aligned} a'ea &= a'aa'eaa'a \;\tau\; b'ba'eab'b && \text{(Since } a'a \,\tau\, b'b\text{)} \\ &\tau\; b'eba'ab'b && \text{(By (ii), since } ba' \in V(ab')\text{)} \\ &\tau\; b'eb && \text{(Since } a'a \,\tau\, b'b\text{).} \end{aligned}$$

(4) Since K is full, from (ii) we obtain that $fef \,\tau\, ef$.

DEFINITION 1. <u>Let</u> K <u>be a normal subsemigroup of</u> S, <u>and let</u> τ <u>be a normal congruence on</u> E(S). <u>The pair</u> (K,τ) <u>is an</u> $\mathcal{L}$<u>-unipotent congruence pair for</u> S <u>if</u> K <u>and</u> τ <u>satisfy the conditions</u> (i) <u>and</u> (ii) <u>of Lemma</u> 2.

DEFINITION 2. [4] . <u>Let</u> ρ <u>be a congruence on</u> S. <u>Then</u>

$$\ker\rho = \{x \in S \mid (\exists\, e \in E(S))\ x \,\rho\, e\}$$
$$\operatorname{tr}\rho = \rho|_{E(S)}.$$

LEMMA 3. <u>Let</u> ρ <u>be an</u> $\mathcal{L}$<u>-unipotent congruence on</u> S. <u>Then, for</u> $a,b \in S$,

$$a \,\rho\, b \Leftrightarrow (\forall a' \in V(a))(\forall b' \in V(b))(a'a \operatorname{tr}\rho\, b'b \wedge ab' \in \ker\rho\,).$$

<u>Proof</u>. Let $a\rho b$, $a' \in V(a)$, $b' \in V(b)$. Then

$$\begin{aligned} a'a \;\rho\; a'bb'b && \text{(Since } a\rho b \text{ and } b=bb'b\text{)} \\ \rho\; a'ab'b && \text{(Since } b\rho a\text{)} \\ \rho\; b'ba'ab'b && \text{(Since } \rho \text{ is } \mathcal{L}\text{-unipotent)} \\ \rho\; b'ab'b && \text{(Since } b \,\rho\, a \text{ and } aa'a=a\text{)} \\ \rho\; b'b && \text{(Since } a\rho b\text{),} \end{aligned}$$

so $a'a \operatorname{tr}\rho\, b'b$. From $ab' \,\rho\, bb'$ it follows that $ab' \in \ker\rho$.

Conversely, let $a'a \operatorname{tr}\rho\, b'b$ and $ab' \in \ker\rho$ for some $a' \in V(a)$ and $b' \in V(b)$. Then

$$\begin{aligned} a \;\rho\; ab'bb'b && \text{(Since } a'a \,\rho\, b'b\text{)} \\ \rho\; bb'ab'b && \text{(Since } \rho \text{ is } \mathcal{L}\text{-unipotent)} \\ \rho\; bb'bb'ab'b && \text{(Since } bb' \in E(S)\text{)} \\ \rho\; ba'ab'ab'b && \text{(Since } b'b \,\rho\, a'a\text{)} \\ \rho\; ba'ab'b && \text{(Since } ab' \in \ker\rho\text{)} \\ \rho\; b && \text{(Since } a'a \,\rho\, b'b\text{).} \end{aligned}$$

THEOREM 1. <u>Let</u> (K,τ) <u>be an</u> $\mathcal{L}$<u>-unipotent congruence pair for a generalized inverse semigroup</u> S, <u>and let</u> $\rho(K,\tau)$ <u>be a relation on</u> S <u>defined by</u>

$$(*)\quad a \,\rho(K,\tau)\, b \overset{\text{def}}{\Longleftrightarrow} (\exists\, a' \in V(a))(\exists\, b' \in V(b))(a'a \,\tau\, b'b \wedge ab' \in K)$$

<u>Then</u> $\rho(K,\tau)$ <u>is the unique</u> $\mathcal{L}$<u>-unipotent congruence on</u> S <u>for</u>

which $\ker \rho(K,\tau)=K$ and $\operatorname{tr} \rho(K,\tau)=\tau$.

Conversely, if ρ is an $\mathcal{L}$-unipotent congruence on S, then $(\ker\rho, \operatorname{tr}\rho)$ is an $\mathcal{L}$-unipotent congruence pair for S and $\rho=\rho(\ker\rho, \operatorname{tr}\rho)$.

Remark 1. By Results 1 and 2 we have
$a\rho(K,\tau)b \Leftrightarrow (\forall a'\in V(a))(\forall b'\in V(b))(a'a\,\tau\, b'b \wedge ab'\in K)$.

Proof. Since K is normal, the relation $\rho(K,\tau)$ is reflexive and symmetric, and by Remark 1 it is transitive.

Let $a\rho(K,\tau)b$, and $c\in S$, $c'\in V(c)$. Then $a'a\,\tau\, b'b$ and $ab'\in K$ for some $a'\in V(a)$ and $b'\in V(b)$. Since τ is normal, we have $a'a\,\tau\, b'b \Rightarrow c'a'ac\,\tau\, c'b'bc$, and by (2) of Lemma 2 we have $ab'\in K \Rightarrow acc'b'\in K$. Since $c'a'\in V(ac)$ and $c'b'\in V(bc)$, if follows that $ac\rho(K,\tau)bc$.

Further, from $ab'\in K$ and $a'a\,\tau\, b'b$ we have $a'(c'c)a\,\tau\, b'(c'c)b$ by (3) of Lemma 2 and $ab'\in K \Rightarrow cab'c'\in K$, since K is self-conjugate. From $a'c'\in V(ca)$ and $b'c'\in V(cb)$ it follows that $ca\ \rho(K,\tau)cb$.
Therefore $\rho(K,\tau)$ is a congruence on S.
If $a\in \ker\rho(K,\tau)$, then $a'a\,\tau\, e$ and $ae\in K$ for some $a'\in V(a)$ and some $e\in E(S)$, which by (i) of Lemma 2 yields $a\in K$. Conversely, if $a\in K$, then $a(a'a)\in K$, $a'a\,\tau\, a'aa'a$, for any $a'\in V(a)$, hence $a\,\rho(K,\tau)a'a$. Consequently, $K=\ker\rho(K,\tau)$, and obviously $\operatorname{tr}\rho(K,\tau)=\tau$.

The uniqueness of $\rho(K,\tau)$ follows from Lemma 3. Observe that it follows also from [1], Theorem 5.1.

Conversely, let ρ be an $\mathcal{L}$-unipotent congruence on S. Then $\operatorname{tr}\rho=\rho|_{E(S)}$ is a normal congruence on E(S), and by orthodoxy of S $\ker\rho$ is a full and selfconjugate subsemigroup of S. Let $a\in\ker\rho$, $a'\in V(a)$. Then $a^2\rho\, a$, and $a'=a'aa'\,\rho\,(a'a)(aa')\in E(S)$, so $a'\in\ker\rho$, and $\ker\rho$ is a regular subsemigroup. Hence, it is a normal subsemigroup of S.

From $ae\in\ker\rho$ and $a'a\,\rho\, e$ it follows $a=aa'a\,\rho\, ae\in\ker\rho$, so (i) of Lemma 2 holds.

Let $a\in\ker\rho$, $a'\in V(a)$, then $a\rho f$ and $a'\rho g$ for some $f,g\in E(S)$, and so $a'ea\,\rho\, gef\,\rho\, egf\,\rho\, ea'a$, since ρ is $\mathcal{L}$-unipotent on S, and the condition (ii) of Lemma 2 holds.

Hence, $(\ker\rho, \operatorname{tr}\rho)$ is an $\mathcal{L}$-unipotent congruence pair for S. By the first part of this theorem, $\rho=\rho(\ker\rho, \operatorname{tr}\rho)$. The theorem is proved.

THEOREM 2. *If ρ is a congruence on a generalized inverse semigroup S, then $(\ker\rho, (\operatorname{tr}\rho)_r)$ is an $\mathcal{L}$-unipotent congruence pair for S, and $\rho(\ker\rho, (\operatorname{tr}\rho)_r)$ is the smallest $\mathcal{L}$-unipotent congruence on S containing ρ.*

Proof. Let ρ be a congruence on S. By Theorem 1 $\ker\rho$ is a normal subsemigroup of S, and by Lemma 1 $(\operatorname{tr}\rho)_r$ is a normal congruence on E(S), and it is the smallest right regular band congruence on E(S) containing $\operatorname{tr}\rho$.

Let $ae \in \ker\rho$ and $a'a(\operatorname{tr}\rho)_r e$. Then $a'ae\,\rho\, a'a$ (for $h=a'a$), so $a=aa'a\,\rho\, aa'ae = ae \in \ker\rho$.

If $a \in \ker\rho$ and $a' \in V(a)$, then $a\rho f$ and $a'\rho g$ for some $f,g \in E(S)$, and by Lemma 1, we have

$a'ea \operatorname{tr}\rho\, gef(\operatorname{tr}\rho)_r\, egf \operatorname{tr}\rho\, ea'a.$

Hence, $(\ker\rho, (\operatorname{tr}\rho)_r)$ is an $\mathcal{L}$-unipotent congruence pair. Since $\operatorname{tr}\rho \subseteq (\operatorname{tr}\rho)_r$, it follows that $\rho \subseteq \rho(\ker\rho, (\operatorname{tr}\rho)_r)$.

Let σ be an $\mathcal{L}$-unipotent congruence on S containing ρ. Then $\ker\rho \subseteq \ker\sigma$, and by Lemma 1 $(\operatorname{tr}\rho)_r \subseteq \operatorname{tr}\sigma$, so $\rho(\ker\rho, (\operatorname{tr}\rho)_r) \subseteq \rho(\ker\sigma, \operatorname{tr}\sigma) = \sigma$.

Hence $\rho(\ker\rho, (\operatorname{tr}\rho)_r)$ is the smallest $\mathcal{L}$-unipotent congruence on S containing ρ. The theorem is proved.

It is possible to establish analogous results for inverse congruence on S. Firstly we have the following statement.

LEMMA 4. *Let τ be a congruence on E(S) and let K be a normal subsemigroup of S such that*

(ii)' $a \in K \Rightarrow a'a\,\tau\, aa'$, *for every* $a \in S$, $a' \in V(a)$.

Then τ is a semilattice congruence on E(S), and

(ii) $a \in K \Rightarrow a'ea\,\tau\, ea'a$, *for every* $a \in S, a' \in V(a)$, $e \in E(S)$.

Proof. Since K is full, and $ef \in V(fe)$, from (ii)' we obtain $efe = ef\cdot fe\,\tau\, fe\cdot ef = fef$, and so $fe\,\tau\, fef\,\tau\, ef$.

If $a \in K$, then $a'e \in K$, so by (ii)' we have

$a'ea = a'e\; ea\,\tau\, eaa'e\,\tau\, eaa'\,\tau\, ea'a.$

DEFINITION 3. *Let K be a normal subsemigroup of S, and τ a normal congruence on E(S). We say that (K, τ) is an inverse congruence pair for S if the conditions (i) of Lemma 2 and (ii)' of Lemma 4 are satisfied.*

Now we can formulate theorems which are analogous to Theorems 1 and 2.

THEOREM 3. *Let* (K,τ) *be an inverse congruence pair for a generalized inverse semigroup* S, *and let* $\rho(K,\tau)$ *be a relation on* S *defined by* (*). *Then* $\rho(K,\tau)$ *is the unique inverse congruence on* S *for which* $\ker\rho(K,\tau)=K$, $\mathrm{tr}\,\rho(K,\tau)=\tau$.

Conversely, if ρ *is an inverse congruence on* S, *then* $(\ker\rho, \mathrm{tr}\,\rho)$ *is an inverse congruence pair for* S *and* $\rho=\rho(\ker\rho,\mathrm{tr}\,\rho)$.

Remark 3. This theorem is a special case of Theorem 1 [3].

THEOREM 4. *If* ρ *is a congruence on a generalized inverse semigroup* S, *then* $(\ker\rho,(\mathrm{tr}\rho)_0)$ *is an inverse congruence pair for* S *and* $\rho(\ker\rho,(\mathrm{tr}\rho)_0)$ *is the smallest inverse congruence on* S *containing* ρ.

From Theorems 2 and 4 we have the following consequence.

COROLLARY 1. *If* ε *is the equality relation on* E(S), *then* $\rho(E(S),\varepsilon_r)$ *is the smallest* $\mathcal{L}$*-unipotent congruence on* S, *and* $\rho(E(S),\varepsilon_0)$ *is the smallest inverse congruence on* S.

REFERENCES

1 C.Eberhart, W.Williams, *Congruences on an orthodox semigroup via the minimum inverse semigroup congruence*, Glasgow Math.J. 18(1977), 181-192.

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

3 D.N.Krgović, *Inverse congruences on orthodox semigroups*, this volume.

4 M.Petrich, *Congruences on inverse semigroups*, J. of Algebra, 55(1978), 231-256.

5 Sh.Shimokawa, *Congruences on* $\mathcal{L}$*-unipotent semigroups*, Proceedings of the 6th Symposium on Semigroups, Kyoto, 1982 (39-51).

6 M.Yamada, *Regular semigroups whose idempotents satisfy permutation identities*, Pac.J.Math. 21(1976) 371-392.

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

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", ZAGREB 1984

SEMIGROUPS OF GALBIATI-VERONESI

Stojan Bogdanović

ABSTRACT. In this paper we consider semigroups which are semilattices of nil-extensions of rectangular groups. Also, we consider semigroups which are chains of nil-extensions of completely simple semigroups.

1. INTRODUCTION AND PRELIMINARIES

In [6] J.L.Galbiati and M.L.Veronesi studied π-regular semigroups in which every regular element is completely regular (semigruppi fortemente regolari). These semigroups are completely described by M.L. Veronesi in [19]. Semigroups which are semilattices of nil-extensions of rectangular groups are considered in the special case by M.S.Putcha, [15]. In this paper we consider the general case.

Throughout this paper, Z^+ will denote the set of all positive integers.

A semigroup S is <u>π-regular</u> if for every $a \in S$ there exists $m \in Z^+$ such that $a^m \in a^m S a^m$. A semigroup S is <u>completely π-regular</u> if for every $a \in S$ there exist $x \in S$ and $m \in Z^+$ such that $a^m = a^m x a^m$ and $a^m x = x a^m$. S is called a <u>semigroup of Galbiati-Veronesi</u> (GV-<u>semigroup</u>) if S is π-regular and every regular element of S is completely regular, [6]. We will say that a semigroup S is <u>π-inverse</u> if S is π-regular and every regular element of S possesses a unique inverse, [5]. S is GV-<u>inverse</u> if S is GV-semigroup and every regular element of S possesses a unique inverse, [6]. S is a <u>strongly π-inverse semigroup</u> if S is π-regular and idempotent elements commute, [2]. A semigroup S with zero 0 is a *nil-semigroup* if for every $a \in S$ there exists $n \in Z^+$ such that $a^n = 0$. By *nil-extension* we mean an ideal extension by a nil-semigroup. If $S = B \times G$, where B is a rectangular band and G is a group, then S is a *rectangular group*; S is a *right group* if B is a right zero semigroup. A semigroup S is *archimedean* (*left archimedean*, *right archimedean*) if for every $a,b \in S$ there exists $n \in Z^+$ such that $a^n \in SbS$ ($a^n \in Sb$; $a^n \in bS$). A semigroup S is t-*archimedean* if it is both left and right archimedean. A semigroup S is *left* (*right*) *weakly commutative* if for every $a,b \in S$ there exists $n \in Z^+$ such that $(ab)^n \in bS$ ($(ab)^n \in Sa$), [18]. A semigroup S is *weakly commutative* if for every $a,b \in S$ there exists $n \in Z^+$ such that $(ab)^n \in bSa$, [10] (see also [12]). A subsemigroup N of a semigroup S is *filter* of S, if for all $x,y \in S$, $xy \in N$ implies $x,y \in N$. For any $x \in S$, $N(x)$ denotes the intersection of all filters containing x. Then $N(x)$ is the least filter containing x. Let S be a semigroup and $a,b \in S$. Following [15] we introduce the following notations:

$a \mid b \Leftrightarrow b \in S^1aS^1$

$a \mid_r b \Leftrightarrow b \in aS^1$

$a \mid_\ell b \Leftrightarrow b \in S^1a$

$a \mid_t b \Leftrightarrow a \mid_r b$ and $a \mid_\ell b$.

By $E(S)$ we denote the set of all idempotents of a semigroup S.

For undefinied notions and notations we refer to [12].

The following proposition is a generalization of results of [1, 5, 10, 12, 14].

PROPOSITION 1.1. *The following conditions are equivalent on a semigroup* S :

(i) S *is left weakly commutative*;

(ii) S *is a semilattice of right archimedean semigroup*;

(iii) $(\forall a,b \in S)\ a \mid b \Rightarrow (\exists i \in Z^+)(\ a \mid_r b^i\ )$;

(iv) $N(x) = \{ y \in S : (\exists n \in Z^+)\ x^n \in yS \}$, *for every* $x \in S$.

Proof. (ii)$\Leftrightarrow$(iii). This is Theorem 3.(1) [16].

(i)$\Rightarrow$(iii). Let S be a left weakly commutative semigroup. Assume that $a \mid b$, i.e. there exist $x,y \in S^1$ such that $b = xay$.

Then there exist $u \in S$ and $i \in Z^{+}$ such that $b^{i} = (xay)^{i} = (ay)u$. Hence, $a \mid_r b^{i}$.

$(ii) \Longrightarrow (i)$. Let S be a semilattice Y of right archimedean semigroups S_{α} $(\alpha \in Y)$. Then for $a \in S_{\alpha}$, $b \in S_{\beta}$ we have that $ab, ba \in S_{\alpha\beta}$ and so $(ab)^{n} = bax$ for some $x \in S$ and $n \in Z^{+}$. Hence, S is left weakly commutative.

$(i) \Longrightarrow (iv)$. For $x \in S$, let

$$T = \{ y \in S : (\exists n \in Z^{+})\ x^{n} \in yS \} .$$

Let $y,z \in T$, then $x^{m} = ya$, $x^{m} = zb$ for some $a,b \in S$ and $m \in Z^{+}$. Fromthis it follows that

$$(1) \qquad yx^{m} = y^{2}a = yzb .$$

Since S is a semilattice Y of right archimedean semigroups S_{α} $(\alpha \in Y)$ (since $(i) \Longleftrightarrow (ii)$) we have

$$x^{m} = ya \in S_{\beta} S_{\gamma} \subseteq S_{\beta\gamma} = S_{\alpha} \text{ and } y^{2}a \in S_{\beta} S_{\gamma} \subseteq S_{\beta\gamma} = S_{\alpha} .$$

So by (1) we have $x, yzb \in S_{\alpha}$. Since S_{α} is a right archimedean semigroup we have that there exist $k \in Z^{+}$ and $u \in S$ such that

$$x^{k} = yzbu \in yzS .$$

Hence, $yz \in T$. Assume now that $yz \in T$. Then there exist $u \in S$ and $r \in Z^{+}$ such that $x^{r} = yzu \in yS$, so $y \in T$. From $x^{r} = yzu$, by left weak commutativity,we have $x^{rk} = (yzu)^{k} = zuv \in zS$ for some $k \in Z^{+}$ and $v \in S$ and thus $z \in T$. Therefore, T is a filter of S.

Let $y \in T$, then $x^{m} = ya \in N(x)$ and so $y \in N(x)$. Hence, $T \subseteq N(x)$ and by minimality of $N(x)$ we have that $T = N(x)$.

$(iv) \Longrightarrow (i)$. Let $x,y \in S$, then $yx \in N(xy)$, so

$$(xy)^{n} = yxS \subseteq yS$$

for some $n \in Z^{+}$. Hence, S is left weakly commutative.□

COROLLARY 1.1. <u>The following conditions are equivalent on a semigroup</u> S :

(i) S <u>is weakly commutative</u>;

(ii) S <u>is a semilattice of t-archimedean semigroups</u>;

(iii) $(\forall a,b \in S)(\ a \mid b \Longrightarrow (\exists i \in Z^{+})\ a \mid_t b^{i}\ )$;

(iv) $N(x) = \{ y \in S : (\exists n \in Z^{+})\ x^{n} \in ySy \}$, <u>for every</u> $x \in S$.□

REMARK. $(i) \Longleftrightarrow (iv)$.This is Theorem 6.5. [11]. $(ii) \Longleftrightarrow (iii)$. This is Theorem 3.3. [16]. $(i) \Longleftrightarrow (ii)$. This is Theorem 1. [1] ,also Proposition 4.2. [5].

2. SEMIGROUPS OF GALBIATI-VERONESI

In our investigations the following result is fundamental (see [19], Theorem 13.1.).

THEOREM (Veronesi). S is a semilattice of nil-extensions of completely simple semigroups if and only if S is a GV-semigroup. □
This theorem will be referred to as "Veronesi's theorem".

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

(i) S is a semilattice of nil-extensions of rectangular groups;

(ii) S is a GV-semigroup and for every $e,f \in E(S)$ there exists $n \in Z^+$ such that

$$(ef)^n = (ef)^{n+1} \quad ; \tag{2}$$

(iii) S is π-regular and $a = axa$ implies $a = ax^2a^2$.

Proof. (i)$\Rightarrow$(ii). Let S be a semilattice Y of nil-extensions of rectangular groups S_α $(\alpha \in Y)$. Then by Veronesi's theorem S is a semigroup of Galbiati-Veronesi. Assume that $e \in S_\alpha$ and $f \in S_\beta$ are idempotents, then $ef, fe \in S_{\alpha\beta}$, so $(ef)^n, (fe)^n \in K_{\alpha\beta}$ for some $n \in Z^+$, where $K_{\alpha\beta}$ is a rectangular group which is the kernel of $S_{\alpha\beta}$. Now, there exist $g,h \in E(S) \cap K_{\alpha\beta}$ such that $(ef)^n \in G_g$, $(fe)^n \in G_h$, where G_g, G_h are subgroups of $K_{\alpha\beta}$. Since $E(S) \cap K_{\alpha\beta}$ is a rectangular band we have $g = ghg$. Furthermore,

$$(ef)^n = (ef)^n g \quad , \quad (fe)^n = (fe)^n h$$

and there exist $x \in G_g$ and $y \in G_h$ such that

$$(ef)^n x = g \quad , \quad (fe)^n y = h \ .$$

From this we have that

$$\begin{aligned}(ef)^n &= (ef)^n g = (ef)^n (ef)^n x = (ef)^n e (ef)^n x = (efe)^n (ef)^n x = (efe)^n y \\ &= e(fe)^n g = e(fe)^n hg = (efe)^n ((fe)^n y) g = (efe)^n ef (fe)^n yg \\ &= (ef)^{n+1} (fe)^n yg = (ef)^{n+1} hg = (ef)(ef)^n g \cdot hg = (ef)^{n+1} g \\ &= (ef)^{n+1} \ .\end{aligned}$$

Hence, for every $e,f \in E(S)$ there exists $n \in Z^+$ such that (2) holds.

(ii)$\Rightarrow$(i). Let S be a semigroup of Galbiati-Veronesi with (2). Then

$$(efe)^n = (ef)^n e = (ef)^{n+1} e = (efe)^{n+1} \ . \tag{3}$$

Hence, $(efe)^n$ is an idempotent. Since S is a semilattice Y of nil-extensions of completely simple semigroups S_α $(\alpha \in Y)$ (Theorem Veronesi) for $e,f \in E(S) \cap S_\alpha$ we have that $e,f \in K_\alpha$, where K_α is the completely simple kernel of S_α . It is clear that $(efe)^n$ is an idempotent in K_α , so

$$(efe)^n = e(efe)^n e$$

and therefore e and $(efe)^n$ are in the same subgroup $H_{i\lambda}$ of K_α. Hence,

(4) $$e = (efe)^n .$$

Now by (3) we have

$$e(fe) = (efe)^n(fe) = (ef)^{n+1}e = (efe)^{n+1} = (efe)^n .$$

From this and (4) it follows that $e = efe$. Hence, K_α is a rectangular group, i.e. S_α is a ni-extension of a rectangular group.

(i) $\Longrightarrow$ (iii). Let S be a semilattice Y of nil-extensions of rectangular groups S_α $(\alpha \in Y)$. Let $a = axa$. Then $ax, xa \in S_\alpha$, so $ax = ax(xa)ax$, since $E(S_\alpha)$ is a rectangular band. Hence,

$$a = ax\cdot a = (ax\cdot xa)axa = ax^2a^2 .$$

(iii) $\Longrightarrow$ (i). Let (iii) holds. Then S is a GV-semigroup, so by Veronesi's theorem we have that S is a semilattice Y of nil-extensions of completely simple semigroups S_α $(\alpha \in Y)$. Since S_α $(\alpha \in Y)$ is a nil-extension of a completely simple semigroup K_α and $a = axa$ implies $a = ax^2a^2$ we have by Proposition IV.3.7. [12] that K_α is a rectangular group. Hence, S is a semilattice of nil-extensions of rectangular groups. □

COROLLARY 2.1. _The following conditions are equivalent on a semigroup_ S :

(i) S _is a_ GV-_semigroup and_ $E(S)$ _is a subsemigroup of_ S ;

(ii) S _is_ π-_regular_, $a = axa$ _implies_ $a = ax^2a^2$ _and_ RegS _is a subsemigroup of_ S ;

(iii) S _is a semilattice of nil-extensions of rectangular groups and_ $E(S)$ _is a subsemigroup of_ S .

Proof. (i) $\Longleftrightarrow$ (iii). This equivalence follows immediately by Theorem 2.1.

(i) $\Longrightarrow$ (ii). Since $E(S)$ is a subsemigroup of S we have by Proposition IV.3.1. [12] that $a,b \in$ RegS implies $ab \in$ RegS .

(ii) $\Longrightarrow$ (i). It is clear that S is a GV-semigroup. Let for $a \in$ RegS be $a = axa$. Then $a = a(xax)a$ and $xax \in$ RegS . Hence, RegS is a regular semigroup. Now by the hypothesis and by Proposition IV.3.7. [12] we have that $E(S)$ is a subsemigroup of S . □

COROLLARY 2.2. S _is a nil-extension of a rectangular group if and only if_ S _is an archimedean_ GV-_semigroup and_ $E(S)$ _is a subsemigroup of_ S . □

THEOREM 2.2. *The following conditions are equivalent on a semigroup* S :

(i) S *is a semilattice of nil-extensions of right groups;*

(ii) S *is* π*-regular and left weakly commutative;*

(iii) S *is a GV-semigroup and for every* $e,f \in E(S)$ *there exists* $n \in Z^+$ *such that* $(ef)^n = (fef)^n$;

(iv) S *is* π*-regular and* $a = axa$ *implies* $ax = xa^2x$.

Proof. (i)$\Leftrightarrow$(ii). This equivalence follows by Proposition 1.1. and by Lemma 3.1. [15] .

(i)$\Rightarrow$(iii). Let $e \in S_\alpha$, $f \in S_\beta$ be idempotents. Then $ef, fef \in S_{\alpha\beta}$, so by Theorem 2.1. we have that $(ef)^n = (ef)^{n+1}$ for some $n \in Z^+$ and $(fef)^n$ are idempotents in $S_{\alpha\beta}$, so

$$(ef)^n(fef)^n = (fef)^n$$

i.e.

$$(ef)^n = (fef)^n$$

(iii)$\Rightarrow$(i). By Theorem 2.1. we have that S is a semilattice Y of nil-extensions of completely simple semigroups S_α $(\alpha \in Y)$. hence, for every $\alpha \in Y$, S_α has the kernel $K_\alpha = \mathrm{Reg}S_\alpha = \mathcal{M}(G_\alpha;I_\alpha,J_\alpha;P_\alpha)$. Now we have that

$$L_j = \{(a;i,j) : i \in I_\alpha , a \in G_\alpha\} , j \in J_\alpha$$

is a left group. Thus for any two idempotents e,f from L_j we have $ef = e$ and since

$$e = e^n = (ef)^n = (fef)^n = f(ef)^n = fe$$

for some $n \in Z^+$ we have that $e = ef = fe$, so $e = f$, since idempotents in K_α are primitive. Hence, $|I_\alpha| = 1$. Thus K_α is a right group. Therefore S is a semilattice of nil-extensions of right groups.

(i)$\Rightarrow$(iv). For $a = axa$ we have that $ax, xa \in S_\alpha$, so $xa = (ax)(xa) = ax^2a$ since $E(S_\alpha)$ is aright zero band.

(iv)$\Rightarrow$(i). If $a = axa$, then

$$a = (ax)a = xa^2x \cdot a = xa \cdot axa = xaa = xa^2$$

so

$$a = ax \cdot a = ax \cdot xa^2 = ax^2a^2$$

which by Theorem 2.1. implies that S is a semilattice of nil-extensions of rectangular groups S_α $(\alpha \in Y)$. Since in the kernel K_α of S_α $(\alpha \in Y)$ the following implication holds: $a = axa \Rightarrow ax = xa^2x$, we have by the dual of Theorem IV.3.10. [12] that K_α is a right group, so S_α $(\alpha \in Y)$ is a nil-extension of a right group.□

COROLLARY 2.3. *S is a semilattice of nil-extensions of right groups and E(S) is a subsemigroup of S if and only if S is a GV-semigroup and ef = fef for every* $e,f \in E(S)$. □

COROLLARY 2.4. *The following conditions are equivalent on a semigroup S :*

(i) *S is a GV-semigroup and for every* $e,f \in E(S)$, $ef=fe$;

(ii) *S is a semilattice of nil-extensions of groups and* $ef=fe$ *for every* $e,f \in E(S)$;

(iii) *S is* π*-regular and RegS is a Cliffordian subsemigroup of S .*

Proof. (i) $\Rightarrow$ (ii). Follows immediately by Corollary 2.3.

(ii) $\Leftrightarrow$ (iii). This is one part of Theorem 2.3. [7].

(iii) $\Rightarrow$ (i). By Theorem 2.3. [7]. □

3. π-INVERSE SEMIGROUPS

THEOREM 3.1. *The following conditions are equivalent on a semigroup S :*

(i) *S is* π*-inverse;*

(ii) *S is* π*-regular and for every* $e,f \in E(S)$ *there exists* $n \in Z^+$ *such that* $(ef)^n = (fe)^n$;

(iii) *S is* π*-regular and*

(5) $$a = axa = aya \Rightarrow xax = yay \ ;$$

(iv) *For every* $a \in S$ *there exists* $m \in Z^+$ *such that* S^1a^m *and* a^mS^1 *contain a unique idempotent generator.*

Proof. (i) $\Leftrightarrow$ (ii). This is Theorem 4.6. [5].

(i) $\Leftrightarrow$ (iv). By Theorem 4.1. [2].

(i) $\Rightarrow$ (iii). Let S be π-inverse. Then S is π-regular. Let $a = axa = aya$. Then $a = a(xax)a$, $xax = (xax)a(xax)$, $a = a(yay)a$, $yay = (yay)a(yay)$ and therefore $xax = yay$.

(iii) $\Rightarrow$ (i). Let S be π-regular with (5) . Assume that $a = axa$, $x = xax$, $a = aya$, $y = yay$. Then by (5) we have that

$$x = xax = yay = y \ .$$

Hence, S is π-inverse. □

THEOREM 3.2. *The following conditions are equivalent on a semigroup S :*

(i) *S is GV-inverse;*

(ii) *S is* π*-regular and* $a = axa$ *implies* $ax = xa$;

(iii) *S is a semilattice of nil-extensions of groups;*

(iv) S is a GV-semigroup and for every $e,f \in E(S)$ there exists $n \in Z^+$ such that $(ef)^n = (fe)^n$;

(v) S is π-regular and weakly commutative.

Proof. (i) $\Rightarrow$ (ii) Let S be GV-inverse and $a = axa$. Element a is in a subgroup G of S and so it has an inverse $y \in G$ such that $ay = ya$. Since xax is also an inverse of a we have that $y = xax$, since S is π-inverse.Hence, $a(xax) = (xax)a$, i.e. $ax = xa$.

(ii) $\Rightarrow$ (i). Let S be π-regular and $a = axa$ implies $ax = xa$. Then S is a GV-semigroup.Assume that $a = axa = aya$, $x = xax$, $y = yay$. Then $ax = xa$, $ay = ya$. Now we have that

$$x = xax = x^2a = x^2aya = xaxya = xya$$

so $ax = axay = ay$. Therefore,

$$x = xax = xay = yay = y .$$

Hence, S is GV-inverse.

(iii) $\Rightarrow$ (iv). Let S be a semilattice Y of nil-extensions of groups S_α $(\alpha \in Y)$. Then S is a GV-semigroup.Assume two idempotents $e \in S_\alpha$ and $f \in S_\beta$, then $ef, fe \in S_{\alpha\beta}$ and there exists $n \in Z^+$ such that $(ef)^n$ and $(fe)^n$ are idempotents in $S_{\alpha\beta}$ and thus $(ef)^n = (fe)^n$.

(iv) $\Rightarrow$ (iii). Let S be a GV-semigroup and for every $e,f \in E(S)$ there exists $n \in Z^+$ such that $(ef)^n = (fe)^n$. Then S is a semilattice Y of nil-extensions of completely simple semigroups S_α (Theorem Veronesi).Assume $e,f \in E(S) \cap S_\alpha$. Then e and f are in the completely simple kernel K_α of S_α . Now we have that $e, efe \in G_e$ and $f, fef \in G_f$, where G_e and G_f are maximal subgroups of K_α . Thus

$$(ef)^n e = (fe)^n e \quad , \quad f(ef)^n = f(fe)^n$$

so

$$(efe)^n = (fe)^n = (fef)^n$$

i.e. $G_e \cap G_f \neq \emptyset$, so $e = f$. Hence, S_α has only one idempotent and it is a nil-extension of a group.

(i) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (v). This is Theorem 2.2. [5] .□

THEOREM 3.3. The following conditions are equivalent on a semigroup S:

(i) S is strongly π-inverse;

(ii) S is π-regular and RegS is inverse subsemigroup of S ;

(iii) S is π-inverse and the product of any two idempotents of S is an idempotent.

Proof. (i)$\Leftrightarrow$(iii). This is Theorem 4.2. [2].

(i)$\Rightarrow$(ii). Let S be strongly π-inverse. Then for $a,b \in RegS$ we have $a = axa$, $b = byb$, so

$$ab = (axa)(aya) = a(xa)(by)b = a(by)(xa)b = ab(yx)ab .$$

Hence, $RegS$ is a subsemigroup of S and it is regular (since if $a = axa$, then $a = a(xax)a$, $xax \in RegS$). $RegS$ is an inverse semigroup since $ef = fe$ for every $e,f \in E(S)$.

(ii)$\Rightarrow$(i). This implication follows immediately.□

4. UNION OF NIL-SEMIGROUPS

LEMMA 4.1. [3]. *S is a nil-semigroup if and only if for every $a,b \in S$ there exists $r \in Z^+$ such that $a^r = b^{r+1}$.*□

LEMMA 4.2. *S is a union of nil-semigroups if and only if for every $a \in S$ there exists $r \in Z^+$ such that $a^r = a^{r+1}$.*

Proof. Let S be a union Y of nil-semigroups S_α ($\alpha \in Y$). Then $a \in S$ is in a S_α and since S_α is a nil-semigrou we have by Lemma 4.1. that there exists $r \in Z^+$ such that $a^r = a^{r+1}$.

The converse follows immediately.□

LEMMA 4.3. *The following conditions are equivalent on a semigroup* S:

(i) *S is a nil-extension of a right zero band;*

(ii) *S is a union of nil-semigroups and $E(S)$ is a right zero band;*

(iii) $(\forall a,b \in S)(\exists m \in Z^+)(a^m = ba^m)$;

(iv) *S is a right archimedean union of nil-semigroups.*

Proof. (i)$\Leftrightarrow$(iii). This is Corollary 7. [4].

(ii)$\Rightarrow$(i). Follows by Theorem 3. [4].

(i)$\Rightarrow$(ii). Follows immediately.

(iv)$\Rightarrow$(ii). For $e,f \in E(S)$ there exist $x,y \in S$ such that $e = fx$, $f = ey$, so $ef = e(ey) = ey = f$. Hence, $E(S)$ is a right zero band.

(iii)$\Rightarrow$(iv). Follows immediately.□

THEOREM 4.1. *S is a semilattice of nil-extensions of right zero bands if and only if S is a union of nil-semigroups and S is left weakly commutative.*

Proof. Let S be a semilattice Y of nil-extensions of right zero bands S_α ($\alpha \in Y$). Then by Lemma 4.2. and Theorem 2.2. we have that S is left weakly commutative.

Conversely, let S be a left weakly commutative union of nil-semigroups. Then by Theorem 2.2. we have that S is a semilattice Y of nil-extensions of right groups S_α $(\alpha \in Y)$. Since S_α is a nil-extension of right group and S_α is union of nil-semigroups we have by Lemma 4.3. that S_α is a nil-extension of right zero band. □

Theorem 4.1. is a generalization of arezult from [9].

5. CHAIN OF NIL-EXTENSIONS OF COMPLETELY SIMPLE SEMIGROUPS

THEOREM 5.1. S _is a chain of nil-extensions of completely simple semigroups if and only if_ S _is a GV-semigroup and for any_ $e,f \in E(S)$ _either_ $e \in efS$ _or_ $f \in feS$.

Proof. Let S be a chain Y of nil-extensions of completely simple semigroups S_α $(\alpha \in Y)$. Assume $e,f \in E(S)$, then $e \in S_\alpha$, $f \in S_\beta$. Suppose that $\alpha \leq \beta$ (ordering of the semilattice Y); the case $\beta < \alpha$ is treted analogously. Then $efe \in S_\alpha$, and we have $e \in H_{i\lambda}$, $(efe)^n \in H_{j\mu}$ for some $n \in Z^+$, where $H_{i\lambda}$, $H_{j\mu}$ are maximal subgroups of the kernel K_α of S_α. Complete simplicity of K_α yields

$$(efe)^n = e(efe)^n e \in H_{i\lambda} H_{j\mu} H_{i\lambda} \subseteq H_{i\lambda} .$$

Letting u be the inverse of $(efe)^n$ in $H_{i\lambda}$, we obtain

$$e = (efe)^n u \in efS .$$

Conversely, by Veronesi's theorem it suffices to show that Y is linearly ordered. For any classes S_α and S_β $(\alpha, \beta \in Y)$, let $e \in S_\alpha$, $f \in S_\beta$ be idempotents. Then $e \in efS$ implies $\alpha \leq \beta$ and $f \in feS$ implies $\beta \leq \alpha$. □

THEOREM 5.2. S _is a chain of nil-extensions of rectangular groups if and only if_ S _is a GV-semigroup and for every_ $e,f \in E(S)$ _there exists_ $n \in Z^+$ _such that_ $e = (efe)^n$ _or_ $f = (fef)^n$.

Proof. Let S be a chain Y of nil-extensions of rectangular groups S_α $(\alpha \in Y)$. Then by Theorem 2.1. for $e \in S_\alpha$, $f \in S_\beta$ there exists $n \in Z^+$ such that $(ef)^n = (ef)^{n+1}$. From this it follows that $(ef)^n e = (ef)^{n+1} e$, i.e. $(efe)^n = (efe)^{n+1}$. Hence, $(efe)^n$ is an idempotent. Suppose that $\alpha \leq \beta$. Then $(efe)^n \in S_\alpha$, so

$$(efe)^n = e(efe)^n e = e$$

(since $E(S_\alpha)$ is a rectangular band).

The converse follows immediately. □

The following theorems follows easily from the results already proved.

THEOREM 5.3. S _is a chain of nil-extensions of right groups if and only if_ S _is a_ GV-_semigroup and for every_ $e,f \in E(S)$ _there exists_ $n \in Z^+$ _such that_ $(ef)^n = f$ _or_ $(fe)^n = e$. □

THEOREM 5.4. S _is a chain of nil-extensions of groups if and only if_ S _is a_ GV-_semigroup and_ E(S) _is a chain_. □

R E F E R E N C E S

[1] Bogdanović,S.:O slabo komutativnoj polugrupi,Mat.Vesnik,5(18)(33),1981, 145-148.

[2] Bogdanović,S.:Power regular semigroups,Zbornik radova PMF Novi Sad 12(1982),418-428.

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

[4] Bogdanović,S. and S.Milić:A nil-extension of a completely simple semigroup,Publ.Inst.Math.(to appear).

[5] Galbiati,J.L. e M.L.Veronesi:Sui semigruppi che sono un band di t-semigruppi,Istituto Lombardo(Rend.Sc.)114(1980),217-234.

[6] Galbiati,J.L. e M.L.Veronesi:Sui semigruppi quasi regolari,Istituto Lombardo (Rend.Sc.)116(1982).

[7] Galbiati,J.L. e M.L.Veronesi:Sui semigruppi quasi completamente inversi (private communication).

[8] Galbiati,J.L. and M.L.Veronesi:On quasi completely regular semigroups, Semigroup Forum (to appear).

[9] Miller,D.W.:Some aspects of Green's relations on periodic semigroups, Czech.Math.J.33(108),1983,537-544.

[10] Petrich,M.:The maximal semilattice decomposition of a semigroup,Math. Zeitsch.85(1964),68-82.

[11] Petrich,M.:Semigroups certain of whose subsemigroups have identities, Czech.Math.J.16(1966),186-198.

[12] Petrich,M.:Introduction to semigroups,Merill Publ.Comp.Ohio 1973.

[13] Petrich,M.:Structure of regular semigroups,Cahiers Math.Montpellier, 11(1977).

[14] Pondělíček,B.:On weakly commutative semigroups,Czech.Math.J.25(100), 1975,20-23.

[15] Putcha,M.S.:Semilattice decomposition of semigroups,Semigroup Forum 6(1973),12-34.

[16] Putcha,M.S.:Rings which are semilattices of archimedean semigroups, Semigroup Forum 23(1981),1-5.

[17] Raju,K.V. and J.Hanumanthachari:On weakly commutative semigroups, Math.Seminar Notes,10(1982),753-765.

[18] Sedlock,J.T.:Green's relations on a periodic semigroup,Czech.Math.J. 19(94),1969,318-323.

[19] Veronesi,M.L.:Sui semigruppi quasi fortemente regolari,Rivisita di Matematica dell'Universita di Parma (to appear).

26000 Pančevo
M.Pijade 114.
Yugoslavia

PROCEEDINGS OF THE CONFERENCE „ALGEBRA AND LOGIC", ZAGREB 1984

A NOTE ON INVARIANT n-SUBGROUPS OF n-GROUPS

Naum Celakoski, Snežana Ilić

Invariant n-subgroups of n-groups are considered here, and the so called "indirect method" for proving theorems on polyadic groups is used.

0. PRELIMINARIES

Invariant n-subgroups of n-groups are considered in Rusakov [3], [4] and some properties are investigated there by "direct technics" (which are used in most papers on n-groups). An "indirect method" which uses binary groups for proving theorems on polyadic groups is proposed in Čupona, Celakoski [2].

We use this method here to give an analogy of the well known result of the binary case that all normal subgroups of a group are exhausted by the kernels of homomorphisms, giving firstly some characterizations of normal n-subgroups of an n-group by the universal covering group.

We will use some definitions and notations as in [1] - [4].

An algebra $\underline{Q} = (Q, [\ ])$ with the carrier Q and an n-ary associative operation on Q, $[\ ] : (x_1, \dots, x_n) \mapsto [x_1 \dots x_n]$ (n being fixed) is called an n-__semigroup__. $\underline{Q}$ is called an n-__group__ if, in addition, all the equations $[a_1 \dots a_{n-1} x] = b$, $[y a_1 \dots a_{n-1}] = b$ on x and y are solvable in $\underline{Q}$. The semigroup $\underline{Q}^{\wedge} = (Q^{\wedge}, \cdot)$ generated by the set Q with the set of defining relations: $a = a_1 \dots a_n$ for every equality $a = [a_1 \dots a_n]$ in $\underline{Q}$, i.e.

$$\underline{Q}^{\wedge} = \langle Q;\ \{a = a_1 \dots a_n \mid a = [a_1 \dots a_n] \text{ in } Q\} \rangle$$

is called the __universal covering semigroup of__ $\underline{Q}$. The set

$Q^\wedge = \bigcup_1^\infty Q^m$, where $Q^m = \{a_1 \dots a_m \mid a_\nu \in Q\}$ can be written in the form ([1; p.25], [2; p.136]):

$$Q^\wedge = Q \cup Q^2 \cup \dots \cup Q^{n-1}, \quad \text{where} \quad Q^i \cap Q^j = \emptyset \quad \text{if} \quad i \neq j.$$

An n-semigroup $\underline{Q}$ can be considered as an n-subsemigroup of its universal covering semigroup $\underline{Q}^\wedge$. If $\underline{Q}$ is an n-group, then $Q^\wedge$ is a group and vice versa.

1. INVARIANT n-SUBGROUPS AND THE UNIVERSAL COVERING GROUP

Let $\underline{Q}$ be an n-group. An n-subgroup $\underline{H}$ of $\underline{Q}$[1] is said to be *invariant* (or *normal*) *in* $\underline{Q}$ iff

$$(\forall x \in Q)(\forall i \in \{2,\dots,n\}) \quad [xH^{n-1}] = [H^{i-1}xH^{n-i}]. \tag{1.1}$$

This is equivalent to the statement ([4; p.104])

$$(\forall x_1,\dots,x_{n-1} \in Q)(\forall i \in \{2,\dots,n-1\})[x_1^{n-1}H] = [x_1^{i-1}Hx_i^{n-1}]. \tag{1.2}$$

(Here, for example, $[H^{i-1}xH^{n-i}]$ is the set $\{[h_1^{i-1}xh_i^{n-1}] \mid h_\nu \in H\}$, where h_k^m stands for $h_k h_{k+1} \dots h_m$ if $k \leq m$, or for the empty symbol if $k > m$.)

The following Lemma gives a characterization of invariant n-subgroups in terms of the universal covering group.

1.1. LEMMA. *An n-subgroup $\underline{H}$ of an n-group $\underline{Q}$ is invariant in $\underline{Q}$ iff*

$$(\forall x \in Q) \quad xH = Hx \quad \textit{in} \quad Q^\wedge.$$

Proof. If $\underline{H}$ is invariant in $\underline{Q}$ and $x \in Q$, then by (1.2) $[x^{n-1}H] = [x^{n-2}Hx]$, which becomes $x^{n-1}H = x^{n-2}Hx$ in $\underline{Q}^\wedge$ and thus (by cancelling x^{n-2} in the group $\underline{Q}^\wedge$) $xH = Hx$.

Conversely, let $xH = Hx$ in $\underline{Q}^\wedge$ for every $x \in Q$. Then

$$[xH^{n-1}] = xH^{n-1} = HxH^{n-2} = \dots = H^{i-1}xH^{n-i} = [H^{i-1}xH^{n-i}]$$

for every $i \in \{2,\dots,n\}$. Thus, $\underline{H}$ is invariant in $\underline{Q}$. □

If $\underline{H}$ is an n-subgroup of an n-group $\underline{Q}$, then $\underline{H}^\wedge$ is a subgroup of $\underline{Q}^\wedge$ ([1; 3.2, 3.9]) and $H^\wedge = H \cup H^2 \cup \dots \cup H^{n-1}$. Therefore, by using Lemma 1.1, we have the following

---

[1] *Throughout the paper $\underline{Q}$ will denote an n-group and $\underline{H}$ an n-subgroup of $\underline{Q}$.*

1.2. THEOREM. *An n-subgroup H of an n-group Q is invariant in Q iff the subgroup $H^\wedge$ is invariant in $Q^\wedge$.*

Proof. Let H be invariant in Q. Then, for every $x \in Q$, $xH = Hx$ in $Q^\wedge$ and

$$xH^\wedge = x(H \cup H^2 \cup \ldots \cup H^{n-1}) = xH \cup xH^2 \cup \ldots \cup xH^{n-1} =$$
$$= Hx \cup H^2x \cup \ldots \cup H^{n-1}x = (H \cup H^2 \cup \ldots \cup H^{n-1})x = H^\wedge x.$$

If $a \in Q^\wedge$, i.e. $a = a_1 \ldots a_i$, $a_\nu \in Q$, then

$$aH^\wedge = a_1 \ldots a_i (H \cup H^2 \cup \ldots \cup H^{n-1}) = a_1 \ldots a_{i-1}(a_i H \cup \ldots \cup a_i H^{n-1}) =$$
$$= a_1 \ldots a_{i-1}(Ha_i \cup \ldots \cup H^{n-1}a_i) = a_1 \ldots a_{i-1}(H \cup \ldots \cup H^{n-1})a_i =$$
$$= \ldots = (H \cup \ldots \cup H^{n-1})a_1 \ldots a_i = H^\wedge a.$$

Thus, $H^\wedge$ is invariant in $Q^\wedge$.

Conversely, let $H^\wedge$ be invariant in $Q^\wedge$. Then $(\forall x \in Q)\ xH^\wedge = H^\wedge x$, i.e.

$$xH \cup xH^2 \cup \ldots \cup xH^{n-1} = Hx \cup H^2x \cup \ldots \cup H^{n-1}x;$$

this is equivalent to the following sequence of equalities in $Q^\wedge$:

$$xH = Hx, \quad xH^2 = H^2x, \ldots, xH^{n-1} = H^{n-1}x;$$

by Lemma 1.1, H is invariant in Q. ∎

An n-group Q is called a *Dedekind n-group* ([3; p.89]) iff every n-subgroup of Q is invariant in Q.

1.3. PROPOSITION. *If Q is an n-group and $Q^\wedge$ is a Dedekind group, then Q is a Dedekind n-group.*

Proof. Let H be any n-subgroup of Q. Since $Q^\wedge$ is a Dedekind group, it follows that $H^\wedge$ is invariant in $Q^\wedge$ and by Th. 1.2, H is invariant in Q. Thus Q is a Dedekind n-group. ∎

The question for the converse of Prop. 1.3:

P.1. Is $Q^\wedge$ a Dedekind group when Q is a Dedekind n-group?

remains here without an answer.

The set of all elements x of Q such that

$$[xH^{n-1}] = [H^{i-1}xH^{n-i}] \quad \text{all} \quad i \in \{2, \ldots, n\} \qquad (1.3)$$

is called the *normalizer* of the n-subgroup H in the n-group Q ([3; p.111]) and it is denoted by $N_Q(H)$ or shortly $N(H)$.

Clearly, $N(H) \neq \emptyset$ since $H \subseteq N(H)$. If $x_1, \ldots, x_n \in N(H)$, then

$$[x_1 \ldots x_n]H = x_1 \ldots x_n H = x_1 \ldots x_{n-1} H x_n = \ldots = H x_1 \ldots x_n = H[x_1 \ldots x_n]$$

in $Q^\wedge$, by which follows that $[x_1 \ldots x_n] \in N(H)$. It is easy to verify that any equation $[a_1 \ldots a_{n-1}x] = a_n$ on x and $[ya_1 \ldots a_{n-1}] = a_n$ on y in $N(H)$ is solvable in $N(H)$ and thus $\underline{N}(H)$ is an n-subgroup of $\underline{Q}$. By the definition of $N(H)$, $\underline{H}$ is invariant in $\underline{N}(H)$ and there is no element $x \in Q \setminus N(H)$ which satisfies the condition (1.3). Thus:

1.4. PROPOSITION. *The normalizer* $\underline{N}(H)$ *of an* n-*subgroup* $\underline{H}$ *of* $\underline{Q}$ *is the largest* n-*subgroup of* $\underline{Q}$ *such that* $\underline{H}$ *is invariant in* $\underline{N}(H)$. ∎

We note that the universal covering group $(N(H))^\wedge$ of $\underline{N}(H)$ is contained in

$$N(H^\wedge) = \{x_1 \ldots x_i \in Q^\wedge \mid x_1 \ldots x_i H^\wedge = H^\wedge x_1 \ldots x_i\},$$

i.e.

$$(N(H))^\wedge \subseteq N(H^\wedge). \qquad (1.4)$$

Namely, if $x_1 \ldots x_i \in (N(H))^\wedge$, where $x_\nu \in N(H)$, then by 1.4 and 1.1

$$\begin{aligned} x_1 \ldots x_i H^\wedge &= x_1 \ldots x_i (H \cup H^2 \cup \ldots \cup H^{n-1}) = x_1 \ldots x_{i-1}(x_i H \cup \ldots \cup x_i H^{n-1}) = \\ &= x_1 \ldots x_{i-1}(H x_i \cup \ldots \cup H^{n-1} x_i) = \ldots = \\ &= H x_1 \ldots x_i \cup \ldots \cup H^{n-1} x_1 \ldots x_i = \\ &= (H \cup \ldots \cup H^{n-1}) x_1 \ldots x_i = H^\wedge x_1 \ldots x_i, \end{aligned}$$

that is $x_1 \ldots x_i \in N(H^\wedge)$. Thus (1.5).

P.2. Does (or under what conditions) equality hold in (1.4)?

The indirect method can be used in obtaining shorter proofs of other results as well as of the following three:

1) If $\underline{H}$ and $\underline{K}$ are n-subgroups of an n-group $\underline{Q}$ such that $M = H \cap K \neq \emptyset$, and $\underline{H}$ is invariant in $\underline{Q}$, then $\underline{M}$ is invariant in $\underline{K}$ [4; p.107] and $M^\wedge = H^\wedge \cap K^\wedge$.

2) If $\underline{X}$ and $\underline{H}$ are invariant n-subgroups of an n-group $\underline{Q}$ such that $[XH^{n-1}] = [H^{n-1}X]$, then the n-subgroup $B = [XH^{n-1}]$ is invariant in $\underline{Q}$ ([4; p.107]) and $B^\wedge = X^\wedge H^\wedge$.

3) The center of $\underline{Q}$, i.e. the set

$$Z(Q) = \{z\in Q \mid (\forall x\in Q)\ [xz^{n-1}] = [z^{i-1}xz^{n-i}],\ i=2,\dots,n\}$$

is a commutative invariant n-subgroup of Q if it is not empty; in that case $(Z(Q))^{\wedge} = Z(Q^{\wedge})$.

(We note that the condition of "non-emptiness" above is omited in [4; p.106], which is a mistake. For example, Z(Q) of the 3-group $Q = \{\sigma \mid \sigma$ is an odd permutation of $\{1,2,3\}\}$ with $[xyz] = x\circ y\circ z$, is empty and thus it is not an n-subgroup of Q.)

2. HOMOMORPHISMS AND INVARIANT n-SUBGROUPS

The notion of homomorphisms of n-groups one defines in a usual way. The well known properties of the surjective homomorphisms (i.e. epimorphisms) of groups that the homomorphic image of a normal subgroup is a normal subgroup one proves easily for the n-ary case directly or indirectly. But the fact that an n-group might have more than one identities or no identity element at all brings the situation that the notion of a kernel of such a homomorphism one can not translate in a usual way.

Therefore we will consider the case when $\phi: Q \to Q'$ is a surjective homomorphism of n-groups, where Q' is an n-group with at least one identity. In this case, for every identity $e'\in Q'$ there exists a kernel

$$\mathrm{Ker}_{e'}\phi = \{x\in Q \mid \phi(x) = e'\}. \qquad (2.1)$$

An analogous relation between the invariant n-subgroups of an n-group and kernels of homomorphisms (of n-groups) can be stated as in the binary case. We note that every homomorphism $\phi: Q \to Q'$ of n-groups induces a homomorphism $\phi^{\wedge}: Q^{\wedge} \to Q'^{\wedge}$ between their universal covering groups, defined by ([1; p.26])

$$\phi^{\wedge}(x_1\dots x_i) = \phi(x_1)\dots\phi(x_i),\quad 1\le i\le n-1,\quad x_\nu\in Q. \qquad (2.2)$$

If ϕ is an epimorphism (monomorphism) of n-groups, then $\phi^{\wedge}$ is an epimorphism (a monomorphism) too ([1; 2.2,2.3]). We will prove first the following

2.1. TEHOREM. *If $\phi: Q \to Q'$ is an epimorphism of n-groups and H' is an invariant n-subgroup of Q', then the complete inverse image of H',*

$$H = \phi^{-1}(H') = \{h\in Q \mid \phi(h)\in H'\}$$

is an invariant n-subgroup of Q.

Proof. Clearly, $H=\phi^{-1}(H')$ is an n-subgroup of $\underline{Q}$ (as a complete inverse image of the n-subgroup $\underline{H}'$ of $\underline{Q}'$).

Since $\underline{H}'$ is invariant n-subgroup of $\underline{Q}'$, it follows by Th. 1.2 that the group $\underline{H}'^{\wedge}$ is invariant in $\underline{Q}'^{\wedge}$; thus $H^{\wedge} = \phi^{\wedge -1}(H'^{\wedge})$ is invariant in $\underline{Q}^{\wedge}$ which again by Th. 1.2 implies that $\underline{H}$ is invariant in $\underline{Q}$. ∎

Now we consider the epimorphisms and invariant n-subgroups of an n-group.

Let $\phi : Q \to Q'$ be an epimorphism from an n-group $\underline{Q}$ onto an n-group $\underline{Q}'$ with at least one identity e' and let

$$\mathrm{Ker}_{e'}\phi = \{a \in Q \mid \phi(a) = e'\} = K.$$

Clearly, K is an n-subgroup of $\underline{Q}$. Since $\{e'\}$ is an invariant n-subgroup of $\underline{Q}'$, it follows by Th. 2.1 that $K = \phi^{-1}(\{e'\})$ is an invariant n-subgroup of $\underline{Q}$.

Now let $\underline{H}$ be an invariant n-subgroup of an n-group $\underline{Q}$. Define an n-ary operation / / on the set

$$Q/H = \{\left[xH^{n-1}\right] \mid x \in Q\}$$

by

$$/[x_1H^{n-1}]\ldots\left[x_nH^{n-1}\right]/ = \left[[x_1\ldots x_n]H^{n-1}\right]. \qquad (2.3)$$

Then $\underline{Q}/H = (Q/H;/\ /)$ is an n-group (called the factor group of $\underline{Q}$ by $\underline{H}$) with an identity H. The n-subgroup $\{H\}$ of $\underline{Q}$ is the kernel of the natural homomorphism $\phi : Q \to Q/H$, $\phi(x) = [xH^{n-1}]$, since $H = \phi^{-1}\{H\}$.

So, we have the following theorem:

2.2. THEOREM. An n-subgroup $\underline{H}$ of an n-group $\underline{Q}$ is invariant in $\underline{Q}$ iff $\underline{H}$ is a kernel of a surjective homomorphism $\phi : Q \to Q'$, where $\underline{Q}'$ is an n-group with at least one identity element. ∎

Invariant n-subgroups of an n-group can be characterized also as kernels of homomorphisms of the n-group into (binary) groups. Namely, if $\underline{Q}$ is an n-group and $\underline{G}$ a group, then a mapping $\phi : Q \to G$ is a homomorphism iff

$$(\forall x_1,\ldots,x_n)\ \phi([x_1\ldots x_n]) = \phi(x_1)\ldots\phi(x_n). \qquad (2.4)$$

Suppose that $\underline{Q}' = (Q', [\ ])$ is an n-group with an identity e' and $\phi: Q \to Q'$ a surjective homomorphism. Putting

$$(\forall x', y' \in Q') \quad x' \cdot y' = [x' y' e'^{n-2}] \tag{2.5}$$

we obtain a group $(Q', \cdot)$ with the identity e'. Moreover, if $x_1, \ldots, x_n \in Q$ and $x'_\nu = \phi(x_\nu)$, then

$$\phi([x_1 \ldots x_n]) = x'_1 \cdot \ldots \cdot x'_n$$

and thus ϕ is a homomorphism of the n-group $(Q, [\ ])$ onto the group $(Q', \cdot)$. Also $\mathrm{Ker}_{e'}\phi = \{x \in Q \mid \phi(x) = e'\}$ is an invariant n-subgroup in $\underline{Q}$. Therefore the following property is true:

2.3. THEOREM. *An n-subgroup H of an n-group Q is invariant in Q iff H is a kernel of a homomorphism from Q onto a (binary) group.* ∎

R E F E R E N C E S

[1] Čupona G., Celakoski N., *On representation of n-associatives into semigroups*, Maced. Acad. Sc. Arts, Contributions VI-2 (1974), 23-34

[2] Čupona G., Celakoski N., *Polyadic subsemigroups of semigroups*, Algebraic conference Skopje 1980, 131-152

[3] Русаков С.А., *Подгрупповое строение дедекиндовых n-арных групп*, Труды Гомель. сем., Минск 1978, 81-104

[4] Русаков С.А., *К теории нильпотентных n-арных групп*, Труды Гомель. сем., Минск 1978, 104-130.

Matematički fakultet, 91000 Skopje,

Filozofski fakultet, 18000 Niš

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC“, ZAGREB 1984

ON A CLASS OF VECTOR VALUED GROUPS

Ǵorǵi Čupona, Dončo Dimovski

Abstract. Vector valued groups are defined in [1], and some existence conditions of a kind of finite vector valued groups are given in [2]. Here we consider (2m,m)-groups and show that there is an analogy between the theory of (2m,m)-groups and the theory of binary groups.

0. In [1], (m + k,m)-groups are defined. Let $m \geqslant 1$ and $G \neq \emptyset$. $(G,[\;])$ is a (2m,m)-group iff:

i) $[\;]:(x_1^{2m}) \longmapsto [x_1^{2m}]$ is an associative map from G^{2m} into G^m, i.e. $[x_1^i[x_{i+1}^{2m+i}]x_{2m+i+1}^{3m}] = [[x_1^{2m}]x_{2m+1}^{3m}]$ for each $i \in \{1,2,\dots,m\}$;

and

ii) $(\forall \underline{a},\underline{b} \in G^m)(\exists\, \underline{x},\underline{y} \in G^m)\ [\underline{a}\ \underline{x}] = \underline{b} = [\underline{y}\ \underline{a}]$.

In i), (x_1^{2m}) stands for $(x_1,x_2,\dots,x_{2m})$ and $[x_1^{2m}]$ stands for $[x_1x_2\dots x_{2m}]$.

If we define a binary operation "$\circ$" on G^m by

(1) $$\underline{x} \circ \underline{y} = [\underline{x}\ \underline{y}]$$

then i) and ii) imply that $(G^m,\circ)$ is a group.

It is clear that a (2,1)-group is the same as a group, so, usually we assume that $m \geqslant 2$.

1. Let $\underline{e} = (e_1^m)$ be the identity element in a given $(2m,m)$-group $(G,[\ ])$ i.e. in $(G^m,\circ)$. Then the equalities

$$(e_2^m,e_1)\circ(e_2^m,e_1) = (e_2^m,e_1)^2 = [e_2^m\ e_1\ e_2^m\ e_1]$$
$$= [[e_2^m\ e_1^m\ e_1]e_1^m] = [e_2^m[e_1^m\ e_1\ e_1^{m-1}]e_m]$$
$$= [e_2^m\ e_1\ e_1^m] = (e_2^m,e_1)$$

imply that $(e_2^m,e_1) = (e_1^m)$, i.e. $e_2 = e_1 = e_m = e_{m-1} = \dots = e_3 = e$. Hence, the components of $\underline{e}$ are equal, i.e.

$$\underline{e} = (\underbrace{e,\dots,e}_{m}) = (e^m).$$

Moreover, $[x_1^{i-1}\ e^m\ x_i^m] = [[x_1^{i-1}\ e^m\ x_i^m]e^m]$

$$= [x_1^{i-1}[e^m\ x_i^m\ e^{m-i}]e^i] = [x_1^{i-1}\ x_i^m\ e^m] = (x_1^m),$$

i.e. for each $i \in \{1,2,\dots,m\}$, $[x_1^{i-1}\ e^m\ x_i^m] = (x_1^m)$.

For each $i \in \{1,2,\dots,m\}$ we define $\varphi_i : G^m \longrightarrow G^m$ by $\varphi_i(x_1^m) = [e^{m-i}\ x_1^m\ e^i]$. Then

$(\varphi_i)^m(x_1^m) = [e^{m(m-1)}\ x_1^m\ e^{mi}] = (e^m)^{m-1}\circ(x_1^m)\circ(e^m)^i = (x_1^m)$.

So, $(\varphi_i)^m = \mathrm{id}$ (identity), and hence φ_i is a permutation on G^m whose order is a divisor of m.

If for some $i \in \{1,2,\dots,m-1\}$ $\varphi_i = \mathrm{id}$, then for each $x \in G$, $(x^{m-i},e^i) = [e^m\ x^{m-i}\ e^i] = [e^{m-i}\ e^i\ x^{m-i}\ e^i]$ $= \varphi_i(e^i,x^{m-i}) = (e^i,x^{m-i})$, and so $x = e$. Thus for each $i \in \{1,2,\dots,m-1\}$ $\varphi_i \neq \mathrm{id}$ provided $|G| \neq 1$, i.e. G has more than one element.

2. Let $(G,\cdot)$ be a group. It is easy to check that $(G,[\ ])$ with $[\ ]: G^{2m} \longrightarrow G^m$ defined by (2) is a $(2m,m)$-group.

(2) $$[x_1^m\ y_1^m] = (x_1y_1, x_2y_2, \dots, x_my_m)$$

Moreover, in this case, $(G^m,\circ)$ is the product

$$\underbrace{(G,\cdot)\times(G,\cdot)\times\ldots\times(G,\cdot)}_{m}\ .$$

We call such (2m,m)-groups <u>trivial</u> (2m,m)-<u>groups</u> .

If $(G,[\ ])$ is a trivial (2m,m)-group, then for each $i\in\{1,\ldots,m-1\}$ $\varphi_i(x_1^m)=[e^{m-i}\ x_1^m\ e^i]$

$$=(e^{m-i},x_1^i)\circ(x_{i+1}^m,e^i)=(x_{i+1}^m,x_1^i)\ .$$

For example, if $m=4$, the order of φ_2 is 2 and the order of φ_3 is 4. In general, the order of φ_i is $m/g.c.d.(m,i)$.

3. If $(G,[\ ])$ is a (2m,m)-group and if we set

(3) $$[x_1^{2m}]=([x_1^{2m}]_1,[x_1^{2m}]_2,\ldots,[x_1^{2m}]_m),$$

then we get an algebra $(G;[\ ]_1,\ldots,[\ ]_m)$ with m 2m-ary operations. This algebra satisfies the following conditions:

(i) For each $p\in\{1,2,\ldots,m\}$ and each $(x_1^{3m})\in G^{3m}$

$$[x_1^p[x_{p+1}^{2m+p}]_1\ldots[x_{p+1}^{2m+p}]_m\ x_{2m+p+1}^{3m}]_i$$
$$=[[x_1^{2m}]_1\ldots[x_1^{2m}]_m\ x_{2m+1}^{3m}]_i\quad ;\ \text{and}$$

(ii) $(\forall \underline{a},\underline{b}=(b_1^m)\in G^m)(\exists\, \underline{x},\underline{y}\in G^m)(\forall i\in\{1,\ldots,m\})$

$$[\underline{a}\ \underline{x}]_i=b_i=[\underline{y}\ \underline{a}]_i\ .$$

And conversselly, if an algebra $(G;[\ ]_1,\ldots,[\ ]_m)$ with m 2m-ary operations satisfies the conditions (i) and (ii), then $(G,[\ ])$ is a (2m,m)-group with $[\ ]$ defined by (3).

In the case of a trivial (2m,m)-group $(G,[\ ])$, $[x_1^{2m}]_i=x_ix_{m+i}$, i.e. all of the operations $[\ ]_i$ are essentially binary and are gotten from the operation of the group $(G,\cdot)$.

PROPOSITION 1. <u>Let</u> $(G,[\ ])$ <u>be a</u> (2m,m)-<u>group</u>, <u>such that for</u> $i\in\{1,..,m\}$ $[x_1^{2m}]_i=x_i*_i x_{m+i}$, <u>where</u>

$*_i : G^2 \longrightarrow G$ <u>is a binary operation</u>. <u>Then</u> $(G,[\ ])$ <u>is a trivial</u> $(2m,m)$-<u>group</u>.

<u>Proof</u>. It is easy to show that for each $i \in \{1,..,m\}$ $(G,*_i)$ is a group with identity element e. Next, $[x_1[x_2^{2m+1}]x_{2m+2}^{3m}] = [[x_1^{2m}]x_{2m+1}^{3m}]$ implies that for each $i \in \{1,\ldots,m-1\}$

$$(x_{i+1} *_i x_{m+i+1}) *_{i+1} x_{2m+i+1}$$
$$= (x_{i+1} *_{i+1} x_{m+i+1}) *_{i+1} x_{2m+i+1} .$$

Using this and the fact that $(G, *_i)$ is a group for each $i \in \{1,\ldots,m\}$ it follows that $*_1 = *_2 = \ldots = *_{m-1} = *_m$. Hence, $(G,[\ ])$ is a trivial $(2m,m)$-group. ∎

REMARK. Since $[x_1^m\ e^m] = (x_1^m) = [e^m\ x_1^m]$, it follows that in every $(2m,m)$-group, $[x_1^{2m}]_i$ depends on x_i and x_{m+i}, for each $i \in \{1,\ldots,m\}$.

Suppose that $(G,[\ ])$ is a trivial $(2m,m)$-group. Then $(G,[\ ])$ satisfies the following conditions for each $i \in \{1,\ldots,m\}$:

(a) $[e^{i-1}\ x\ e^{m-1}\ y\ e^{m-i}]_j = e$ for $j \neq i$; and

(b) $[e^{m-i}\ x_1^m\ e^i] = (x_{i+1}^m, x_1^i)$.

PROPOSITION 2. <u>If</u> $(G,[\ ])$ <u>is a</u> $(2m,m)$-<u>group satisfying the conditions</u> (a) <u>and</u> (b), <u>then</u> $(G,[\ ])$ <u>is a trivial</u> $(2m,m)$-<u>group</u>.

<u>Proof</u>. Let $x * y = [x\ e^{m-1}\ y\ e^{m-1}]_1$. Let $(x_1^m) \in G^m$ and $(y_1^i) \in G^i$ for some $i \in \{1,\ldots,m\}$. Then

$$[x_1^m\ y_1^i\ e^{m-i}] = [x_1^{i-1}\ x_i(x_{i+1}^m\ y_1^{i-1}\ y_i)\ e^{m-i}]$$
$$= [x_1^{i-1}\ x_i[e^{m-1}\ y_i\ x_{i+1}^m\ y_1^{i-1}\ e]e^{m-i}]$$
$$= [x_1^{i-1}[x_i\ e^{m-1}\ y_i\ e^{m-1}]e\ x_{i+1}^m\ y_1^{i-1}\ e^{m-i+1}]$$

$$= [x_1^{i-1} (x_i * y_i)\ e^{m-1}\ e\ x_{i+1}^m\ y_1^{i-1}\ e^{m-i+1}]$$
$$= [x_1^{i-1}\ (x_i * y_i)\ x_{i+1}^m\ y_1^{i-1}\ e^{m-i+1}]$$

implies that

$$[x_1^m\ y_1^m] = [x_1^{m-1}\ (x_m * y_m)\ y_1^{m-1}\ e]$$
$$= [x_1^{m-2}\ (x_{m-1} * y_{m-1})(x_m * y_m)\ y_1^{m-2}\ e^2]$$
$$= \dots = [(x_1 * y_1)(x_2 * y_2) \dots (x_m * y_m)\ e^m]$$
$$= (x_1 * y_1,\ x_2 * y_2,\ \dots,\ x_m * y_m).$$

This shows that $(G,[\ ])$ is a trivial $(2m,m)$-group. ∎

4. Let $(G,[\ ])$ and $(K,[\ ])$ be $(2m,m)$-groups. A map $f:G \longrightarrow K$ is called $(2m,m)$-homomorphism if

$$f^{(m)}([x_1^{2m}]) = [f(x_1)\,f(x_2) \dots f(x_{2m})],$$

where $f^{(m)}:G^m \longrightarrow K^m$ is the m^{th} product of f, i.e. $f^{(m)}(y_1^m) = (f(y_1),\ f(y_2), \dots, f(y_m))$. It is clear that f is a $(2m,m)$-homomorphism iff $f^{(m)}:(G^m,\circ) \longrightarrow (K^m,\circ)$ is a group homomorphism.

Let $f:(G^m,[\ ]) \longrightarrow (K^m,[\ ])$ be a $(2m,m)$-homomorphism, (e^m) the identity in $(G,[\ ])$, (k^m) the identity in $(K,[\ ])$ and $H = \ker(f) = \{x \mid x \in G,\ f(x) = k\} = f^{-1}(k)$. Let us examine some properties of H. First of all, H^m is a normal subgroup of $(G^m,\circ)$. Moreover, H satisfies the following conditions for each $i \in \{1,2,\dots,m\}$:

(4) $\quad [x_1^{i-1}\ H^m\ x_i^m] = [x_1^m\ H^m]$; and

(5) $\quad [x_1^m\ H^m] = [y_1^m\ H^m] \Longleftrightarrow [(x_i)^m\ H^m] = [(y_i)^m\ H^m]$.

Above, $[x_1^{i-1}\ H^m\ x_i^m]$ stands for the set $\{[x_1^{i-1}\ h_1^m\ x_i^m] \mid (h_1^m) \in H^m\}$.

For $m=1$, the condition (5) is trivial, and the condition (4) is equivalent to H being a normal subgroup, provided that H is a subgroup.

Let us show (4). Because $e \in H$, it follows that $[e^i \, H^m \, e^{m-i}] = H^m$ for each $i \in \{0,1,\dots,m\}$. Since H^m is normal in $(G^m,\circ)$ it follows that $[x_1^m \, H^m] = [H^m \, x_1^m]$.

Now, $[x_1^{i-1} H^m x_i^m] = [x_1^{i-1} \, H^m \, x_i^m \, e^m] = [x_1^{m-1} H^m (x_i^m \, e^{i-1}) e^{m-i+1}]$

$= [x_1^{i-1} \, x_i^m \, e^{i-1} \, H^m \, e^{m-i+1}] = [x_1^m \, H^m]$.

This shows that (4) follows only from the fact that H^m is a normal subgroup of $(G^m,\circ)$.

The condition (5) is a consequence of the following equivalences:

$$[x_1^m \, H^m] = [y_1^m \, H^m] \iff f^{(m)}(x_1^m) = f^{(m)}(y_1^m)$$

$$\iff f(x_i) = f(y_i) \quad \text{for each } i \in \{1,\dots,m\}$$

$$\iff f^{(m)}((x_i)^m) = f^{(m)}((y_i)^m) \quad \text{for each } i \in \{1,\dots,m\}$$

$$\iff [(x_i)^m \, H^m] = [(y_i)^m \, H^m] \quad \text{for each } i \in \{1,\dots,m\}.$$

We say that a subset H of a given $(2m,m)$-group $(G,[\;])$ is a $(2m,m)$-<u>subgroup</u> if H^m is a subgroup of $(G^m,\circ)$. A $(2m,m)$-subgroup H of $(G,[\;])$ is called <u>normal</u> $(2m,m)$-<u>subgroup</u> if it satisfies the condition (5) and H^m is a normal subgroup of $(G^m,\circ)$.

Hence $\ker(f)$ is a normal $(2m,m)$-subgroup of a given $(2m,m)$-group $(G,[\;])$ for any $(2m,m)$-homomorphism f from $(G,[\;])$ to some $(2m,m)$-group $(K,[\;])$.

5. Let $(H,[\;])$ be a normal $(2m,m)$-subgroup of $(G,[\;])$. We define a relation $\sim$ on G by

(6) $\quad a \sim b \iff [a^m \, H^m] = [b^m \, H^m]$.

It is easy to check that $\sim$ is an equivalence on G. We denote the factor set $G/\!\sim$ by G/H, and its elements by aH . Next we define $[\;]$ on G/H by:

(7) $\quad [(x_1H)(x_2H)\ldots(x_{2m}H)] = ([x_1^{2m}]_1H,\ldots,[x_1^{2m}]_mH)$.

PROPOSITION 3. (i) $(G/H,[\ ])$ *is a* $(2m,m)$-*group*.

(ii) *The natural map* $\pi : G \longrightarrow G/H$ *defined by* $\pi(x) = xH$ *is a* $(2m,m)$-*homomorphism*.

(iii) $\ker(\pi) = H$.

Proof. (i) Suppose that $x_jH = y_jH$ for each $j \in \{1,2,\ldots,2m\}$, i.e. $[(x_j)^m H^m] = [(y_j)^m H^m]$. Then (5) implies that $[x_1^m H^m] = [y_1^m H^m]$ and $[x_{m+1}^{2m} H^m] = [y_{m+1}^{2m} H^m]$. Now, $[[x_1^{2m}] H^m] = [x_1^m[x_{m+1}^{2m} H^m]]$ $= [x_1^m[y_{m+1}^{2m} H^m]] = [x_1^m H^m y_{m+1}^{2m}] = [y_1^m H^m y_{m+1}^{2m}] = [[y_1^{2m}] H^m]$. This, and (5) imply that for each $i \in \{1,\ldots,m\}$ $[x_1^{2m}]_iH = [y_1^{2m}]_iH$, i.e. $[\ ]$ is well defined.

The associativity and the condition $\underline{0}$. ii) for $[\ ] : (G/H)^{2m} \longrightarrow (G/H)^m$ follow directly from the associativity and the condition $\underline{0}$. ii) for $[\ ] : G^{2m} \longrightarrow G^m$.

(ii) $\pi^{(m)}([x_1^{2m}]) = \pi^{(m)}([x_1^{2m}]_1,\ldots,[x_1^{2m}]_m)$

$=([x_1^{2m}]_1H, \ldots ,[x_1^{2m}]_mH) = [x_1H\ldots\ldots x_{2m}H]$

$= [\pi(x_1)\ \pi(x_2)\ldots \pi(x_{2m})]$.

(iii) $\ker(\pi) = \{x \mid \pi(x) = eH\} = \{x \mid xH = eH\}$

$= \{x \mid x \in H\} = H$. ∎

The $(2m,m)$-group $(G/H,[\ ])$ is called $(2m,m)$-*factor group* of G by H .

PROPOSITION 4. *Let* $(H,[\ ])$ *be a normal* $(2m,m)$-*subgroup of a given* $(2m,m)$-*group* $(G,[\ ])$. *Then* $(G^m/H^m,\circ)$ *is isomorphic to the group* $((G/H)^m,\circ)$ *via an isomorphism* g *defined by* $g((x_1^m)H^m) = (x_1H,\ldots,x_mH) = \pi^{(m)}((x_1^m))$.

Proof. g is well defined because $[x_1^m H^m]=[y_1^m H^m]$ implies that $\pi^{(m)}((x_1^m)) = \pi^{(m)}((y_1^m))$. Since $\pi^{(m)}$ is an epimorphism it follows that g is an epimorphism . If $g((x_1^m)H^m) = (eH)^m$, then $\pi^{(m)}((x_1^m)) = (eH)^m$, which implies that $[(x_1^m)H^m] = H^m$. Hence, g is a monomorphism. ∎

6. Suppose that $(G,[\ ])$ is a trivial $(2m,m)$-group gotten from a group $(G,\cdot)$. Let H be a normal subgroup of $(G,\cdot)$. Then H^m is a normal subgroup of $(G^m,\circ)$. To show that H satisfies (5), let $(x_1^m), (y_1^m) \in G^m$. Then $[x_1^m\ H^m] = [y_1^m\ H^m] \iff x_iH = y_iH$ for each $i \in \{1,\ldots,m\}$

$\iff [(x_i)^m\ H^m] = [(y_i)^m\ H^m]$ for each $i \in \{1,\ldots,m\}$.

Hence, $(H,[\ ])$ is a normal $(2m,m)$-subgroup of $(G,[\ ])$.

Conversely, suppose that H is a normal $(2m,m)$-subgroup of a trivial $(2m,m)$-group $(G,[\ ])$. If $h_1,h_2 \in H$, then $[h_1\ e^{m-1}\ h_2\ e^{m-1}] = (h_1h_2,e^{m-1}) \in H^m$, and $(h_1,e^{m-1})^{-1} = (h_1^{-1},e^{m-1}) \in H^m$. Hence, H is a subgroup of $(G,\cdot)$. Because H^m is a normal subgroup of $(G^m,\circ)$, it follows that $(x,e^{m-1})H^m = H^m(x,e^{m-1})$ i.e. $xH = Hx$ for each $x \in G$. Hence, H is a normal subgroup of $(G,\cdot)$.

The above discussion shows that the notion of normal $(2m,m)$-subgroups makes sense only for "pure" $(2m,m)$-groups, i.e. for $(2m,m)$-groups that are not trivial $(2m,m)$-groups. Otherwise, it is the same as the notion of normal subgroups.

7. A $(2m,m)$-group can be thought of as an algebra $(G,e;\{[\ ]_i, [\backslash]_i, [/]_i\}_{i=1,\ldots,m})$ where $[\ ]_i, [\backslash]_i, [/]_i$ are $2m$-ary operations , e is a constant, and the following identities are satisfied for each $i \in \{1,\ldots,m\}$:

$$[x_1^p[x_{p+1}^{p+2m}]_1 \ldots [x_{p+1}^{p+2m}]_m\ x_{p+2m+1}^{3m}]_i =$$

$$= [[x_1^{2m}]_1 \ldots [x_1^{2m}]_m \, x_{2m+1}^{3m}]_i \;,$$

$$[x_{m+1} \ldots x_{2m} \setminus x_1 \ldots x_m]_i = x_i \;,$$

$$[x_1 \ldots x_m \,/\, x_{m+1} \ldots x_{2m}]_i = x_i \;, \quad \text{and}$$

$$[e^m \, x_1^m]_i = x_i = [x_1^m \, e^m]_i \,.$$

Hence, the class of (2m,m)-groups is a variety of algebras. So, for better understanding of the (2m,m)-groups it is needed to obtain canonical forms for the elements in free (2m,m)-groups.

We note that free (2m,m)- groups are not trivial (2m,m)-groups.

References

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

[2] D. Dimovski, Some existence conditions for vector valued groups, Godišen Zbornik na Mat. Fak., 33-34 (1982-1983) 99-103 .

Ǵ. Čupona, D. Dimovski
Matematički Fakultet, P.F. 504
91000 SKOPJE

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", ZAGREB 1984

SOME PROPERTIES OF Δ-ENDOMORPHISM NEAR-RINGS

Vučić Dašić

Abstract. The purpose of this note is to investigate some properties of a Δ-endomorphism near-ring EΔ(G) which depend upon the structure of the group (G,+). In this sence the properties which are attribute for a normal subgroup Δ of G act on the properties of the Δ-endomorphism near-ring EΔ(G).

By $M_0(G)$ we shall denote the set of all zero preserving mappings of a group (G,+) into itself.If Δ is a normal subgroup of G, then $f \in M_0(G)$ is an Δ-endomorphism of G if and only if $(\Delta)f \subseteq \Delta$ and for all $x,y,\in G$ there exists $d\in\Delta$ such that

$$(x+y)f=(x)f+(y)f+d.$$

The near-ring generated additively by the set $End_\Delta(G)$ of all Δ-endomorphisms of a group (G,+), will be called a Δ-endomorphism near-ring and will be denoted by $E_\Delta(G)$. We consider a near-ring of these Δ-endomorphisms for which is invariant every fully invariant subgroup of the group G. We recall that these subgroups are EΔ-invariant.

A normal subgroup $\mathfrak{D}$ of the group (EΔ(G),+) generated by the set

$$\{\delta / \delta=-(ht+ft)+(h+f)t,\ h,f\ E_\Delta(G), t\in End_\Delta(G)\}$$

is called a defct of distributivity of $E_\Delta(G)$. It is clear that

$$\mathfrak{D} \subseteq (G,\Delta)_0$$

where $(G,\Delta)_0$ is the set of all zero preserving mappings $f:G\to\Delta$. Note that the defect $\mathfrak{D}$ of $E_\Delta(G)$ depends upon the choice of the normal subgroup Δ. For details see [2].

Let (R,S) (or brieflly R) be a subnear-ring of $E_\Delta(G)$ generated by $S \subseteq End_\Delta(G)$. We consider the group G as an (R,S)-group and suppose $Inn(G) \subseteq S \subseteq End_\Delta(G)$. Also, E_Δ -invariant subgroups become (R,S)-subgroups of G.

The following theorem gives some information about the structure of the Δ-endomorphism near-ring (R,S).

THEOREM 1. If H is a nonzero (R,S)-subgroup of G such that $\Delta \cap H=(0)$, then (R,S) is equal either to the endomorphism nearring or to the Δ-endomorphism near-ring whose restrictions on H are the endomorphisms of (H,+).

Proof. If $\Delta=(0)$, then a Δ-endomorphism is just an endomorphism of (G,+). Assume that $\Delta \neq (0)$ and $\Delta \cap H=(0)$. For all $t \in S \subseteq End_\Delta(G)$ and all $a_1, a_2 \in H$ there exists $d \in \Delta$ such that

$$(a_1+a_2)t=(a_1)t+(a_2)t+d.$$

Since, by assumption, H is a (R,S)-subgroup, we have $(a_1+a_2)t \in H$, $(a_1)t \in H$ and $(a_2)t \in H$. Therefore $d \in H$. But $\Delta \cap H=(0)$ and hence d=o. Thus the restriction $t|H$ is an endomorphism of (H,+).

The following theorem characterises the defect $\mathcal{D}$ of the Δ-endomorphism near-ring (R,S).

THEOREM 2. Let H be a (R,S)-subgroup of G and let $\mathcal{D}$ be the defect of (R,S). If for all $t \in S$ the restriction $t|H$ is an endomorphism of (H,+), then $(H)\mathcal{D}=(0)$ and R/Ann(H) is a distributively generated (d.g.) near-ring.

Proof. For all $\delta \in \mathcal{D}$ we have $\delta = \sum_i (r_i+\theta_i-r_i)$, where $r_i \in R$ and $\theta_i =-(x_i t_i + y_i t_i)+(x_i+y_i)t_i, (x_i, y_i \in R, t_i \in S)$. Thus, for all $a \in H$

$$(a)\theta_i=-(a)y_i t_i-(a)x_i t_i+((a)x_i+(a)y_i)t_i=0,$$

because, by assumption, the restrictions $t_i|H$ are the endomorphisms of (H,+). Hence, for all $a \in H$ and $\delta \in \mathcal{D}$, $(a)\,\delta=0$, i.e. $(H)\mathcal{D}=(0)$. Thus $\mathcal{D} \subseteq Ann(H)$ and from Corollary of Theorem 2.6 of [1], R/Ann(H) is a d.g. near-ring.

Applying theorems 1 and 2, we obtain the following.

COROLLARY. If H is a nonzero (R,S)-subgroup of G such that $\Delta \cap H=(0)$, then $(H)\mathcal{D}=(0)$, where $\mathcal{D}$ is a defect of (R,S). Further R/Ann(H) is a d.g. near-ring.

Like in [3] we shall supose the existence of minimal (R,S)-subgroups of G. In this sence the following theorem generalizes the Theorem 1.4 in [3]

THEOREM 3. Let G be a (R,S)-group such that $\Delta \cap H=(0)$ for every (R,S)-subgroup H of G. Then G and all its (R,S) images have minimal (R,S)-subgroups, either

1^o if G satisfies the minimum condition on (R,S)-subgroups, or

2^o if R satisfies the descending chain condition on right ideals.

Proof. 1^o The first case is obvious.

2^o Let R satisfies the descending chain condition on right ideals of R and let

$$G = H_0 \supset H_1 \supset \dots \supset H_i \supset H_{i+1} \supset \dots \quad (1)$$

be a decreasing sequence of (R,S)-subgroups. By using Theorem 1, we have that the relative defect of the set $B_i = \{r \in R/(H_i)r \subseteq H_i\}$ with respect to R is contained in B_i, i.e.

$$\{-bs-xs+(x+b)s/b \in B_i,\ x \in R, s \in S\} \subseteq B_i$$

Thus, by Proposition 3.1 of [2], B_i is a right ideal of R. Consequently, the chain (1) induces the chain of right ideals

$$R=B_0 \supset B_1 \supset \dots \supset B_i \supset B_{i+1} \supset \dots \quad (2).$$

Assume that the chain (1) does not stabilize after finitely many steps, i.e. there is an integer n such that $H_i \supset H_{i+1}$ for all i>n. We seek a contradiction to this assumption. According to Proposition 3.2 in [2], B_i is a nonzero right ideal of R, where $B_i \supset B_{i+1}$ for all i>n. This contradicts to the fact that the chain (2) terminates after finitely many steps.

THEOREM 4. Let $\mathcal{D}$ be a defect of a near-ring (R,S) and let H be a minimal (R,S)-subgroup of G. For all $t \in S$ the restriction $t|H$ is an endomorphism of (H,+) if, and only if, $(H)\mathcal{D}=(0)$.

Proof. If for all $t \in S$ the restriction $t|H$ is an endomorphism of (H,+), then the result follows from Theorem 2.

Conversely, let $(H)\mathcal{D}=(0)$. Since H is a minimal (R,S)-subgroup, it follows that for all a, $a_1, a_2 \in H$ there exist $x, y \in R$ such that $(a)x=a_1$ and $(a)y=a_2$ (Prop.2.3, [2]). By definition of therelative defect $\mathcal{D}$, for all $t \in S$ and $x, y \in R$ there exists $\delta \in \mathcal{D}$, such that $\delta=-yt-xt+(x+y)t$. By assumption, $(a)\delta=0$ for all $a \in H$ and all $\delta \in \mathcal{D}$. Thus,

$$0 = -(a)yt-(a)xt+((a)x+(a)y)t, \text{i.e.}$$
$$0 = -(a_1)t-(a_2)t+(a_1+a_2)t.$$

Hence, for all $a_1, a_2 \in H$ and all $t \in S$, $(a_1+a_2)t=(a_1)t+(a_2)t$ and this finishes the proof.

Let H be a subgroup of G and denote the derived subgroup of H by H'. We remember that H is perfect if, and only if, H'=H. As a generalization of the result (Th. 1.9, [3] we obtain the following.

THEOREM 5. *Let H be a perfect minimal (R,S)-subgroup of G such that $\Delta \cap H=(0)$. Then R/Ann(H) is a d.g. near-ring which is isomorphic to a dense subnear-ring of $M_0(H)$.(Density means that for all $m \in M_0(H)$ and given any finite set of distinct nonzero elements $h_1,\dots,h_n$ H, there is an $\bar{r} \in R/Ann(H)$ such that $(h_i)\bar{r}=((h_i)m, i=1,\dots,n)$.*

Proof. Since $\Delta \cap H=(0)$, then by Theorem 1 it follows that for each Δ-endomorphism, the restriction on H is an endomorphism of (H,+). Thus H is an (R,S)-subgroup of type 2. On the other hand,by Corollary,it follows $(H)\mathcal{D}=$ $=(0)$. Consequently,$\mathcal{D} \subseteq Ann(H)$, where $\mathcal{D}$ is a defect of (R,S). By using the Corollary of Therorem 2.6. of [1], we have that R/Ann(H) is a d.g. near-ring and result follows from Theorem 1.9 of [3].

REFERENCES

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

[2] V.Dašić, *Δ-endomorphism near-rings*, Publ.Inst.Math.(Beograd) 28(42) (1980), 61-75.

[3] C.G. Lyons, J.D.P.Meldrum, *Reduction theorems for endomorphism near-rings*, Monats. Math. 89(1980), 301-313.

INSTITUT ZA MATEMATIKU I FIZIKU
Univerzitet u Titogradu
81000 Titograd
JUGOSLAVIJA

ON PSEUDOAUTOMORPHISMS AND NUCLEI OF RD-GROUPOIDS

Ivo Đurović

Abstract. In this work the pseudoautomorphisms of the regular groupoids with division are investigated. Some properties of the pseudoautomorphisms and relations between pseudoautomorphisms and nuclei of such groupoids have been described.

According to [1.] and [2.] we can give these definitions:

DEFINITION 1. A groupoid with division $(G,\cdot)$ is a regular groupoid with division (briefly RD-groupoid) if and only if it satisfies the conditions:

$$(\exists z \in G)\, z\cdot x = z\cdot y \Rightarrow (\forall z \in G)\, z\cdot x = z\cdot y$$
$$(\exists z \in G)\, x\cdot z = y\cdot z \Rightarrow (\forall z \in G)\, x\cdot z = y\cdot z .$$

DEFINITION 2. The left /right/ translation of the groupoid $(G,\cdot)$ by $a \in G$ is a mapping $\lambda_a : G \to G$, $\lambda_a x = a\cdot x$ / $\rho_a : G \to G$, $\rho_a x = x\cdot a$ /.

DEFINITION 3. A bijection $\pi: G\to G$ is a right /left/ pseudoautomorphism of the groupoid $(G,\cdot)$ if and only if there exists $c \in G$ such that $(\lambda_c\pi, \pi, \lambda_c\pi)$ / $(\pi, \rho_c\pi, \rho_c\pi)$/ is an autotopy of the groupoid $(G,\cdot)$, i.e. $(\forall x,y \in G)\, \lambda_c\pi(x\cdot y) = \lambda_c\pi x\cdot \pi y$ / $(\forall x,y \in G)\, \rho_c\pi(x\cdot y) = \pi x\cdot \rho_c\pi y$/ holds. c is called the companion of the right /left/pseudoautomorphism. If π is the left pseudoautomorphism and the right pseudoautomorphism we call it twosided pseudoautomorphism.

DEFINITION 4. The left /right/ nucleus of the groupoid $(G,\cdot)$ is the set $N_\ell = \{x \in G : (\forall y,z \in G)\; x\cdot(y\cdot z) = (x\cdot y)\cdot z\}$ / $N_r = \{z \in G : (\forall x,y \in G)\; x\cdot(y\cdot z) = (x\cdot y)\cdot z\}$ /.

Let us first prove two lemmas:

LEMMA 1. The groupoid with division $(G,\cdot)$ has at least one right /left/ pseudoautomorphism if and only if it has at least one left /right/ identity element.

Proof. 1° Let π be the right pseudoautomorpfism of the groupoid with division $(G,\cdot)$ and let $c \in G$ be one of its companions. Let $e \in G$ be a right local identity element of c, i.e. $c \cdot e = c$, which by Definition 2. we can write in the form $\lambda_c e = c$. Then we have

$(\forall x,y \in G)\, \lambda_c \pi(x\cdot y) = \lambda_c \pi x \cdot \pi y$ (by Definition 3)

$(\forall y \in G)\, \lambda_c \pi(\pi^{-1}e\cdot y) = \lambda_c \pi\pi^{-1} e \cdot \pi y$ (by the substitution x with $\pi^{-1}e$)

$(\forall y \in G)\, \lambda_c \pi(\pi^{-1}e\cdot y) = \lambda_c e \cdot \pi y$ (since $\pi\pi^{-1}$ is identity mapping)

$(\forall y \in G)\, \lambda_c \pi(\pi^{-1}e\cdot y) = c \cdot \pi y$ (since $\lambda_c e = c$)

$(\forall y \in G)\, \lambda_c \pi(\pi^{-1}e\cdot y) = \lambda_c \pi y$ (by Definition 2)

$(\forall y \in G)\, \pi^{-1}e \cdot y = y$ (since $\lambda_c \pi$ is bijection),

which means that $\pi^{-1}e$ is the left identity element of $(G,\cdot)$.

2° Let e be a left identity element of the groupoid with division $(G,\cdot)$ and let $\imath$ be identity mapping of the set G. Then we have

$(\forall x,y \in G)\, e\cdot(x\cdot y) = (e\cdot x)\cdot y$ (since e is the left identity element)

$(\forall x,y \in G)\, e\cdot \imath(x\cdot y) = (e\cdot \imath x)\cdot \imath y$ (since $\imath$ is the identity mapping)

$(\forall x,y \in G)\, \lambda_e \imath(x\cdot y) = \lambda_e \imath x \cdot \imath y$ (by Definition 2),

hence identity mapping is a right pseudoautomorphism with companion e of the groupoid $(G,\cdot)$.

Remark. The proof for the left pseudoautomorphism and the right identity element is completely analogous to the given proof for the right pseudoautomorphism and left identity element, and such we omit it. We shall omit furthermore the proof for the left pseudoautomorphism, right identity element and right nucleus whenever it is analogous with the proof for the right pseudoautomorphism, left identity element and left nucleus.

LEMMA 2. The RD-groupoid $(G,\cdot)$ has a non-empty left /right/ nucleus if and only if it has at least one left /right/ identity element.

Proof. 1° Let e be a left identity element of $(G,\cdot)$. Then $(e\cdot x)\cdot y = x\cdot y = e\cdot(x\cdot y)$ for each $x,y \in G$. Therefore $e \in N_\ell$ and accordingly $N_\ell \neq \emptyset$.

2° Let $N_\ell \neq \emptyset$, i.e. there exists $a \in N_\ell$, and let $b \in G$ be a right local identity element of a, i.e. $a\cdot b = a$. Then

$(\forall x \in G)\ (a\cdot b)\cdot x = a\cdot(b\cdot x)$ (since $a \in N_\ell$)

$(\forall x \in G)\ a\cdot x = a\cdot(b\cdot x)$ (since $a\cdot b = a$)

$(\forall x \in G)(\forall z \in G)\ z\cdot x = z\cdot(b\cdot x)$ (by Definition 1)

Interchanging z by b it follows that $(\forall x \in G)\ b\cdot x = b\cdot(b\cdot x)$ and by interchanging $b\cdot x$ by y we get $(\forall y \in G)\ y = b\cdot y$, i.e. b is the left identity element of $(G,\cdot)$.

From the Lemma 1. and Lemma 2. immediately follows

THEOREM 1. For each RD-groupoid $(G,\cdot)$ these conditions are equivalent:

(i) $(G,\cdot)$ has at least one right /left/ pseudoautomorphism,

(ii) $(G,\cdot)$ has at least one left /right/ identity element,

(iii) $(G,\cdot)$ has non-empty left /right/ nucleus.

COROLLARY 1. If RD-groupoid $(G,\cdot)$ has at least one twosided pseudoautomorphism then $(G,\cdot)$ is a loop.

Proof. By Theorem 1. $(G,\cdot)$ is a RD-groupoid with twosided identity element. Let e be a left identity element of $(G,\cdot)$. Then

$a\cdot x = a\cdot y \Rightarrow (\forall z \in G)\ z\cdot x = z\cdot y$ (by Definition 1)

$\Rightarrow e\cdot x = e\cdot y$ (by the substitution of z with e)

$\Rightarrow x = y$ (since e is the left identity element),

i.e. the RD-groupoid $(G,\cdot)$ satisfies the left-cancellation law.

THEOREM 2. Every element of the left nucleus N_ℓ /right nucleus N_r/ of the RD-groupoid $(G,\cdot)$ is the companion of at least one right /left/ pseudoautomorphism of that groupoid.

Proof. From the fact that $(G,\cdot)$ is a groupoid with division and proof of Corollary 1. immediately follows that for each $a \in G$ the mapping λ_a is bijective. Let $a \in N_\ell$ and let $\imath$ be identity mapping of the set G. Then

$(\forall x,y \in G)\ a\cdot(x\cdot y) = (a\cdot x)\cdot y$ (by Definition 4)

$(\forall x,y \in G)\ \lambda_a(x\cdot y) = \lambda_a x\cdot y$ (by Definition 2)

$(\forall x,y \in G)\ \lambda_a \imath(x\cdot y) = \lambda_a \imath x\cdot \imath y$ (since $\imath$ is the identity mapping),

which by Definition 3. means that the identity mapping $\imath$ is a right pseudoautomorphism with companion a of the RD-groupoid $(G,\cdot)$.

THEOREM 3. Let π be a right /left/ pseudoautomorphism with the companion c of the RD-groupoid $(G,\cdot)$. π is the automorphism of the RD-groupoid $(G,\cdot)$ if and only if c is an element of the left /right/ nucleus of $(G,\cdot)$.

Proof. 1° Let π be an automorphism of the RD-groupoid $(G,\cdot)$, i.e. $(\forall x,y \in G)\ \pi(x\cdot y)=\pi x\cdot\pi y$ holds. Then

$(\forall x,y \in G)\ \lambda_c\pi(x\cdot y) = \lambda_c\pi x\cdot\pi y$ (by supposition of Theorem 3)

$(\forall x,y \in G)\ \lambda_c(\pi x\cdot\pi y) = \lambda_c\pi x\cdot\pi y$ (since $\pi(x\cdot y)=\pi x\cdot\pi y$)

$(\forall x,y \in G)\ \lambda_c(x\cdot y) = \lambda_c x\cdot y$ (by the substitution of x, y with $\pi^{-1}x, \pi^{-1}y$ respectively)

$(\forall x,y \in G)\ c\cdot(x\cdot y) = (c\cdot x)\cdot y$ (by Definition 2),

which by Definition 4. gives that c is the element of the left nucleus N_ℓ of the RD-groupoid $(G,\cdot)$.

2° Let c be an element of the left nucleus N_ℓ of the RD-groupoid $(G,\cdot)$. Then

$(\forall x,y \in G)\ \lambda_c\pi(x\cdot y) = \lambda_c\pi x\cdot\pi y$ (by the supposition of Theorem 3)

$(\forall x,y \in G)\ c\cdot\pi(x\cdot y) = (c\cdot\pi x)\cdot\pi y$ (by Definition 2)

$(\forall x,y \in G)\ c\cdot\pi(x\cdot y) = c\cdot(\pi x\cdot\pi y)$ (since $c \in N_\ell$).

Since by Theorem 1. RD-groupoid $(G,\cdot)$ has at least one left identity element and by the proof of Corollary 1. RD-groupoid with left identity element satisfies the left-cancellation law, it follows that $(\forall x,y \in G)\ \pi(x\cdot y)=\pi x\cdot\pi y$, i.e. π is the automorphism of that groupoid.

THEOREM 4. Let $\mathcal{P}$ be the set of all right /left/ pseudoautomorphisms of the RD-groupoid $(G,\cdot)$ with the left /right/ identity element e. The set $\mathcal{P}$ with the composition of mappings as binary operation is a group.

Proof. By Theorem 1. $\mathcal{P}$ is a non-empty set. Let $\pi_1, \pi_2 \in \mathcal{P}$, c_1 companion of π_1 and c_2 companion of π_2, i.e. let $(\lambda_{c_1}\pi_1, \pi_1, \lambda_{c_1}\pi_1)$ and $(\lambda_{c_2}\pi_2, \pi_2, \lambda_{c_2}\pi_2)$ be autotopies of the groupoid $(G,\cdot)$. Then $(\lambda_{c_1}\pi_1\lambda_{c_2}\pi_2, \pi_1\pi_2, \lambda_{c_1}\pi_1\lambda_{c_2}\pi_2)$ is an autotopy of $(G,\cdot)$, and since

$$\lambda_{c_1}\pi_1\lambda_{c_2}\pi_2 x = \lambda_{c_1}\pi_1(\lambda_{c_2}\pi_2 x)$$

$$= \lambda_{c_1}\pi_1(c_2\cdot\pi_2 x) \quad \text{(by Definition 2)}$$

$$= \lambda_{c_1}\pi_1 c_2\cdot\pi_1\pi_2 x \quad \text{(since } (\lambda_{c_1}\pi_1, \pi_1, \lambda_{c_1}\pi_1) \text{ is the autotopy)}$$

$$= (c_1\cdot\pi_1 c_2)\cdot\pi_1\pi_2 x \quad \text{(by Definition 2)}$$

$$= \lambda_{c_1\cdot\pi_1 c_2}\pi_1\pi_2 x \quad \text{(by Definition 2),}$$

it follows that $(\lambda_{c_1\cdot\pi_1 c_2}\pi_1\pi_2, \pi_1\pi_2, \lambda_{c_1\cdot\pi_1 c_2}\pi_1\pi_2)$ is an autotopy of the given groupoid, i.e. $\pi_1\pi_2$ is a right pseudoautomorphism with the companion $c_1\cdot\pi_1 c_2$ of the groupoid $(G,\cdot)$. It holds as well (by the part 2° of the proof of Theorem 1) that the identity mapping ι is a right pseudoautomorphism with the companion e of the given groupoid and the composition of mappings is associative, so $\mathcal{P}$ is a semigroup with identity element.

Let π be a right pseudoautomorphism with the companion c of the groupoid $(G,\cdot)$. Then by Definition 3. there exists the mapping π^{-1} and $(\lambda_c\pi, \pi, \lambda_c\pi)$ is an autotopy of $(G,\cdot)$. It follows that $((\lambda_c\pi)^{-1}, \pi^{-1}, (\lambda_c\pi)^{-1}) = (\pi^{-1}\lambda_c^{-1}, \pi^{-1}, \pi^{-1}\lambda_c^{-1})$ is an autotopy of the given groupoid, and since

$$\pi^{-1}\lambda_c^{-1} x = \pi^{-1}\lambda_c^{-1}(e\cdot x) \quad \text{(since } e \text{ is the left identity element)}$$

$$= \pi^{-1}\lambda_c^{-1} e\cdot\pi^{-1} x \quad \text{(since } (\pi^{-1}\lambda_c^{-1}, \pi^{-1}, \pi^{-1}\lambda_c^{-1}) \text{ is the autotopy)}$$

$$= \lambda_{\pi^{-1}\lambda_c^{-1} e}\pi^{-1} x \quad \text{(by Definition 2),}$$

it follows that $(\lambda_{\pi^{-1}\lambda_c^{-1} e}\pi^{-1}, \pi^{-1}, \lambda_{\pi^{-1}\lambda_c^{-1} e}\pi^{-1})$ is an autotopy, i.e. that $\pi^{-1} \in \mathcal{P}$, which completes the proof.

THEOREM 5. The set $\mathcal{P}_c$ of all right /left/ pseudoautomorphisms with companion c is the left /right/coset in the decomposition of the group $\mathcal{P}$ of all right /left/ pseudoautomorphisms of the RD-groupoid $(G,\cdot)$ with the left /right/ identity element with respect to the subgroup $\mathcal{A}$ of the automorphisms of that groupoid, i.e. if $\pi \in \mathcal{P}_c$ then $\mathcal{P}_c = \pi\mathcal{A}$ $/\mathcal{P}_c = \mathcal{A}\pi/$.

Proof. 1° Let $\pi \in \mathcal{P}_c$ and $\alpha \in \mathcal{A}$. Then $(\lambda_c\pi, \pi, \lambda_c\pi)$ and (α,α,α) are autotopies of the groupoid $(G,\cdot)$ and thus $(\lambda_c\pi\alpha, \pi\alpha, \lambda_c\pi\alpha)$ is an autotopy of that groupoid as well, consequently $\pi\alpha \in \mathcal{P}_c$, which gives $\pi\mathcal{A} \subseteq \mathcal{P}_c$.

2° Let $\pi \in \mathcal{P}_c$ and let ψ be any element of the set $\mathcal{P}_c$, i.e. let $(\lambda_c\pi, \pi, \lambda_c\pi)$ and $(\lambda_c\psi, \psi, \lambda_c\psi)$ be autotopies of the groupoid $(G,\cdot)$. Then $(\lambda_c\pi, \pi, \lambda_c\pi)^{-1}(\lambda_c\psi, \psi, \lambda_c\psi) = (\pi^{-1}\lambda_c^{-1}\lambda_c\psi, \pi^{-1}\psi, \pi^{-1}\lambda_c^{-1}\lambda_c\psi) = (\pi^{-1}\psi, \pi^{-1}\psi, \pi^{-1}\psi)$, i.e. $\pi^{-1}\psi$ is an automorphism of $(G,\cdot)$. It follows that $\psi = \pi(\pi^{-1}\psi) \in \pi\mathcal{A}$, i.e. $\mathcal{P}_c \subseteq \pi\mathcal{A}$, which completes the proof.

REFERENCES

1. V.D. Belousov, Osnovy teorii kvazigrupp i lup, Nauka, Moskva, 1967.
2. N.I. Prodan, Pravil'nye gruppoidy s deleniem, Issledovanija po teorii kvazigrupp i lup, Štiinca, Kišinev, 1973, 139-145.

Ivo Đurović
Fakultet graditeljskih znanosti
51000 Rijeka
Tršćanska obala 6.

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", ZAGREB 1984

THE ELATION SEMI-BIPLANE WITH 22 POINTS ON A LINE

Ksenija Horvatić-Baldasar

Abstract. In this article we give the proof of the existence of the elation semi-biplane with k=22 points on a line.

As it is already known there exists the elation semi-biplane with k=6 and k=10 points on a line respectively [1]. The elation semi-biplane with k=14 points on a line is determined and constructed as well [2].

The following member of this series, if does it exist, would be the elation semi-biplane with k=22 points on a line. The series, as one can see, consists of the elation semi-biplanes with k=2p, p >2 prime number.

It is of interest to observe that for k=6,14 and 22 there doesn't exist the projective plane of the same order, and for k=10 the corresponding projective plane of order 10 is still in doubt.

All necessary facts about semi-biplanes can be found in [1] and [3].

Applying the well known relations:

$$v = t + \binom{k}{2} \quad (1) \qquad \text{and} \qquad kt \leq v \quad (2)$$

we get for k=22:

$$v = t + 231 \qquad \text{and} \qquad t \leq 11.$$

Taking for t=1,2,...,11 in turn, we can see that the only possibilities for a divisible semi-biplane are for t=1,3,7 and 11.

For t=1 a biplane doesn't exist (according to the Bruck-Ryser-Chowla theorem). According to another necessary condition, i.e. Bose-O'Conner theorem [4] for divisible semi-biplanes, in the cases t=3,7 and 11 the semi-biplanes could exist.

In this paper we shall investigate only the case t=11 and v=242. This is actually an elation semi-biplane as k=22 is even and $t = \frac{k}{2} = 11$.

So let the 242 points of that semi-biplane be denoted with:

$$1_i, 2_i, \ldots, 22_i \qquad i=0,1,\ldots,10$$

and let us suppose the automorphism ϱ which acts on these points as follows:

$(A_i)^{\varrho} = A_{i+1}$ for all $A \in \{1,2,\ldots,22\}$ and for all indices $i \in \{0,1,\ldots,10\}$. The indices i are to be considered as integers mod 11. The automorphism ϱ acts transitevely on every "parallel class" of lines and on every "system" of points.

For the first line p_1 we can take without loss of generality:

$$p_1 = \{1_0,2_0,3_0,4_0,5_0,6_0,7_0,8_0,9_0,10_0,11_0,12_0,13_0,14_0,15_0,16_0,17_0,18_0,19_0,20_0,21_0,22_0\}.$$

Then the whole first "parallel class" will be obtained with $<\varrho>$ from p_1.

So we have still to construct 21 "parallel classes", but it will be sufficient to construct only the first line from each class as the automorphism ϱ will produce the remaining.

Let these lines be denoted with: $p_2,p_3,\ldots,p_{22}$. We shall find them with the help of another automorphism σ of order 11 which commutes with ϱ and respects the compatibility conditions for the lines of semi-biplanes:

$$|p_i^{\varrho^k} \cap p_j^{\varrho^m}| = 2 \quad \text{for all } k,\ m = 0,1,\ldots,10 \quad i \neq j \quad i,j \in \{1,2,\ldots,22\}.$$

The action of σ on the points of this semi-biplane is given as follows:

$$\sigma = (1_0)(1_1)(1_2)(1_3)(1_4)(1_5)(1_6)(1_7)(1_8)(1_9)(1_{10})$$
$$(2_0, 2_1, 2_2, 2_3, 2_4, 2_5, 2_6, 2_7, 2_8, 2_9, 2_{10})$$
$$(3_0, 3_2, 3_4, 3_6, 3_8, 3_{10}, 3_1, 3_3, 3_5, 3_7, 3_9)$$
$$(4_0, 4_3, 4_6, 4_9, 4_1, 4_4, 4_7, 4_{10}, 4_2, 4_5, 4_8)$$
$$(5_0, 5_4, 5_8, 5_1, 5_5, 5_9, 5_2, 5_6, 5_{10}, 5_3, 5_7)$$
$$(6_0, 6_5, 6_{10}, 6_4, 6_9, 6_3, 6_8, 6_2, 6_7, 6_1, 6_6)$$
$$(7_0, 7_6, 7_1, 7_7, 7_2, 7_8, 7_3, 7_9, 7_4, 7_{10}, 7_5)$$
$$(8_0, 8_7, 8_3, 8_{10}, 8_6, 8_2, 8_9, 8_5, 8_1, 8_8, 8_4)$$
$$(9_0, 9_8, 9_5, 9_2, 9_{10}, 9_7, 9_4, 9_1, 9_9, 9_6, 9_3)$$
$$(10_0, 10_9, 10_7, 10_5, 10_3, 10_1, 10_{10}, 10_8, 10_6, 10_4, 10_2)$$
$$(11_0, 11_{10}, 11_9, 11_8, 11_7, 11_6, 11_5, 11_4, 11_3, 11_2, 11_1)$$
$$(12_0, 13_1, 14_4, 15_9, 16_5, 17_3, 18_3, 19_5, 20_9, 21_4, 22_1)$$
$$(12_1, 13_2, 14_5, 15_{10}, 16_6, 17_4, 18_4, 19_6, 20_{10}, 21_5, 22_2)$$
$$(12_2, 13_3, 14_6, 15_0, 16_7, 17_5, 18_5, 19_7, 20_0, 21_6, 22_3)$$

$$(12_3,\ 13_4,\ 14_7,\ 15_1,\ 16_8,\ 17_6,\ 18_6,\ 19_8,\ 20_1,\ 21_7,\ 22_4\ )$$
$$(12_4,\ 13_5,\ 14_8,\ 15_2,\ 16_9,\ 17_7,\ 18_7,\ 19_9,\ 20_2,\ 21_8,\ 22_5\ )$$
$$(12_5,\ 13_6,\ 14_9,\ 15_3,\ 16_{10},17_8,\ 18_8,\ 19_{10},20_3,\ 21_9,\ 22_6\ )$$
$$(12_6,\ 13_7,\ 14_{10},15_4,\ 16_0,\ 17_9,\ 18_9,\ 19_0,\ 20_4,\ 21_{10},22_7\ )$$
$$(12_7,\ 13_8,\ 14_0\ \ 15_5,\ 16_1,\ 17_{10},18_{10},19_1,\ 20_5,\ 21_0,\ 22_8\ )$$
$$(12_8,\ 13_9,\ 14_1,\ 15_6,\ 16_2,\ 17_0,\ 18_0,\ 19_2,\ 20_6,\ 21_1,\ 22_9\ )$$
$$(12_9,\ 13_{10},14_2,\ 15_7,\ 16_3,\ 17_1,\ 18_1,\ 19_3,\ 20_7,\ 21_2,\ 22_{10})$$
$$(12_{10},13_0,\ 14_3,\ 15_8,\ 16_4,\ 17_2,\ 18_2,\ 19_4,\ 20_8,\ 21_3,\ 22_0\ ),$$

where: $p_2 = p_1^{\sigma}$, $p_3 = p_2^{\sigma}, \dots, p_{11} = p_{10}^{\sigma}$.

Actually, we have found the first half of the elation semi-biplane as the automorphism ϱ will produce all remaining parallel lines.

The next line we have to determine is p_{12}. Considering the elation semi-biplanes with k=10 and k=14 from [1] and [2], p_{12} is determined (without the help of a computor) to be:

$$p_{12} = \{1_0,\ 2_5.\ 3_9,\ 4_1,\ 5_3,\ 6_4,\ 7_4,\ 8_3,\ 9_1,\ 10_9,\ 11_5,$$
$$12_0,\ 13_2,\ 14_8,\ 15_7,\ 16_{10},\ 17_6,\ 18_6,\ 19_{10},\ 20_7,\ 21_8,\ 22_2\}$$

Acting again with the automorphism σ we find:

$$p_{13} = p_{12}^{\sigma},\ p_{14} = p_{13}^{\sigma}, \dots, p_{22} = p_{21}^{\sigma}.$$

The complete second half of the lines of the elation semi-biplane will be obtained with $\langle \varrho \rangle$.

We have proved:

THEOREM. There exist at least one elation semi-biplane with 22 points on every line with the group $G = \langle \varrho, \sigma \rangle$ of automorphisms where $\varrho^{11} = \sigma^{11} = 1$ and $\varrho \cdot \sigma = \sigma \cdot \varrho$.

Open problem: Does there exist the series of the elation semi-biplanes for every k=2p, p>2 prime number?

Acknowledgement. The author is grateful to Professor Z.Janko for the useful suggestions.

$$P_1 = \{1_0, 2_0, 3_0, 4_0, 5_0, 6_0, 7_0, 8_0, 9_0, 10_0, 11_0, 12_0, 13_0, 14_0, 15_0, 16_0, 17_0, 18_0, 19_0, 20_0, 21_0, 22_0\}$$

$$P_2 = P_1^{\sigma} = \{1_0, 2_1, 3_2, 4_3, 5_4, 6_5, 7_6, 8_7, 9_8, 10_9, 11_{10}, 12_{10}, 13_1, 14_3, 15_5, 16_7, 17_9, 18_0, 19_2, 20_4, 21_6, 22_8\}$$

$$P_3 = P_2^{\sigma} = \{1_0, 2_2, 3_4, 4_6, 5_8, 6_{10}, 7_1, 8_3, 9_5, 10_7, 11_9, 12_7, 13_0, 14_4, 15_8, 16_1, 17_5, 18_9, 19_2, 20_6, 21_{10}, 22_3\}$$

$$P_4 = P_3^{\sigma} = \{1_0, 2_3, 3_6, 4_9, 5_1, 6_4, 7_7, 8_{10}, 9_2, 10_5, 11_8, 12_2, 13_8, 14_3, 15_9, 16_4, 17_{10}, 18_5, 19_0, 20_6, 21_1, 22_7\}$$

$$P_5 = P_4^{\sigma} = \{1_0, 2_4, 3_8, 4_1, 5_5, 6_9, 7_2, 8_6, 9_{10}, 10_3, 11_7, 12_6, 13_3, 14_0, 15_8, 16_5, 17_2, 18_{10}, 19_7, 20_4, 21_1, 22_9\}$$

$$P_6 = P_5^{\sigma} = \{1_0, 2_5, 3_{10}, 4_4, 5_9, 6_3, 7_8, 8_2, 9_7, 10_1, 11_6, 12_8, 13_7, 14_6, 15_5, 16_4, 17_3, 18_2, 19_1, 20_0, 21_{10}, 22_9\}$$

$$P_7 = P_6^{\sigma} = \{1_0, 2_6, 3_1, 4_7, 5_2, 6_8, 7_3, 8_9, 9_4, 10_{10}, 11_5, 12_8, 13_9, 14_{10}, 15_0, 16_1, 17_2, 18_3, 19_4, 20_5, 21_6, 22_7\}$$

$$P_8 = P_7^{\sigma} = \{1_0, 2_7, 3_3, 4_{10}, 5_6, 6_2, 7_9, 8_5, 9_1, 10_8, 11_4, 12_6, 13_9, 14_1, 15_4, 16_7, 17_{10}, 18_2, 19_5, 20_8, 21_0, 22_3\}$$

$$P_9 = P_8^{\sigma} = \{1_0, 2_8, 3_5, 4_2, 5_{10}, 6_7, 7_4, 8_1, 9_9, 10_6, 11_3, 12_2, 13_7, 14_1, 15_6, 16_0, 17_5, 18_{10}, 19_4, 20_9, 21_3, 22_8\}$$

$$P_{10} = P_9^{\sigma} = \{1_0, 2_9, 3_7, 4_5, 5_3, 6_1, 7_{10}, 8_8, 9_6, 10_4, 11_2, 12_7, 13_3, 14_{10}, 15_6, 16_2, 17_9, 18_5, 19_1, 20_8, 21_4, 22_0\}$$

$$P_{11} = P_{10}^{\sigma} = \{1_0, 2_{10}, 3_9, 4_8, 5_7, 6_6, 7_5, 8_4, 9_3, 10_2, 11_1, 12_{10}, 13_8, 14_6, 15_4, 16_2, 17_0, 18_9, 19_7, 20_5, 21_3, 22_1\}$$

$$P_{12} = \{1_0, 2_5, 3_9, 4_1, 5_3, 6_4, 7_4, 8_3, 9_1, 10_9, 11_5, 12_0, 13_2, 14_8, 15_7, 16_{10}, 17_6, 18_6, 19_{10}, 20_7, 21_3, 22_2\}$$

$$P_{13} = P_{12}^{\sigma} = \{1_0, 2_6, 3_0, 4_4, 5_7, 6_9, 7_{10}, 8_{10}, 9_9, 10_7, 11_4, 12_1, 13_1, 14_5, 15_2, 16_3, 17_8, 18_6, 19_8, 20_3, 21_2, 22_5\}$$

$$P_{14} = P_{13}^{\sigma} = \{1_0, 2_7, 3_2, 4_7, 5_0, 6_3, 7_5, 8_6, 9_6, 10_5, 11_3, 12_4, 13_2, 14_4, 15_{10}, 16_9, 17_1, 18_8, 19_8, 20_1, 21_9, 22_{10}\}$$

$$P_{15} = P_{14}^{\sigma} = \{1_0, 2_8, 3_4, 4_{10}, 5_4, 6_8, 7_0, 8_2, 9_3, 10_3, 11_2, 12_9, 13_5, 14_5, 15_9, 16_6, 17_7, 18_1, 19_{10}, 20_1, 21_7, 22_6\}$$

$$P_{16} = P_{15}^{\sigma} = \{1_0, 2_9, 3_6, 4_2, 5_8, 6_2, 7_6, 8_9, 9_0, 10_1, 11_1, 12_5, 13_{10}, 14_8, 15_{10}, 16_5, 17_4, 18_7, 19_3, 20_3, 21_7, 22_4\}$$

$$P_{17} = P_{16}^{\sigma} = \{1_0, 2_{10}, 3_8, 4_5, 5_1, 6_7, 7_1, 8_5, 9_8, 10_{10}, 11_0, 12_3, 13_6, 14_2, 15_2, 16_6, 17_3, 18_4, 19_9, 20_7, 21_9, 22_4\}$$

$$P_{18} = P_{17}^{\sigma} = \{1_0, 2_0, 3_{10}, 4_8, 5_5, 6_1, 7_7, 8_1, 9_5, 10_8, 11_{10}, 12_3, 13_4, 14_9, 15_7, 16_9, 17_4, 18_3, 19_6, 20_2, 21_2, 22_6\}$$

$$P_{19} = P_{18}^{\sigma} = \{1_0, 2_1, 3_1, 4_0, 5_9, 6_6, 7_2, 8_8, 9_2, 10_6, 11_9, 12_5, 13_4, 14_7, 15_3, 16_3, 17_7, 18_4, 19_5, 20_{10}, 21_3, 22_{10}\}$$

$$P_{20} = P_{19}^{\sigma} = \{1_0, 2_2, 3_3, 4_3, 5_2, 6_0, 7_8, 8_4, 9_{10}, 10_4, 11_8, 12_9, 13_6, 14_7, 15_1, 16_{10}, 17_1, 18_7, 19_6, 20_9, 21_5, 22_5\}$$

$$P_{21} = P_{20}^{\sigma} = \{1_0, 2_3, 3_5, 4_6, 5_6, 6_5, 7_3, 8_0, 9_7, 10_2, 11_7, 12_4, 13_{10}, 14_9, 15_1, 16_8, 17_8, 18_1, 19_9, 20_{10}, 21_4, 22_2\}$$

$$P_{22} = P_{21}^{\sigma} = \{1_0, 2_4, 3_7, 4_9, 5_{10}, 6_{10}, 7_9, 8_7, 9_4, 10_0, 11_6, 12_1, 13_5, 14_2, 15_3, 16_8, 17_6, 18_8, 19_3, 20_2, 21_5, 22_1\}$$

REFERENCES

1. Z. Janko, T. van Trung, Two new semi-biplanes, Journ. of Comb. Theory Series A(1982)

2. K. Horvatić-Baldasar, The elation semi-biplane with 14 points on a line (to appear)

3. D. R. Hughes, Biplanes and semi-biplanes, Lecture Notes p.p.55-58, Comb. Math. Proc., Springer Camberra 1977.

4. D. R. Hughes, On designs, Lecture Notes in Math. Nr.893 Geometries and Groups Proc., Springer Berlin 1981.

Dr Ksenija Horvatić-Baldasar
Fakultet strojarstva i brodogradnje
Sveučilišta u Zagrebu
41000 Zagreb, Đ. Salaja 5

СИСТЕМА АВТОМАТИЧЕСКОГО ДОКАЗАТЕЛЬСТВА ТЕОРЕМ С РЕЗОЛЮЦИЕЙ, ИНДУКЦИЕЙ И СИММЕТРИЕЙ

Петар Хотомски

Резюме. Приводятся сведенья о вполне автоматизированой програм мной системе предназначеной для доказательства теорем на языке исчисления предикатов I порядка. Доказательство в форме опровер жения обоснованно на следующих правилах вывода: упорядоченая линейная резолюция с маркированными литерами, правило бинарной индукции и правило симметрии. Система работает в составе систе мы "Граф" разработаной на Электротехническом факултете Белград ского университета. Приводится пример доказательства на машине PDP 11/34 с использованием правил резолюции и симметрии.

Входными данными системы "Граф" /см. в [4], [5], [6], [7]/ являются предложения английского языка, либо формулы исчисления предикатов I порядка. Отдельные программные модули переводят предложения английского языка в формулы исчисления предикатов, а затем каждую из них переводят в множество дизьюнктов, при чем элиминируются кванторы и вводятся функции Сколема. Входными данными вполне автоматизированой системы доказательства явля ются дизьюнкты порожденные из отрицания предложения подлежаще го доказательству, а также и дизьюнкты порожденные из аксиом теории I порядка, либо из ранее доказанных теорем, лемм или из определений. Дизьюнкты происходящие из схемы-аксиом математиче ской индукции либо симметрии не включаются в исходное множест во, так как эти схемы замещенны правилами бинарной индукции и симметрии.

Упорядоченая линейная резолюция с маркированными литера ми /см. в [1] / использованна в системе благодаря следующим ха рактеристикам: I В резолюцию поступает только последняя литера дизьюнкта D_1 , называемого "центральным" и к-тая /к$\geq$1 / литера дизьюнкта D_2 называемого "боковым". II Она включает стратегию множества поддержки и устранения тавтологий. III Благодаря за держиванию маркированных литерь в порожденных резольвентах до статочно запоминать только дизьюнкты порожденные на промежуто чных-соседних уровнях поиска. Следующий пример илюстрирует про цесс отыскания упорядоченой линейной резольвенты центрального дизьюнкта D_1 и бокового дизьюнкта D_2 .

Пример. D_1: $P(x)/Q(x)/R(x)T(x)$ D_2: $\neg R(x)\neg T(x)P(x)$[1].

1^o переименование переменных: D_2 становится $\neg R(y)\neg T(y)P(y)$

2^o отыскание найболее общего унификатора НОУ для $T(x)$ и к-той (к=1,2,3) литеры в D_2 : для к=2 НОУ существует и имеет вид $\theta=\{y/x\}$.

3^o оформление резольвенты: $P(y)/Q(y)/R(y)/T(y)\neg R(y)P(y)$

4^o сжатие резольвенты - стирание немаркированных литерь совпа дающих с предшествующими с лева литерами и иследование на тавтологию: $P(y)/Q(y)/R(y)/T(y)\neg R(y)$

5^o сокращение резольвенты - стирание маркированных литерь за которими нет немаркированных: таких пока в нашем примере нет

6^o стирание последних литерь комплементарных /по отношению к от рицанию/ к некоторой предшествующей маркированной литере по унификатору λ : для $\lambda=\emptyset$ получается $P(y)/Q(y)/R(y)/T(y)$

7^o к λ-примеру полученному в 6^o применяются шаги 5^o и 6^o пока по следняя литера не окажется не маркированной либо резольвента не окажется пустым дизьюнктом. В нашем примере упорядоченая ли нейная резольвента имеет окончательный вид: $P(y)$.

В системе использованно следующее правило бинарной индукции /подробнее см. в [2] и [3] /:

Из центрального дизьюнкта D_1 вида $C_1 V A$ и бокового дизьюнкта D_2 вида $\neg B V C_2$ где A и B литеры, C_1 и C_2 дизьюнкты, не содер жащих общих переменных и таких что существует подстановка σ дающая σ-примери вида $A_\sigma = L_x(0)$ и $B_\sigma = L_x(t)$ (либо $A_\sigma = L_x(t)$ и $B_\sigma = L_x(0)$), при чем $L_x(t)$ литера получена из $L(x)$ замещением каждого вхождения переменной x на терм t который свободен для x в $L(x)$, выводятся дизьюнкты:

$$C_{1\sigma} V C_{2\sigma} V L_x(g(z_1,..,z_s)) \quad ; \quad C_{1\sigma} V C_{2\sigma} V \neg L_x(Sg(z_1,..,z_s))$$

Символ дизьюнкции в дизьюнктах между литерами опускается. Символ "/" в дизьюнкте маркирует следующую за ним литеру.

где g новая функция Сколема s аргумментов; $z_1,\dots,z_s$ все различные переменные в литере $L_x(0)$; S сукцессор. Первый из них запоминается в качестве центрального дизьюнкта для следующего уровня, а другой записывается в исходное множество боковых дизьюнктов. Правило бинарной индукции применяется только если правило упорядоченой линейной резолюции к дизьюнктам D_1 и D_2 не применимо.

Пример. D_1: $P(x)Q(0,h(y))$ D_2: $\neg Q(f(y),z)R(z)$

1^o переименнование переменных: D_2 становится $\neg Q(f(y_1),z)R(z)$

2^o определение подстановки 1) $\sigma = \{h(y)/z\}$

3^o определение σ-примеров: $D_{1\sigma}$: $P(x)Q(0,h(y))$

$D_{2\sigma}$: $\neg Q(f(y_1),h(y))R(h(y))$

4^o порождение индуцированных дизьюнктов:

$P(x)R(h(y))Q(g(y),h(y))$; $P(x)R(h(y))\neg Q(Sg(y),h(y))$

Правило симметрии

Если к исходному множеству принадлежит дизьюнкт выражающий аксиому симметрии: $\neg R(x,y) \vee R(y,x)$, то он приводит к порождению лишних дизьюнктов которые "загрязняют" пространство поиска. Поэтому в системе использованно следующее процедуральное правило симметрии:

К центральному дизьюнкту вида $C \vee R(t_1,t_2)$, где t_1,t_2 терми, C дизьюнкт, применяются следующие трансформации:

1^o перемещение термов t_1 и t_2 : $C \vee R(t_2,t_1)$

2^o применение шагов 4^o–7^o применяемых при отысканию линейной упорядоченой резольвенты.

Пример. D_1: $P(x)/\neg R(f(x),y)/Q(z)R(0,z)$

1^oперемещение термов: $P(x)/\neg R(f(x),y)/Q(z)R(z,0)$

2^oсжатие не применимо ; 3^o сокращение не применимо

4^o стирание последней литеры комплементарной маркированной:

для $\lambda=\{f(x)/z,0/y\}$ получается $P(x)/\neg R(f(x),0)/Q(f(x))$

5^o сокращение: $P(x)$

Далнейшее стирание не применимо, поэтому дизьюнкт порожден по правилу симметрии имеет окончательный вид: $P(x)$.

1) НОУ для $Q(0,h(y))$ и $Q(f(y_1),z)$ не существует. Подстановка определяется по оссобому алгоритму описанному в [3] .

Если считать что R является любым бинарным предикатным символом, то правило симметрии заменяет схему-аксиом симметрии.Кроме того, в системе предусмотрена возможность применять правило симметрии только к тем бинарным предикатам которые зафиксированны в качес тве симметрических, а не к каждому бинарному предикату.

Пользователь системи может выбрать один из следующих режи мов работы: только резолюция, резолюция и симметрия, резолюция и индукция, резолюция,индукция и симметрия.

В режиме с резолюцией, индукцией и симметрией для определе ного центрального и бокового дизьюнкта порождаются дизьюнкты по правилу линейной упорядоченой резолюции либо бинарной индукции, а затем к центральному дизьюнкту применяется правило симметрии. Если правило симметрии применимо, то порожденный дизьюнкт стано вится новым центральным дизьюнктом для применения правил резолю ции либо индукции на следующем уровне поиска. Все дизьюнкты поро жденные на одном уровне по указаным правилам запоминаются до сле дующего уровня на котором используются по очереди в качестве но вых центральных дизьюнктов.На каждом уровне боковыми дизьюнкта ми по очереди являются дизьюнкты исходного множества.
Начальный центральный дизьюнкт берется из множества дизьюнктов происходящих из отрицания предложения подлежащего доказательст ву. Это достаточно для нахождения опровержения если оно сущест вует, в противном поиск в общем случае превращается в бесконеч ную процедуру и переривается в моменте исчерпания предназначен ых ресурсов памяти машины. Опровержение найдено если на некото ром уровне порожден пустой дизьюнкт.

На выходе получается доказательство в форме отпечатаного опровержения, при чем печатаются только дизьюнкты принадлежащие опровержению, либо сообщение о невозможности опровержения в пред назначенных размерах запоминающего устройства. Предусмотренна также возможность наложить ограничения на длину литерь, длину дизьюнктов и количество дизьюнктов порождаемых на каждом уров не. Дизьюнкты превосходящие эти ограничения не порождаются. Использованные ограничения можно считать удовлетворительными так как система включена в интерактивную систему доказательства которая обоснованна на идеях естественного вывода и разбиения задач на менее сложные подзадачи.

Полные сведенья о том как работает система "Граф" можно получить из [8]. Сдесь отметим только условия перехода из интерактивной к вполне автоматизированой системе доказательства в рамках системи "Граф". Упомянутый переход предусмотрен в том и только в том случае когда формула исчисления предикатов приведенна к импликативной форме $F_1 \Rightarrow F_2$, при чем все предикатные буквы принадлежащие правой части F_2 существуют и в левой части F_1.
Конечно, когда вполне автоматизированая система доказательства используется самостоятельно и независимо от системи "Граф", то эти предположения не обязаны.

Пример отладки на ЭВМ [1)]

Аксиомы: 1. $\forall x \forall y (R(x,y) \Rightarrow R(y,x))$
2. $\forall x \forall y (R(x,y) \wedge R(y,z) \Rightarrow R(x,z))$
3. $\neg \forall x \forall y R(x,y)$

Утверждение: $\forall x \forall y (R(x,y) \Rightarrow \exists z (\neg R(x,z) \wedge \neg R(y,z)))$

Сколемизированое отрицание утверждения: $R(a,b) \wedge (R(a,z) \vee R(b,z))$
a , b – константы Сколема.

Исходное множество дизьюнктов:
1. $R(a,b)$
2. $R(a,z) \vee R(b,z)$
3. $\neg R(m,n)$ из аксиомы 3 ; m,n – константы Сколема
4. $\neg R(y,z) \vee \neg R(x,y) \vee R(x,z)$ из аксиомы 2.

Дизьюнкт происходящий из аксиомы симметрии не нужен.
Начальный дизьюнкт: $R(a,z) \vee R(b,z)$
Режим работы: упорядоченая линейная резолюция с правилом симметрии, без индукции.
Полученно следующее опровержение исходного множества дизьюнктов в виде линейного вывода пустого дизьюнкта /приводим его в переводе с английского языка/:

ДОКАЗАТЕЛЬСТВО НАЙДЕНО
ОПРОВЕРЖЕНИЕ СОСТОИТ ИЗ СЛЕДУЮЩЕЙ ПОСЛЕДОВАТЕЛЬНОСТИ:
ЦЕНТРАЛЬНЫЙ ДИЗЬЮНКТ: $R(a,z)R(b,z)$
БОКОВОЙ ДИЗЬЮНКТ: $\neg R(y,z_1)\neg R(x,y)R(x,z_1)$ 4. в исходном множ.
НОУ: $b/y, z/z_1$
ЦЕНТРАЛЬНЫЙ ДИЗЬЮНКТ: $R(a,z)/R(b,z)\neg R(x,b)R(x,z)$
БОКОВОЙ ДИЗЬЮНКТ: $\neg R(m,n)$ 3. в исходном множ.
НОУ: $m/x, n/z$

---

1) **Пример подсказал Д. Цветкович**

ЦЕНТРАЛЬНЫЙ ДИЗЪЮНКТ: R(a,n)/R(b,n)ㄱR(m,b)
действовала операция сокращения
R(a,n)/R(b,n)ㄱR(b,m)
действовало правило симметрии
БОКОВОЙ ДИЗЪЮНКТ: R(a,z)R(b,z) 2. в исходном множ.
НОУ: m/z
ЦЕНТРАЛЬНЫЙ ДИЗЪЮНКТ: R(a,n)/R(b,n)/ㄱR(b,m)R(a,m)
БОКОВОЙ ДИЗЪЮНКТ:ㄱR(y,z)ㄱR(x,y)R(x,z) 4. в исходном множ.
НОУ: a/y,m/z

ЦЕНТРАЛЬНЫЙ ДИЗЪЮНКТ: R(a,n)/R(b,n)/ R(b,m)/R(a,m)ㄱR(b,a)
действовала операция сжатия ,λ =a/x
R(a,n)/R(b,n)/ㄱR(b,m)/R(a,m)ㄱR(a,b)
действовало правило симметрии
БОКОВОЙ ДИЗЪЮНКТ: R(a,b) 1. в исходном множестве
НОУ: пустая подстановка
ЦЕНТРАЛЬНЫЙ ДИЗЪЮНКТ: R(a,n) действовала операция сокращения
БОКОВОЙ ДИЗЪЮНКТ:ㄱR(y,z)ㄱR(x,y)R(x,z) 4. в исходном множ.
НОУ: a/y,n/z
ЦЕНТРАЛЬНЫЙ ДИЗЪЮНКТ: /R(a,n)ㄱR(x,a)R(x,n)
БОКОВОЙ ДИЗЪЮНКТ: ㄱR(m,n) 3. в исходном множ.
НОУ: m/x
ЦЕНТРАЛЬНЫЙ ДИЗЪЮНКТ: /R(a,n)ㄱR(m,a)
действовала операция сокращения
/R(a,n)ㄱR(a,m)
действовало правило симметрии
БОКОВОЙ ДИЗЪЮНКТ: R(a,z)R(b,z) 2. в исходном множ.
НОУ: m/z
ЦЕНТРАЛЬНЫЙ ДИЗЪЮНКТ: /R(a,n)/ㄱR(a,m)R(b,m)
БОКОВОЙ ДИЗЪЮНКТ:ㄱR(y,z)ㄱR(x,y)R(x,z) 4. в исходном множ.
НОУ: b/y,m/z
ЦЕНТРАЛЬНЫЙ ДИЗЪЮНКТ: /R(a,n)/ㄱR(a,m)/R(b,m)ㄱR(a,b)
действовала операция сжатия, λ =a/x
БОКОВОЙ ДИЗЪЮНКТ: R(a,b) 1.в исходном множ.
НОУ: пустая подстановка
ЦЕНТРАЛЬНЫЙ ДИЗЪЮНКТ: ПУСТОЙ ДИЗЪЮНКТ действ.опер.сокращения
ДОКАЗАТЕЛЬСТВО ОТПЕЧАТАНО
ДОКАЗАНА НЕВЫПОЛНИМОСТЬ ИСХОДНОГО МНОЖЕСТВА

Примечание: В процессе опровержения символ дизьюнкции не пишется. Каждый центральный дизьюнкт, кроме начального, является упорядоченой линейной резольвентой предшествующего центрального и бокового дизьюнкта, либо выведен из предшествующего центрального дизьюнкта по правилу симметрии. Символ "/" перед литерой маркирует стоящую за ним литеру.

ЛИТЕРАТУРА

Попов Э.В.,Фирдман Г.Р., Алгоритмические основы интеллектуальных роботов и искусственного интеллекта, Наука Москва 1976.

2. Хотомски П., Правило индукции в доказательствах опровержением с применением к автоматическому доказательству теорем, Publication de l'Institut mathematique, tome 31(45), Beograd 1982.

3. Хотомски П., Способ встроения правила индукции в процедури автоматического доказательства теорем с резолюцией, Publication de l'Institut mathematique, tome 33(47), Beograd 1983.

4. D.M.Cvetković, A project for using computers in further development of graph theory, The Theory and Applications og Graphs, Proc. of the 4th Internat. Conf. on the Theory and Application of Graphs. Kolomazo 1980, Wiley 1981, 285-296.

5. D.M.Cvetković, L.L.Kraus, S.K.Simić, Discussing graph theory with a computer I, Implementation of graph theoretic algorithms, Univ. Beograd, Publ. Elektrotehn.Fak.,Serija Mat.Fiz.N° 716-734 1981.

6. D.M.Cvetković, Discussing graph theory with a computer II, Theorems suggested by the computer,Publication de l'Institut mathematique, tome 33(47), Beograd 1983.

7. D.M.Cvetković,I.Pevac, Discussing graph theory with a computer III, Man-machine theorem proving, Publ.Inst.Math.(Beograd) 34(48)1983,37-47.

8. Cvetković D.,Kraus L.,"Graph" an expert system for the classification and extension of the knoulendge in the field of graph theory,User's Manual, Elektrotehnički fakultet, Beograd,1983.

Pedagoška Akademija
Sremska Mitrovica
Yugoslavia

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", ZAGREB 1984

SOME CONNECTIONS BETWEEN FINITE SEPARABILITY PROPERTIES OF AN n-SEMIGROUP AND ITS UNIVERSAL COVERING

Biljana Janeva

Abstract. It is known that for any n-semigroup there exists a universal covering semigroup, and there is a connection between some properties of an n-semigroup and its universal covering. In this paper such a connection for finite separability properties is studied. It is proved that:

1. If a covering semigroup $\underline{Q}'$ of an n-semigroup $\underline{Q}$ is residually finite, then $\underline{Q}$ is residually finite as well.

2. If a cancellative n-semigroup $\underline{Q}$ is residually finite, then the cancellative universal covering semigroup $\underline{Q}^{\sim}$ is residually finite as well.

3. If the universal covering group $\underline{Q}^{\wedge}$ of an n-group $\underline{Q}$ has the finite separability property , so does $\underline{Q}$.

As a consequence of these results, the results given in [3] , some known results for n-semigroups, and the fact that finite separability properties imply solvability of algorithmic problems, some n-semigroup classes with solvable algorithmic problems are obtained.

1. Preliminary definitions

An n-semigroup is an algebra $(Q,[\ ])$ with an associative n-ary operation $[\ ]:(x_1,x_2,\dots,x_n)\mapsto [x_1x_2\dots x_n]$. Then the semigroup $\underline{Q}^{\wedge}$ given by the following presentation (in the class of all semigroups)

$$\langle Q;\ \{a=a_1a_2\dots a_n \mid a=[a_1a_2\dots a_n] \text{ in } \underline{Q}\}\rangle \tag{1}$$

is called the universal covering semigroup of $\underline{Q}$. It can be assumed that $Q\subseteq Q^{\wedge}$, moreover, Q is a generating subset of $\underline{Q}^{\wedge}$ and any element $u\in Q^{\wedge}$ has a form $u=a_1a_2\dots a_i$, where

$1 \leqslant i < n$, $a_\nu \in Q$, and $i = |u|$ is uniquely determined by u. If $\underline{P}$ is an n-subsemigroup of $\underline{Q}$ then there is a (unique) homomorphism $\lambda : \underline{P}^\wedge \to \underline{Q}^\wedge$ such that $\lambda(p) = p$, for any $p \in P$. $\underline{P}$ is said to be compatible in $\underline{Q}$ if λ is injective, and then we can assume $\underline{P}^\wedge$ to be a subsemigroup of $\underline{Q}^\wedge$ ([1]).

A cancellative n-semigroup is an n-semigroup which satisfy the cancellative laws. Then the semigroup $\underline{Q}^\sim$ given by the presentation (1) (in the class of cancellative semigroups) is called the universal cancellative covering semigroup of $\underline{Q}$. We note that $a_1 a_2 \ldots a_i = b_1 b_2 \ldots b_i$ in $\underline{Q}$ iff $[a^{n-i} a_1 \ldots a_i] = [a^{n-i} b_1 \ldots b_i]$ in $\underline{Q}$, for each $a \in Q$.

An n-semigroup $(Q, [\ ])$ is called an n-group if $(\forall a_1, \ldots, a_n \in Q)(\exists x, y \in Q)\,[x a_1 \ldots a_{n-1}] = a_n,\ [a_1 \ldots a_{n-1} y] = a_n$, or equivalently, if $\underline{Q}^\wedge$ is a group. An n-group $\underline{Q}$ is a cancellative n-semigroup and $\underline{Q}^\sim = \underline{Q}^\wedge$.

We note that every n-subgroup $\underline{P}$ of an n-semigroup $\underline{Q}$ is compatible in $\underline{Q}$ ([1]).

2. Some connections between finite separability properties of an n-semigroup and its universal covering

Let $\mathcal{K}$ be a class of n-semigroups and $\underline{Q} \in \mathcal{K}$.

DEFINITION 1. $\underline{Q}$ is said to be residually finite in $\mathcal{K}$ if for each $x, y \in Q, x \neq y$, there is a surjective homomorphism φ from $\underline{Q}$ to a finite n-semigroup of $\mathcal{K}$ such that $\varphi(x) \neq \varphi(y)$.

DEFINITION 2. $\underline{Q}$ is said to have the finite separability property in $\mathcal{K}$ if for each $x \in Q$, and n-subsemigroup $\underline{P}$ of $\underline{Q}$, $x \notin P$, there is a surjective homomorphism φ from $\underline{Q}$ to a finite n-semigroup of $\mathcal{K}$, such that $\varphi(x) \notin \varphi(\underline{P})$.

Replaceing the words "n-semigroup","n-subsemigroup" by "n-group", "n-subgroup" respectively, we obtain the corresponding classes of n-groups.

Remark In the propositions below by a residually finite n-semigroup we will always mean a residually finite n-semigroup in a class of n-semigroups. The cinsidered class of n-semigroups will be clearly understood by the context.

PROPOSITION 2.1. If a covering semigroup $\underline{Q}'$ 1) of an n-semigroup $\underline{Q}$ is residually finite, then $\underline{Q}$ is residually finite as well.

1) $\underline{Q}'$ is a covering semigroup of an n-semigroup $\underline{Q}$ is Q is a generating subset of Q' and $[x_1 \ldots x_n] = x_1 \ldots x_n$ for any $x_\nu \in Q$.

Proof: Let a,b be two distinct elements of $\underline{Q}$. Then $a \neq b$ in $\underline{Q}'$, and, by the assumtion, there is a surjective homomorphism $\varphi : \underline{Q}' \to \underline{S}$, such that $\underline{S}$ is a finite semigroup and $\varphi(a) \neq \varphi(b)$. If we put $\psi = \varphi_Q$ and $\underline{T} = \psi(\underline{Q})$, then $(T,[\,])$ is a finite n-semigroup where $[x_1 \dots x_n] = x_1 \dots x_n$, and, thus, $\psi : \underline{Q} \to \underline{T}$ is a surjective homomorphism such that $\psi(a) \neq \psi(b)$. □

It is not known whether the residual finitness of an n-semigroup $\underline{Q}$ induces the corresponding property for its universal covering. We will show, now, that we have the positive answer if we consider the class of cancellative n-semigroups and its cancellative universal covering semigroup.

PROPOSITION 2.2. If a cancellative n-semigroup $\underline{Q}$ is residually finite, then the cancellative universal covering semigroup $\underline{Q}$ is residually finite as well.

Proof: Let $a \neq b$, $a = a_1 \dots a_i, b = b_1 \dots b_j \in \underline{Q}^\sim$, $a_\nu, b_\lambda \in Q$, $1 \leq i \leq j < n$. If $i \neq j$ then $|\,| : c \mapsto |c|$ is a surjective homomorphism from $\underline{Q}^\sim$ to $(Z_n,+)$ such that $|a| \neq |b|$. Assume, now, that $i=j$. Then $a' = [a_1^{n-i} a_1 \dots a_i] \neq [a_1^{n-i} b_1 \dots b_i] = b'$, and, thus, there is a surjective homomorphism ψ from $\underline{Q}$ into a finite cancellative n-semigroup $\underline{S}$, such that $\psi(a') \neq \psi(b')$. Then ψ induces a surjective homomorphism $\psi^\sim : \underline{Q}^\sim \to \underline{S}^\sim$, where $\underline{S}^\sim$ is a finite cancellative semigroup. Moreover, we have $\psi^\sim(a) \neq \psi^\sim(b)$, for if $\psi^\sim(a) = \psi^\sim(b)$, then $\psi(a') = \psi(a_1^{n-i} a_1 \dots a_n) = \psi(a_1)^{n-i} \psi^\sim(a_1 \dots a_i) = \psi(a_1)^{n-i} \psi^\sim(b_1 \dots b_i) = \psi(b')$. □

As a consequence of these two properties we obtain:

COROLLARY 2.3. The universal covering group $\underline{Q}^\wedge$ of an n-group $\underline{Q}$ is residually finite iff $\underline{Q}$ is residually finite. □

As for the finite separability properties we have the following results.

PROPOSITION 2.4. If the universal covering group $\underline{Q}^\wedge$ of an n-group $\underline{Q}$ has the finite separability property, then $\underline{Q}$ also has the finite separability property.

Proof: Let $\underline{P}$ be an n-subgroup of $\underline{Q}$ and $x \in Q \setminus P$. Then $\underline{P}^\wedge$ is a subgroup of $\underline{Q}^\wedge$ and $x \notin P^\wedge$. Therefore, if $\underline{Q}^\wedge$ has the finite separability property then there is a finite group $\underline{G}$ and a surjective homomorphism $\varphi : \underline{Q}^\wedge \to \underline{G}$ such that $\varphi(x) \notin \varphi(\underline{P}^\wedge)$.

The restriction $\varphi_Q = \Psi$ of φ on Q is a surjective homomorphism from $\underline{Q}$ into a finite n-group $\Psi(\underline{Q})=\underline{G}'$ and $\Psi(x) \notin \Psi(\underline{P}) \subseteq \varphi(\underline{P}^\wedge)$.□

PROPOSITION 2.5. If each n-subsemigroup of an n-semigroup $\underline{Q}$ is compatible in $\underline{Q}$, and the universal covering semigroup $Q^\wedge$ has the finite separability property, then $\underline{Q}$ also has the finite separability property.

Proof: The proof is the same as the proof of 2.4.□

3. Some n-semigroup classes with solvable algorithmic problems

Certain connections between the finite separability properties and solvability of algorithmic problems are given in [3]. To be able to state them for n-semigroup classes, let me note that if $\mathcal{P}$ is a property for n-semigroups, then a class $\mathcal{K}$ of n-semigroups is a $\mathcal{P}$-class if each finitely presented member of $\mathcal{K}$ has the property $\mathcal{P}$. Now, if a class $\mathcal{K}$ of n-semigroups is residually finite (has the finite separability property), then $\mathcal{K}$ has a solvable word problem (has a solvable generalized word problem).

Also, a table of some varieties and classes with solvable algorithmic problems and with some finite separability properties is given in [3]. Among others, the following results are given:

(i) The variety of commutative groups (commutative semigroups) is residually finite.

(ii) The class of free groups (free semigroups, free commutative semigroups) has the finite separability property.

Using these results, the results given in 2., as well as known results for n-semigroups and n-groups, some corollaries are obtained.

COROLLARY 3.1. The variety of commutative n-groups is residually finite.□

COROLLARY 3.2. The variety of commutative n-semigroups is residually finite.

Proof: Let $\underline{Q}$ be a finitely presented n-semigroup. The semigroup $\underline{Q}'$ given by the presentation (1)(in the class of commutative semigroups) is the universal commutative covering semigroup of Q ([7]). Q′ is finitely generated commutative semigroup, so ([5],Th 9.28, pg.172, II) it is finitely presented and is residually finite. Now, by 2.1, Q is residually finite as well.□

COROLLARY 3.3. *The class of free n-groups has the finite separability property.*□

Using the connections between finite separability properties and solvability of algorithmic problems, it follows immediately that:

1) The variety of commutative n-groups (commutative n-semigroups) has a solvable word problem.

2) The class of free n-groups has a solvable generalized word problem.

Remark: The result 1) could be obtained as a direct consequence of the results in [2] for connections between solvability of the word problem in n-semigroups (n-groups) and their universal covering. It could be proved that: if Q^ is the universal covering group of an n-group Q with solvable generalized word problem, then Q has a solvable generalized word problem as well.The proof of this last property essentially uses the fact that each n-subgroup of Q is compatible in Q, so this result could be proved for n-semigroups in which each n-subsemigroup is compatible.

REFERENCES

1. G.Čupona, N.Celakoski, *On representations of n-assiciatives into semigroups*, MANU, Contributions VI. 2 (1974) 23-34
2. G.Čupona, N.Celakoski, *Polyadic subsemigroups of semigroup*, Algebraic Conference Skopje (1980) 131-152
3. T.Evans, *Word problems*, Word problem II, North Holland (1980) 87-100
4. B.Janeva, *Word problem for n-groups*, Proc. Sym. n-ary structures, Skopje (1982) 157-160
5. А.Клиффорд, Г.Престон, *Алгебраическая теория полугрупп*, I,II, "Мир" Москва 1972 (превод)
6. R.Lyndon, P.Schupp, *Combinatorial group theory*, Springer-Verlag, New York 1977
7. Ѓ.Чупона, *Полугрупи генерирани од асоцијативи*, Год. Зб. на ПМФ Скопје, 15(1964)5-25

Biljana Janeva
Matematički Fakultet-Skopje
"Pirinska" bb
91000 S k o p j e

PROCEEDINGS OF THE CONFERENCE „ALGEBRA AND LOGIC", ZAGREB 1984

ON SOME CONGRUENCES ON FACTORIZABLE SEMIGROUPS

Vesna Kilibarda

Abstract. The purpose of this note is to describe some congruences on a factorizable semigroup S. A necessary and sufficient condition for (K, τ), with $K = K\omega$, to be a congruence pair for S is given (Theorem 1). Similary, a necessary and sufficient condition for any (K, τ) to be a congruence pair for a Clifford uniquely factorizable semigroup is given (Theorem 2).

First, we give some results about factorizable semigroups studied by Chen and Hsieh [1].[1)] An inverse semigroup S is called a <u>factorizable inverse semigroup</u> if there exist a subgroup G of S and a subset E of the set E_S of idempotents of S such that $S = GE$. Any factorizable semigroup has an identity, and if an inverse semigroup S is factorizable as $S = GE$, then $S = EG$, G is the unit group of S, and $E = E_S$.

1) All undefined terminology can be found in [2] .

RESULT 1. [1] *Let S be a semigroup. Up to isomorphism, the following statements are equivalent:*

(i) S is the direct product $G \times E$ of a group G and a semilattice E with the greatest element.

(ii) S is a Clifford semigroup $\mathcal{S}(Y; G_\alpha, \varphi_{\alpha,\beta})$ such that every $\varphi_{\alpha,\beta}$ is an isomorphism and Y is a semilattice with the greatest element.

(iii) S is factorizable as GE_S for some subgroup G of S, such that every $e \in E_S$ is uniquely represented in the form 1e, where 1 is the identity of G, and $ge=eg$, for all $e \in E_S$ and $g \in G$.

If S is semigroup described in Result 1, every $s \in S$ is uniquely represented in the form ge, with $g \in G$ and $e \in E_S$. Such a semigroup is called a Clifford uniquely factorizable semigroup.

Next we mention congruence pair and a characterization theorem for congruences on an inverse semigroup due to Petrich [3].

Let S be an inverse semigroup. For a congruence ρ on S the *kernel* and the *trace* of ρ is defined by

$\ker\rho = \{a \in S \mid (\exists e \in E_S)\ a \rho e\}$

$\operatorname{tr}\rho = \rho \mid E_S$

respectively. This associates to each congruence ρ on S the ordered pair $(\ker\rho, \operatorname{tr}\rho)$.

An inverse semigroup K of S is *normal* if it is full ($E_S \subseteq K$) and selfconjugate ($s^{-1}Ks \subseteq K$, for all $s \in S$). A congruence τ on the set E_S is *normal* if for any $e, f \in E_S$ and $s \in S$, $e\tau f$ implies $s^{-1}es\tau s^{-1}fs$.

DEFINITION 1. *The pair (K, τ) is a congruence pair for S if K is a normal subsemigroup of S, τ is a normal congruence on E_S and these two satisfy:*

(i) $ae \in K,\ e\tau a^{-1}a \Rightarrow a \in K$,

(ii) $a \in K \Rightarrow a^{-1}a\tau aa^{-1}$ $(a \in S,\ e \in E_S)$.

Using these concepts, we have the mentioned characterization theorem of congruences on an inverse semigroup.

RESULT 2.[3] Let S be an inverse semigroup. If (K,τ) is a congruence pair for S, then the relation $\rho_{(K,\tau)}$ on S defined by

$a\,\rho_{(K,\tau)}\,b \Leftrightarrow a^{-1}a\,\tau\,b^{-1}b,\ ab^{-1} \in K$

is the unique congruence ρ on S for which $\ker\rho = K$ and $\operatorname{tr}\rho = \tau$. Conversely, if ρ is a congruence on S, then $(\ker\rho, \operatorname{tr}\rho)$ is a congruence pair for S and $\rho_{(\ker\rho,\operatorname{tr}\rho)} = \rho$.

Now we describe congruence pairs on a Clifford semigroup.

RESULT 3.[3] Let $S = \mathcal{S}(Y;\ G_\alpha, \varphi_{\alpha,\beta})$ be a Clifford semigroup. The pair (K,τ) is a congruence pair for S if and only if $K = \mathcal{S}(Y;\ K_\alpha, \psi_{\alpha,\beta})$, where

(i) K_α is a normal subgroup of G_α, $\alpha \in Y$

(ii) $e_\alpha > e_\beta \Rightarrow K_\alpha\varphi_{\alpha,\beta} \subseteq K_\beta$

(iii) $\psi_{\alpha,\beta} = \varphi_{\alpha,\beta}|K$

(iv) τ is a congruence on E_S such that

$e_\alpha > e_\beta,\ e_\alpha\tau e_\beta \Rightarrow K_\beta\varphi_{\alpha,\beta}^{-1} \subseteq K_\alpha$.

If H is an arbitrary subset of an inverse semigroup S, the closure $H\omega$ of H is defined by $H\omega = \{x \in S \mid (\exists e \in E_S)\, xe \in H\}$ [2].

In the next theorem we give a description of congruence pair (K,τ) with $K = K\omega$ for a factorizable semigroup.

THEOREM 1. Let $S = GE_S$ be a factorizable semigroup, K a subset of S such that $K = K\omega$, and τ a congruence on E_S. Then (K,τ) is a congruence pair for S if and only if there exists a normal subgroup H of G such that $K = HE_S$, and

(1) $e\tau f \Rightarrow g^{-1}eg\,\tau\,g^{-1}fg$, for all $g \in G$, $e, f \in E_S$,

(2) $h^{-1}eh\,\tau\,e$, for all $h \in H$, $e \in E_S$.

Proof. Let $K = HE_S$, and the conditions (1) and (2) are satisfied. If $x, y \in K$, then there are $h_1, h_2 \in H$, $e_1, e_2 \in E_S$ such that $x = h_1 e_1$, $y = h_2 e_2$. So

$$xy = h_1 e_1 h_2 e_2 = h_1 1 e_1 h_2 e_2 = h_1 h_2 (h_2^{-1} e_1 h_2) e_2 \in HE_S$$

and

$$x^{-1} = e_1 h_1^{-1} = h_1^{-1}(h_1 e_1 h_1^{-1}) \in HE_S.$$

Hence, K is an inverse subsemigroup of S.

From $E_S = 1E_S \subseteq HE_S$ it follows that K is full.

Let $s \in S$ and $k \in K$. Then $s = ge$ and $k = hf$ for some $g \in G$, $h \in H, e, f \in E_S$. So $g^{-1}hg = h_1 \in H$, $g^{-1}fg = f_1 \in E_S$, and
$s^{-1}ks = eg^{-1}hfge = e(g^{-1}hg)(g^{-1}fg)e = eh_1 f_1 e = h_1(h_1^{-1}eh_1)f_1 e \in HE_S$.
Thus, K is a normal subsemigroup of S.

Suppose that $e, f \in E_S$, $s \in S$ and $e \tau f$. Then $s = ge_1$, for some $g \in G$ and $e_1 \in E_S$, and

$$s^{-1}es = e_1(g^{-1}eg)e_1 \tau e_1(g^{-1}fg)e_1 = s^{-1}fs,$$

by the condition (1). Hence, τ is a normal congruence on E_S.

Now we prove that conditions (i) and (ii) of Definition 1 are satisfied.

If $ae \in K$, then $a \in K\omega = K$, so the condition (i) holds. Let $a \in K$. Then $a = hf$, for some $h \in H$, $f \in E_S$, and we have

$$aa^{-1} = hffh^{-1} = hfh^{-1} \tau f = f1f = fh^{-1}hf = a^{-1}a$$

by (2), so the condition (ii) holds.

Thus, (K, τ) is a congruence pair for S.

Conversely, let (K, τ) be a congruence pair for S such that $K = K\omega$. We define the subset H of G by

$$H = \{g \in G \mid (\exists e \in E_S) ge \in K\}.$$

From $(\exists e \in E_S) ge \in K$ it follows $g \in K\omega = K$, so we have

$$H = \{g \in G / g \in K\} = G \cap K \subseteq K,$$

which yields $HE_S \subseteq KE_S \subseteq K$, since $E_S \subseteq K$, and $K^2 \subseteq K$. Since $K \subseteq HE_S$ by definition of H, it follows $K = HE_S$.

From $H = G \cap K$ we conclude that H is a subgroup of G.

Let $g \in G$ and $h \in H$. Then there is $e \in E_S$ such that $he \in K$, and $g^{-1}(he)g = (g^{-1}hg)(g^{-1}eg) \in K$, since K is self-conjugate in S. Hence $g^{-1}hg \in H$, by definition of H.

The conditions (1) and (2) follow immediately from the normality of τ and the condition (ii) of Definition 1, respectively. The theorem is proved.

The next theorem gives a simple characterization of a congruence pair for a Clifford uniquely factorizable semigroup.

THEOREM 2. Let $S = GE_S$ be a Clifford uniquely factorizable semigroup, K a subset of S and τ a congruence on E_S. The pair (K,τ) is a congruence pair for S if and only if there exists a normal subgroup H of S such that $K = HE_S$.

Proof. From Result 1. it follows that $S = \mathcal{S}(Y;\ G_\alpha, \varphi_{\alpha,\beta})$, $G_\alpha = Ge_\alpha \cong G1 = G$, where 1 is the greatest idempotent of S, $g\varphi_{1,\alpha} = ge_\alpha$, for every $g \in G$, $e_\alpha \in E_S$.

If $K = HE_S$, it follows that $K = \mathcal{S}(Y;\ K_\alpha, \psi_{\alpha,\beta})$ such that $K_\alpha = He_\alpha \cong H1 = H$, so the conditions (i) - (iv) of Result 3. are satisfied and (K,τ) is a congruence pair.

Conversely, if (K,τ) is a congruence pair for S, then $K = \mathcal{S}(Y;\ K_\alpha, \psi_{\alpha,\beta})$ and the condition (i) - (iv) of Result 3. are satisfied. Hence, $\psi_{\alpha,\beta}$ are isomorphisms and so $K_\alpha = He_\alpha$ for some normal subgroup H of G and $K = HE_S$. The theorem is proved.

R E F E R E N C E S

[1] Chen, S.Y. and S.C. Hsieh: Factorizable Inverse Semigroups, Semigroup Forum (8), 283-297, (1974).

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

[3] Petrich, M.: Inverse Semigroups, to appear.

Vesna Kilibarda
Nastavnički fakultet - Nikšić
81400 Nikšić
ul. Danila Bojovića bb

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", ZAGREB 1984

INVERSE CONGRUENCES ON ORTHODOX SEMIGROUPS

Dragica N. Krgović

Abstract. The purpose of this paper is to consider inverse congruences on an arbitrary orthodox semigroup S. Necessary and sufficient conditions on a pair (K, τ), for the existence of an inverse congruence ρ on S such that K is the kernel and τ is the trace of ρ, are established. The main result is the characterization of inverse congruences on an orthodox semigroup (Theorem 1). Petrich's characterization [9] of congruences on an inverse semigroup and Feigenbaum's characterization [3] of group congruences on an orthodox semigroup are derived as particular cases of Theorem 1. Also, the characterization of semillatice congruences on an orthodox semigroup is obtained (Corollary 2). We give also a new description of the minimum inverse congruence Y on an orthodox semigroup, as a consequence of the Theorem 1.

Let S be a regular semigroup, E its set of idempotents. For any element a in S, V(a) will denote the set of inverses of a. Recall that a subsemigroup H of S is self-conjugate if $x'Hx \subseteq H$ for all x in S and all x' in V(x), and H is called full if $E \subseteq H$. A subsemigroup H of S is inverse-closed if $V(x) \subseteq H$ for all x in H [5].

It is easy to prove the next useful lemmas.

LEMMA 1. *Let ρ be an inverse congruence on a regular semigroup S. Then*

$$(\forall a,b \in S)(a \rho b \Rightarrow (\forall a' \in V(a))(\forall b' \in V(b)) a' \rho b').$$

LEMMA 2. *For a congruence ρ on an orthodox semigroup S, the following conditions are equivalent.*

(i) *ρ is inverse.*

(ii) $(\forall a,b \in S)(a \rho b \Rightarrow (\forall a' \in V(a))(\forall b' \in V(b)) a' \rho b')$.

(iii) $(\forall a \in S)(\forall e \in E)(a \rho e \Rightarrow (\forall a' \in V(a)) a' \rho e)$.

(iv) $(\forall e,f \in E)(e \rho f \Rightarrow (\forall e' \in V(e))(\forall f' \in V(f)) e' \rho f')$.

(v) $(\forall e \in E)(\forall e' \in V(e))e' \varrho e$.

(vi) $(\forall a \in S)(\forall a', a'' \in V(a))a' \varrho a''$.

For any congruence ϱ on S, let $tr\varrho = \varrho|_E$ and $ker\varrho = \{x \in S \mid x\varrho e \text{ for some } e \in E\}$. This associates to each congruence ϱ on S the ordered pair $(ker\varrho, tr\varrho)$. We will introduce a pair (K, τ) which is an abstraction of the properties of $(ker\varrho, tr\varrho)$ for some inverse congruence ϱ.

DEFINITION 1. _Let_ S _be an orthodox semigroup. A full, self-conjugate inverse-closed subsemigroup of_ S _is a normal subsemigroup of_ S. _A congruence_ τ _on_ E _is normal if for any_ $e, f \in E$ _and_ $x \in S$, $x' \in V(x)$, $e\tau f$ _implies_ $x'ex \,\tau\, x'fx$. _The pair_ (K, τ) _is an inverse congruence pair for_ S _if_ K _is a normal subsemigroup of_ S, τ _is a normal congruence on_ E _and these two satisfy:_

i) $(ae \in K,\ e\tau a'a) \Rightarrow a \in K \qquad (a \in S,\ e \in E,\ a' \in V(a))$

ii) $aa' \tau a'a$ _for every_ $a \in K$, $a' \in V(a)$.

Using these concepts and notations we will obtain the characterization of inverse congruences on orthodox semigroups. We start with a lemma.

LEMMA 3. _Let_ (K, τ) _be an inverse congruence pair for an orthodox semigroup_ S. _Then_

i) $(aeb \in K,\ e\tau a'a) \Rightarrow ab \in K$,

ii) $(ab' \in K,\ a'a \tau b'b) \Rightarrow a'ea \,\tau\, b'eb$,

iii) $e' \tau e$,

for every $a, b \in S$, $e \in E$, $a' \in V(a)$, $b' \in V(b)$, $e' \in V(e)$.

Proof. Note first that $b'a' \in V(ab)$ for every $a, b \in S$, $a' \in V(a)$, $b' \in V(b)$.

Let $a, b \in S$, $e \in E$, $a' \in V(a)$, $b' \in V(b)$ and $e' \in V(e)$.

i) Let $aeb \in K$ and $e \tau a'a$. Then

$(ab)(b'ea'aeb) = (abb'ea')(aeb) \in K$ (since $E \subseteq K$, $K^2 \subseteq K$),

$b'a'ab \,\tau\, b'eb = b'eeeb \,\tau\, b'ea'aeb$ (since $b'e \in V(eb)$ and τ is normal), which implies $ab \in K$ by Def 1. i).

ii) Let $ab' \in K$ and $a'a \tau b'b$. Then

$a'ea = a'aa'eaa'a \,\tau\, b'ba'eab'b$ (since $a'a \,\tau\, b'b$),

$\tau\, b'eab'ba'eb$ (using Def 1.ii) on $eab' \in K$),

$\tau\, b'eba'ab'eb$ (using Def 1.ii) on $ab' \in K$),

$\tau\, b'eb$ (since $a'a \tau b'b$).

iii) According to Def.1.ii), $ee'\tau e'e$. Hence $e\tau e'e$ and $e'\tau e'e$ since $e'\in E$. Therefore, $e'\tau e$.

THEOREM 1. <u>Let</u> S <u>be</u> <u>an</u> <u>orthodox</u> <u>semigroup</u>. <u>If</u> (K,τ) <u>is</u> <u>an</u> <u>inverse</u> <u>congruence</u> <u>pair</u> <u>for</u> S, <u>then</u> <u>the</u> <u>relation</u> $\rho_{(K,\tau)}$ <u>defined</u> <u>on</u> S <u>by</u>

$$a\ \rho_{(K,\tau)}\ b \overset{def}{\Longleftrightarrow} (\exists a'\in V(a))(\exists b'\in V(b))(a'a\,\tau\, b'b,\ ab'\in K)$$

<u>is</u> <u>the</u> <u>unique</u> <u>inverse</u> <u>congruence</u> <u>on</u> S <u>for</u> <u>which</u> $\ker\rho = K$ <u>and</u> $\mathrm{tr}\rho = \tau$.

<u>Conversely</u>, <u>if</u> ρ <u>is</u> <u>an</u> <u>inverse</u> <u>congruence</u> <u>on</u> S, <u>then</u> $(\ker\rho, \mathrm{tr}\rho)$ <u>is</u> <u>an</u> <u>inverse</u> <u>congruence</u> <u>pair</u> <u>for</u> S <u>and</u> $\rho_{(\ker\rho,\mathrm{tr}\rho)} = \rho$.

<u>Proof</u>. Let (K,τ) be an inverse congruence pair for S, and let $\rho = \rho_{(K,\tau)}$. Then ρ is reflexive since K is full, and it is symmetric since τ is symmetric and K is an inverse-closed semigroup. Let $a\rho b$ and $b\rho c$, so that $a'a\,\tau\, b'b$, $b''b\,\tau\, c'c$ and $ab', bc'\in K$ for $a'\in V(a)$, $b', b''\in V(b)$ and $c'\in V(c)$. Hence $a(b'b)c'=(ab')(bc')\in K$ which together with $b'b\,\tau\, a'a$ by Lemma 3 i) yields $ac'\in K$. According to Lemma 3 iii), $b'b\,\tau\, b''b$ since $b''b\in V(b'b)$, so that $a'a\,\tau\, c'c$. Thus $a\rho c$ and ρ is transitive.

Next let $a\rho b$ and $c\in S$, so that $a'a\,\tau\, b'b$ and $ab'\in K$ for some $a'\in V(a)$, $b'\in V(b)$. If $c'\in V(c)$, then $c'a'\in V(ac)$, $c'b'\in V(bc)$ and $b'bcc'a'\in V(acc'b'b)$. Thus $c'a'ac\,\tau\, c'b'bc$ (since $a'a\,\tau\, b'b$). Further,
$(acc'b'b)(a'bcc'a'acc'b'a)b'=(acc'b'ba')(bcc'a'acc'b')(ab')\in K$ (since $E\subseteq K$ and $K^2\subseteq K$),
$a'bcc'a'acc'b'a\,\tau\, b'bcc'a'acc'b'b$ (using Lemma 3 ii) on $bcc'a'acc'b'\in E$), which implies $(acc'b'b)b'\in K$ by Lemma 3 i). Thus $acc'b'\in K$. It follows that $ac\,\rho\, bc$. According to Lemma 3 ii), $a'c'ca\,\tau\, b'c'cb$. Since $ab'\in K$ and K is self-conjugate we have $cab'c'\in K$. Therefore $ca\,\rho\, cb$ and ρ is a congruence on S.

Let $a\rho e$ for $e\in E$, so that $a'a\,\tau\, e'e$, $ae'\in K$ for $a'\in V(a)$, $e'\in V(e)$. Then $a(e'e)=(ae')e\in K$ which implies $a\in K$ by Def 1 i). Conversely, assume that $a\in K$. Then $a=a(a'a)\in K$ and $a'a=(a'a)(a'a)$ for $a'\in V(a)$, which implies that $a\rho a'a$. Consequently, $\ker\rho = K$.

If $e,f\in E$ and $e'\in V(e)$, $f'\in V(f)$, then by Lemma 3 iii), $e\tau e'e$ and $f\tau f'f$ since $e\in V(e'e)$ and $f\in V(f'f)$. It follows that

$e\rho f \Leftrightarrow (\exists e'\in V(e))(\exists f'\in V(f))e'e\,\tau\, f'f \Leftrightarrow e\,\tau\, f$,

for any $e,f\in E$. Therefore $\mathrm{tr}\rho = \tau$.

The congruence ρ is inverse by Lemma 2 and Lemma 3 iii) since $\mathrm{tr}\rho = \tau$.

Now let γ be an inverse congruence on S such that $\ker\gamma = K$ and $\mathrm{tr}\gamma = \tau$. Assume first that $a\gamma b$. If $a'\in V(a)$ and $b'\in V(b)$, then by Lemma 2, $a'\gamma b'$ so that $a'a\gamma b'b$; also $ab'\gamma bb'$. This shows that $a'a\,\tau\, b'b$ and $ab'\in K$, which implies that $a\rho b$. Conversely, assume that $a\rho b$. Then $a'a\,\tau\, b'b$ and $ab'\in K$ for some $a'\in V(a)$ and $b'\in V(b)$, which implies that $a'a\gamma b'b$ and $ab'\gamma e$ for some $e\in E$. Then by Lemma 2, $ba'\gamma e$ since $ba'\in V(ab')$. Hence $ab'\gamma ba'\gamma ba'ba'$ which together with $a'a\gamma b'b$ yields

$$a=aa'a\gamma ab'b\gamma ba'bb'b\gamma ba'ba'a\gamma ba'a\gamma bb'b = b.$$

Consequently, $\rho = \gamma$ which proves uniqueness.[1)]

Conversely, let ρ be an inverse congruence on S. A simple verification shows that $\ker\rho$ is a self-conjugate subsemigroup of S. According to Lemma 2.3[7] $\ker\rho$ is inverse-closed. Consequently, $\ker\rho$ is a normal subsemigroup of S. Let $a\in S$ and $e\in E$. If $ae\in\ker\rho$ and $e\rho a'a$ for some $a'\in V(a)$, then $f\rho ae\rho aa'a = a$ for some $f\in E$. Thus $a\in\ker\rho$.

Let $a\in S$ and $a'\in V(a)$. If $a\in\ker\rho$, then $a\rho e$ for some $e\in E$. Hence $a'\rho e$ by Lemma 1. It follows that $aa'\rho e$ and $a'a\rho e$ which implies $aa'\rho a'a$. Thus $aa'\rho a'a$ for every $a\in\ker\rho$ and $a'\in V(a)$. Therefore $(\ker\rho, \mathrm{tr}\rho)$ is an inverse congruence pair for S. That $\ker\rho_{(\ker\rho,\mathrm{tr}\rho)}=\ker\rho$, $\mathrm{tr}\rho_{(\ker\rho,\mathrm{tr}\rho)}=\mathrm{tr}\rho$ follows from above. Now the uniqueness just proved implies that $\rho_{(\ker\rho,\mathrm{tr}\rho)}= \rho$.

If S is an inverse semigroup, then Theorem 1 reduces to Theorem 4.4[9].

Since a group congruence on an orthodox semigroup is also inverse, we have

---

1) The uniqueness also follows from Theorem 5.1[2].

COROLLARY 1. *Let K be a normal subsemigroup of an orthodox semigroup S and let $ae \in K \Rightarrow a \in K$, for every $a \in S$, $e \in E$. Then the relation ϱ_K defined on S by*

$$a \varrho_K b \overset{DEF}{\Longleftrightarrow} (\exists b' \in V(b))ab' \in K$$

is a group congruence on S.

Conversely, if ϱ is a group congruence on S, then $\ker\varrho$ is a normal subsemigroup of S with, $ae \in \ker\varrho \Rightarrow a \in \ker\varrho$, for every $a \in S$, $e \in E$, and $\varrho = \varrho_{\ker\varrho}$.

Let K be a subset of a semigroup S. For any $H \subseteq S$ define the *left K-closure* of H to be $H\omega_K^{\ell} = \{x \in S \mid (\exists k \in K) kx \in H\}$, *the right K-closure* of H to be $H\omega_K^{r} = \{x \in S \mid (\exists k \in K) xk \in H\}$. If $H\omega_K^{\ell} = H\omega_K^{r}$, then it will be called the *K-closure* of H and we write $H\omega_K$. H will be called *left K-closed* [*right K-closed*] if $H\omega_K^{\ell} = H$ [$H\omega_K^{r} = H$]. If H is both left and right K-closed, H will be called *K-closed* ($H\omega_K = H$).

If K=H then left H-closure of H will be called left closure of H and similarly in other cases.

Let S be a regular semigroup. Notice that $H \subseteq HE \cap EH$ for any $H \subseteq S$. According to the proof of Lemma 2, Proposition 1 and Lemma 3 [6] it is easy to see that the following Lemma holds.

LEMMA 4. *Let H be a subsemigroup of a regular semigroup S. If HE=EH=H we have*

i) *If H is regular, then $H\omega_E^{\ell} = H\omega^{\ell}$,*

ii) *If H is self-conjugate, then $H\omega^{\ell} = H\omega^{r}$,*

iii) *H is regular if and only if H is inverse-closed.*

Therefore, if H is a self-conjugate subsemigroup of S such that HE=EH=H, then H is left-closed if and only if H is closed. Also, if H is a self-conjugate regular (that is inverse-closed), subsemigroup of S such that HE=EH=H, then $H\omega_E^{\ell} = H\omega^{\ell} = H\omega^{r} = H\omega_E^{r}$. In such a case,

(1) H is left-closed $\Leftrightarrow$ H is left E-closed
$\Leftrightarrow$ H is E-closed
$\Leftrightarrow$ H is closed.

Let $\mathcal{K} = \{K \subseteq S \mid K$ is a full, inverse-closed, self-conjugate subsemigroup of S and $ae \in K \Rightarrow a \in K$ for any $a \in S$, $e \in E\}$ and let $\bar{\mathcal{C}} = \{C \subseteq S \mid C$ is a full, closed, self-conjugate subsemigroup of $S\}$. We have just proved that $\mathcal{K} = \bar{\mathcal{C}}$. Therefore, for orthodox semigroups the following theorem reduces to the Corrolary 1.

THEOREM 2. (Feigenbaum, [3]). Let S be a regular semigroup. The map $C \to (C) = \{(a,b) \in S \times S \mid ab' \in C$ for some $b' \in V(b)\}$ is a 1-1 order preserving map of $\bar{\mathcal{C}}$ onto the set of group congruences on S.

Remark. For an orthodox semigroup S we have

LEMMA 5. If H is a subsemigroup of an orthodox semigroup S such that HE=EH=H, then $H\omega_E^{\ell} = H\omega_E^{r}$.

Proof. We prove $H\omega_E^{\ell} \subseteq H\omega_E^{r}$.

$$a \in H\omega_E^{\ell} \Rightarrow ea \in H \text{ for some } e \in E,$$
$$\Rightarrow aa'ea \in H \text{ for } a' \in V(a) \quad \text{(since EH=H)},$$
$$\Rightarrow a \in H\omega_E^{r} \quad \text{(since } a'ea \in E).$$

The proof of the converse is similar.

Therefore, if H is a subsemigroup of S such that HE=EH = H, then H is left E-closed if and only if H is E-closed. According to Lemma 4 and Lemma 5, if H is a regular (i.e inverse--closed) subsemigroup of S such that HE=EH=H, then $H\omega^{\ell} = H\omega_E^{\ell} = H\omega_E^{r} = H\omega^{r}$. It follows that for any regular subsemigroup H of an orthodox semigroup S such that HE=EH=H, (1) holds.

Since a semillatice congruence on an orthodox semigroup is also inverse, we get the following corollary of Theorem 1.

COROLLARY 2. Let S be an orthodox semigroup. Let τ be a normal congruence on E and $aa' \tau a'a$ for every $a \in S$ and $a' \in V(a)$. Then the relation ρ_τ defined on S by

$$a \, \rho_\tau \, b \overset{def}{\Longleftrightarrow} (\exists a' \in V(a))(\exists b' \in V(b)) a'a \, \tau \, b'b$$

is a semillatice congruence on S.

Conversely, if ρ is a semillatice congruence on S, then $tr\rho$ is a normal congruence on E, $aa'(tr\rho)a'a$ for every $a \in S$, $a' \in V(a)$ and $\rho = \rho_{tr\rho}$.

The minimum inverse congruence on an orthodox semigroup S is given by

aYb if and only if $V(a) = V(b)$.

It is known that Y is an idempotent pure congruence on S. According to Theorem 1 we have

$$aYb \Leftrightarrow (\exists a'\in V(a))(\exists b'\in V(b))(V(a'a)=V(b'b),\ ab'\in E).$$

Therefore

$$aYb \Leftrightarrow (\exists a'\in V(a))(\exists b'\in V(b))(a'a=a'ab'ba'a,\ b'b=b'ba'ab'b, ab'\in E).$$

Let S be a semigroup, $a,b \in S$ and $a'\in V(a)$, $b'\in V(b)$. It is evident that

$$a'a=a'ab'ba'a \Leftrightarrow a = ab'ba'a \Leftrightarrow aa' = ab'ba',$$

$$aa'=ab'ba' \Rightarrow (ab'aa'=aa' \Leftrightarrow ab'\in E).$$

If S is orthodox then

$$a'aYb'b \Leftrightarrow a = ab'ba'a,\quad b = ba'ab'b$$

$$\Leftrightarrow aa' = ab'ba',\ bb' = ba'ab'.$$

We have therefore established the following result:

COROLLARY 3. *If a,b are elements of an orthodox semigroup S then the following statements are equivalent.*

(i) a Y b.

(ii) $(\exists a'\in V(a))(\exists b'\in V(b))(V(a'a)=V(b'b),\ ab'\in E)$

(iii) $(\exists a'\in V(a))(\exists b'\in V(b))(aa'=ab'ba'=ab'aa',\ bb'=ba'ab')$.

Acknowledgement. The author would like to Thank Professor Dr Mario Petrich for his valuable comments on the first version of this paper.

REFERENCES

1. A.H.Clifford, and G.B.Preston, "*The Algebraic Theory of Semigroups*", Amer.Math.Soc., Providence, R.I. Vol.I, 1961; vol.II, 1967.

2. C.Eberhart, and W.Williams, *Congruences on an orthodox semigroup via the minimum inverse semigroup congruence*, Clasgow Math.J. 18(1977) 181-192.

3. R.Feigenbaum, *Kernels of regular semigroup homomorphisms*, Doctoral dissertation, University of South Carolina,1975.

4. J.M.Howie, "*An Introduction to Semigroup Theory*" Academic Press, London/New York/San Francisko, 1976.

5. D.N.Krgović, *Idempotent separating congruences on regular semigroups*, Algebraic conference, Beograd 1982.

6. D.R. LaTorre, Group congruences on regular semigroups, Semig. oup Forum 24(1982) 327-340.

7. J.Meakin, Congruences on orthodox semigroups, J.Austral. Math.Soc. 12(1971).

8. M.Petrich, "Introduction to Semigroups", Merill, Columbus, 1973.

9. M.Petrich, Congruences on inverse semigroups, J.Algebra, 55(1978), 231-256.

10. M.Petrich, "Inverse semigroups", A Wiley-Interscience, New York, 1984.

Matematički institut
Kneza Mihaila 35
11000 Beograd
Jugoslavija

Poljoprivredni fakultet
Nemanjina 6
11080 Zemun
Jugoslavija

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", ZAGREB 1984

SEMILATTICES OF SIMPLE n-SEMIGROUPS

P. Kržovski

The purpose of this paper is to show that the well known characteristic of semilattices of simple semigroups ([1],[2]) could be generalized for the class of n-semigroups for $n>2$.

1. SOME DEFINITIONS AND RESULTS

Let S be on n-semigroup, i.e. an algebra with an associattive n-ary operation $(x_1,x_2,\dots,x_n)\to x_1x_2\dots x_n$. An n-semigroup S is called a semilattice if S is commutative, idempotent and satissies the sollowing identity

$$x_1^{i_1}x_2^{i_2}\dots x_k^{i_k}=x_1^{j_1}x_2^{j_2}\dots x_k^{j_k},$$

where $i_1+i_2+\dots+i_k=j_1+j_2+\dots j_k=n,\ i_\nu,\ j_\nu>0$.

A congruence on an n-semigroup S is called a semilattice congruence if S/α is a n-semilattice.

A nonempty subset A of an n-semigroup S is called an ideal of S iff $a\in S$, $x_i\in S$ imply $x_1\dots x_{i-1}\,a\,x_i\dots x_n\in A$ for every $i=1,2,\dots,n$.

An ideal J of S is said to be completely prime iff $x_1x_2\dots x_n\in J$ $x_1\in J$ or $x_2\in J$ or ... or $x_n\in J$.

A subset F of S is a filter in S iff $J=S\setminus F$ is a completely prime ideal.

An ideal A of an n-semigroup S is completely semiprime if for any $x\in S$, $x^n\in A$ implies $x\in A$.

An characterisation of all semilattice decompositions of an n-semigroup S in terms of completely prime ideals is given in [3]. The least semilattice congruence is denated by η. The minimal filtre in S which contains x is denoted by N(x), i.e. N(x) is the filtre generated by x. The classes of the congruence η are called N-classes. If $x \in S$, then the N-class which contains x is denated by N_x. The class N_x is the largest n-subsemigroup of S containing x and containing no proper completely prime ideals.

An n-semigroup S is said to be *η-simple* iff S has no proper completely prime ideals. For n-ary case the following theorem is given in [3] (3.5):

1.1 Is I is an ideal of some N class of an n-semigroup S, then I has no proper completely prime ideal.

As a consequence of 1.1 we conclude that:

1.2 Every n-semigroup is a semilattice of η - simple n-semigroups.

The principal left, right two sided ideals and ideal of a semigroup S generated by an element $x \in S$ have the following form:

$$L(x) = x \cup S^{n-1}x, \quad R(x) = x \cup xS^{n-1},$$

$$I(x) = x \cup S^{n-1}x \cup xS^{n-1} \cup S^{n-1}xS^{n-1},$$

$$J(x) = x \cup S^{n-1}x \cup S^{n-2}xS \cup \ldots \cup xS^{n-1} \cup S^{n-1}xS^{n-1}.$$

An n-semigroup S is *left* (right) *simple* if S is its only left (right) ideal; S is *two-sided simple* if S is its only two-sided ideal; S is *simple* if S is its only ideal. These notions can be characterised in the following way:

1.3 Let S be an n-semigroup:

S is left simple iff $S^{n-1}a=S$ for all $a \in S$;

S is two-sided simple iff $S^{n-1}aS^{n-1} = S$ for all $a \in S$

S is simple iff $S=(\bigcup_{i=2}^{n-1} S^{n-i}aS^{i-1}) \cup S^{n-1}aS^{n-1}$ for all $a \in S$.

We note also the following results.

1.4 A semilattice S with respect to the relation $\leqslant$ defined by

$$x \leqslant y \Leftrightarrow xy^{n-1}=x$$

is partial ordered set.

2. A SEMIGROUP AND ITS N-CLASSES

Now we shalt establish some equivalent statements on the N-classes, when they are left simple, and certain properties of S in terms of either elements of S or some tipes of ideals of S. ([2], II.4.9 for the binary case).

2.1 *The following conditions on an n-semigroup S are equivalent.*

i) *Every η-class is a left simple n-semigroup.*

ii) *Every left ideal of S is completely semiprime and ideal*

iii) *For every $x \in S$, $x \in S^{n-1}x^n$ and $xS^{n-1} \subseteq S^{n-1}x$.*

iv) *For every $x \in S$, $N_x = L_x$.*

v) *For every $x \in S$, $N_x = \{y \in S \mid x \in S^{n-1}y, x \in S^{n-1}x\}$*

vi) *Every left ideal is a union of η-classes.*

Proof. i) $\Rightarrow$ ii) Let L be a left ideal. If $x^n \in L$, then $x^n \in L \cap N_x$; hence $L \cap N_x$ is a left ideal of N_x and we must have $L \cap N_x = N_x$. But then $x \in L$ and thus L is completely semiprime. If $x \in L$ and $y_1, y_2, \dots, y_{n-1} \in S$, then $y_1 y_2 \dots y_{n-1} x \in L \cap N_{y_1 y_2 \dots y_{n-1}} x$. Hence $L \cap N_{y_1 y_2 \dots y_{n-1}} x$ is a left ideal of $N_{y_1 y_2 \dots y_{n-1} x}$ and we have that $L \cap N_{y_1 y_2 \dots y_{n-1}} = N_{y_1 y_2 \dots y_{i-1} x y_i \dots y_{n-1}}$ for every $i = 1, 2, \dots, n-1$. But then $y_1 y_2 \dots y_{i-1} x y_i \dots y_{n-1} \in N_{y_1 y_2 \dots y_{n-1} x}$ for every $i = 1, 2, \dots, n-1$. This implies $y_1 \dots y_{i-1} x y_i \dots y_{n-1} \in L$, which means that L is an ideal of S.

ii) $\Rightarrow$ iii) For any $x \in S$, $S^{n-1}x^n$ is a left ideal of S and thus it is completely semiprime. Since $x^{2n-1} \in S^{n-1}x^n$, we have $x \in S^{n-1}x^n \subseteq S^{n-1}x$. The set $S^{n-1}x$ is a left ideal and thus an ideal of S and contains x, so that $xS^{n-1} \subseteq J(x) \subseteq S^{n-1}x$.

iii) $\Rightarrow$ iv) First we will prove that $L_x \subseteq N_x$. By the hypothesis, $x \in S^{n-1}x^n \subseteq S^{n-1}x$. Then $L(x) = S^{n-1}x$ for every $x \in S$. If $y \in L_x$, then $L(x) = L(y)$ and thus $x = a_1 a_2 \dots a_{n-1} y$, $y = b_1 b_2 \dots b_{n-1} x$ for some $a_1, a_2, \dots, a_{n-1}, b_1, b_2, \dots, b_{n-1} \in S$. Therefore $N_x = N_{a_1 a_2 \dots a_{n-1} y} = N_{xy^{n-1}} = N_{yx^{n-1}} = N_{b_1 b_2 \dots b_{n-1} x} = N_y$ and thus $y \in N_x$, that is $L_x \subseteq N_x$.

Now we will prove that the relatation $\mathcal{L}$, defined by $x \mathcal{L} y \Longleftrightarrow L(x) = L(y)$ is a semilattice congruence. Since η is the least semilattice congruence we have that $N_x \subseteq L_x$.

By the hypothesis we have that $u \in S^{n-1}u^n = L(u^n)$. Thus $L(u) \subseteq L(u^n)$, $L(u^n) = S^{n-1}u^n \subseteq S^{n-1}u = L(u)$, i.e. $L(u) = L(u^n)$.

We show next that for any $x_1, x_2, \dots, x_n \in S$,

$$L(x_1 x_2 \dots x_n) = L(x_1) \cap L(x_2) \cap \dots \cap L(x_n) \tag{1}$$

Since $(x_1 x_2 \dots x_n)^n \in x_1 x_2 \dots x_{n-1} \dots x_1 x_2 \dots x_{n-1} S^{n-1} \subseteq S^{n-1} x_1 x_2 \dots x_{n-1} \dots x_1 x_2 \dots x_{n-1} \subseteq S^{n-1} x_n x_1 x_2 \dots x_{n-1} = L(x_n x_1 x_2 \dots x_{n-1})$, we have that $x_1 x_2 \dots$

$x_n \in L(x_n x_1 \ldots x_{n-1})$ i.e. $L(x_1 x_2 \ldots x_{n-1} x_n) = L(x_n x_1 \ldots x_{n-1})$.

Similarly

$L(x_n x_1 \ldots x_{n-1}) \subseteq L(x_{n-1} x_n x_1 \ldots x_{n-2})$ and so

$L(x_1 x_2 \ldots x_n) \subsetneq L(x_n x_1 \ldots x_{n-1}) \subseteq \ldots \subsetneq L(x_1 x_2 \ldots x_n)$. Thus

$L(x_1 x_2 \ldots x_n) \subseteq L(x_1) \cap L(x_2) \cap \ldots \cap L(x_n)$.

Let $z \in L(x_1) \cap L(x_2) \cap \ldots \cap L(x_n)$, then $z = a_{11} a_{12} \ldots a_{1n-1} x_1$, $z = a_{21} a_{22} \ldots a_{2n} x_2, \ldots, z = a_{n1} a_{n2} \ldots a_{nn-1} x_n$, for some $a_{ij} \in S$, where $i=1,2,\ldots,n$; $j=1,2,\ldots,n-1$ and consequently

$$Z^n \in L(a_{11} a_{12} \ldots a_{1n-1} x_1 \ldots a_{n1} a_{n2} \ldots a_{nn-1} x_n) \subseteq$$

$$\subseteq L(x_n x_1 a_{21} a_{22} \ldots a_{2n-1} x_2 \ldots a_{n-1n-1} x_{n-1}) \subseteq \ldots \subseteq L(x_1 x_2 \ldots x_n)$$

From the equality (1) follows that

$$L_{x_{i-1} x_{i_2} \ldots x_{i_n}} = L_{x_{j_1} x_{j_2} \ldots x_{j_n}}, \quad L_{x_1^{i_1} x_2^{i_2} \ldots x_k^{i_k}} = L_{x_1^{j_1} x_2^{j_2} \ldots x_k^{j_k}},$$

where $(i_1, i_2, \ldots, i_m)$, $(j_1, j_2, \ldots, j_m)$ are some permutation of the numbres $(1,2,\ldots,n)$ and $i_1 + i_2 + \ldots + i_k = j_1 + j_2 + \ldots + j_k = n$.

iv) $\Rightarrow$ v) Let x be any element of S. Since $x^n \in N_x$, then $x^n \in L_x$. But $L_x = \{y \in S \mid L(x) = L(y)\}$. So, we obtain $L(x) = L(x^n)$. From this it follows that $x \in L(x^n) = x^n \cup S^{n-1} x^n$. If $x = x^n$, then $x = x^n \in S^{n-1} x^n \subsetneq S^{n-1} x$. If $x \in S^{n-1} x^n$, we have that $x \in S^{n-1} x$. Thus $L(x) = S^{n-1}$. Then we can write

$$N_x = L_x = \{y \in S \mid L(x) = L(y)\} = \{y \in S \mid y \in S^{n-1} x,\ x \in S^{n-1} y\}.$$

v) $\Rightarrow$ v) If L is a left ideal of S, x an element of L, and y an element of N_x, then $y \in S^{n-1} x \subseteq L$, that is vi) holds

vi) $\Rightarrow$ i) It suffices to show that $N_x \subseteq N_x^{n-1} y$ for all $y \in N_x$. For $y, z \in N_x$, the hypothesis implies $N_x \subseteq L(y^{2n-1})$. Since $z \in N_x \subseteq L(y^{2n-1}) = y^{2n-1} \cup S^{n-1} y^{2n-1}$ we have that $z = a_1 \ldots a_{n-1} y^{2n-1}$ for some $a_1, a_2, \ldots, a_{n-1} \in S$. Hence $N_x = N_z = N_{a_1 \ldots a_{n-1}} y^{2n-1} = N_{a_1 a_2 \ldots a_{n-1}}$ and $a_1 \ldots a_{n-1} y \in N_x$ which implies $z = a_1 \ldots a_{n-1} y^{2n-1} = a_1 \ldots a_{n-1} y y^{2n-3} y \subseteq N_x^{n-1} y$, and this proves that $N_x \subseteq N_x^{n-1} y$.

A similar proposition holds for right simple N-classes.

By a simple modification of the proof of 2.1, one can prove the following theorem:

2.2. The following conditions on an n-semigroup S are equivalent

i) Every class is two-sided simple.

ii) Every two-sided ideal of S is completely semiprime and ideal.

iii) For every $x \in S$, $x \in S^{n-1}x^nS^{n-1}$

iv) For every $x \in S$, $N_x = I_x$.

v) For every $x \in S$, $N_x = \{y \in S \mid x \in S^{n-1}yS^{n-1},\ y \in S^{n-1}xS^{n-1}\}$

vi) Every two-sided ideal is union of η-classes.

3. Y_s IS LINEARLY ORDERED

In this section we perform an analysis simplar to that of section two. Here we suppose that Y_s is linearly ordered, where $Y_s = S/\eta$ is the set of η-classes of S which constitutes the greatest semilattice decomposition of S.

3.1 The following conditions on an n-semigroup are equivalent.

i) Every η-class is left simple and Y_s is linearly ordered.

ii) Every left ideal of S is completely prime and ideal.

iii) For every $x_1, x_2, \dots, x_n \in S$, $\{x_1, x_2, \dots, x_n\} \cap S^{n-1}x_1x_2\dots x_n \neq \emptyset$ and $xS^{n-1} \subseteq S^{n-1}x$.

Proof. i) $\Rightarrow$ ii) Let L be a left ideal of S. Since every N-class is left simple, by 2.1, L is a union of N-classes. If $x_1x_2\dots x_n \in L$, then $N_{x_1x_2\dots x_n} \subseteq L$. By hypothesis Y_s is linearly ordered, which means that $N_{x_{i_1}} \leqslant N_{i_2} \leqslant \dots \leqslant N_{x_{i_n}}$, where $(i_1, i_2, \dots,, i_n)$ is some permutation of the numbers $(1,2,\dots,n)$. We have that

$$N_{x_{i_1}} = N_{x_{i_1}^{n-1}x_{i_2}} = N_{x_i^{n-1}x_{i_2}^{n-1}x_{i_3}} = \dots N_{x_{i_1}^{n-1}x_{i_2}^{n-1}\dots x_{i_{n-1}}^{n-1}x_{i_n}} = N_{x_i^{n-1}x_{i_2}^{n-1}\dots x_{i_{n-1}}^{n-1}x_{i_n}^{n}} = N_{y_{i_1}^{n-1}x_{i_n}x_{i_2}^{n-1}x_{i_n}\dots x_{i_{n-1}}^{n-1}x_{i_n}} = N_{x_{i_1}x_{i_2}\dots x_{i_n}},$$

and thus L is completely prme.

Let $x_1,x_2,\dots,x_{n-1}\in S$ and $y\in L$, then $x_1x_2\dots x_ny \in N_{x_1x_2\dots x_{n-1}} \subseteq L$. Since $N_{x_1x_2\dots x_{n-1}y} = N_{x_1x_2\dots x_{i-1}yx_i\dots x_n}$, we have that $x_1x_2\dots x_{i-1}yx_i\dots x_n\in L$ and thus L is ideal of S.

ii) ⇒ iii) For any $x_1,x_2,\dots,x_n\in S$, $S^{n-1}x_1x_2\dots x_n$ is a left ideal of S and completely prime ideal. Since $(x_1x_2\dots x_n)^n\in S^{n-1}x_1x_2\dots x_n$, we have that $x_1x_2\dots x_n$ $S^{n-1}x_1x_2\dots x_n$ and thus either $x_1\in S^{n-1}x_1x_2\dots x_n$ or $x_2\in S^{n-1}x_1x_2\dots x_n$ or ... or $x_n\in S^{n-1}x_1x_2\dots x_n$. From 2.1 it foollows that $xS^{n-1}\subseteq S^{n-1}x$.

iii) ⇒ i) Let $x,y\in S$ and suppose that $x\in S^{n-1}xy^{n-1}$; the case $y\in S^{n-1}xy^{n-1}$ is treated similarly. Then $x=a_1a_2\dots a_{n-1}xy^{n-1}$ for some $a_1,a_2,\dots,a_{n-1}\in S$, and thus $N_x=N_{a_1a_2\dots a_{n-1}xy^{n-1}} = N_{a_1a_2\dots a_{n-1}xy^{n-2}y} = N_{a_1a_2\dots a_{n-1}xy^{n-2}y^n} = N_{a_1a_2\dots a_{n-1}xy^{n-1}y^{n-1}} = N_{xy^{n-1}}$, that is $N_x\leqslant N_y$ and therefore Y_s is linearly ordered. Left simplicity of each N_x follows immediately form 2.1 since $x\in S^{n-1}x^n$ for all $x\in S$.

A proof of the next theorem can be given by a modification of the proof of 3.1.

3.2. <u>The following conditions on an n-semigroup S are quivalent.</u>

i) <u>Every η - class is two-sided simple and Y_s is linearly ordered</u>

ii) <u>Every ideal of S is completely prime and ideal</u>

iii) <u>For every</u> $x_1,x_2,\dots,x_n\in S$, $\{x_1,x_2,\dots,x_n\}\cap S^{n-1}x_1x_2\dots x_nS^{n-1}\neq\emptyset$.

R E F E R E N C E S

[1] Petrich M., The maximal semilattice decomposition of a semigroup, Math. Zeitschnift 85, 68-82 (1964)

[2] Petrich M., Introduction to semigroups, Charles E. Merill publ. Co.Columbus, Ohio 1973

[3] Kržovski P., The maximal semilattice decomposition of an n-semigroup, Algebraic Conference, Novi Sad, 1981 (93-107).

Mašinski fakultet
91000 Skopje
Yugoslavia

ON IRREDUCIBILITY OF WEIERSTRASS POLYNOMIALS OF LOW DEGREE IN THE RING $K[[x,y]]$

Aleksandar Lipkovski

Abstract. The notion of unibranched singularities of algebraic curves on surfaces is closely related to the notion of irreducible element in the ring $K[[x,y]]$ of the formal power series. In this article some explicit criteria for irreducibility of Weierstrass polynomials of low degree (≤ 7) in the ring $K[[x,y]]$ are described, thus giving us a possibility to recognize unibranched singularities of low multiplicities by their local equations.

Let S be a smooth algebraic surface over algebraically closed field K of characteristic 0, $C \subset S$ a curve with a singular point $P \in C$, x and y local parameters of the surface S in P and $f(x,y)$ a local equation of C in S. Then $\widehat{\mathcal{O}}_{P,S} = K[[x,y]]$, $\widehat{\mathcal{O}}_{P,C} = \widehat{\mathcal{O}}_{P,S}/(f)$ where $\widehat{A}$ denotes the completion of the local ring A with respect to its maximal ideal. The singular point P is called unibranched, if $\widehat{\mathcal{O}}_{P,C}$ is a domain, in other words if f is irreducible in $K[[x,y]]$.

For a formal power series $f = \sum_{(i,j)} a_{ij} x^i y^j$ let $\mathrm{Supp}(f) = \{(i,j) \mid a_{ij} \neq 0,\ i,j \in \mathbb{N}^0\}$. Consider the boundary of the convex hull of the set $\mathrm{Supp}(f) + \mathbb{R}^2_+$. Its compact part, a polygonal line, is called the Newton polygon of f and denoted $N(f)$. The following simple lemma will be used in the sequel.

LEMMA 1. The Newton polygon of the product fg is composed of the Newton polygons of the factors f, g by attaching the segments of both diagrams one to another, ordered by decreasing slope (see [1]p.639).

Let f be as above. Write it in the form $f = f_\mu + f_{\mu+1} + \dots$ where $f_n \in (x,y)^n$ is homogeneous of degree n. The number $\mu \in \mathbb{N}$ is the multiplicity of the singular point P. According to the Weierstrass preparation theorem, there exists invertible $u(x,y) \in K[[x,y]]$ and $a^{(1)}(x), \dots, a^{(\mu)}(x) \in K[[x]]$ such that $\mathrm{mult}\, a^{(i)} \geq i$ and $f(x,y) = u(x,y)\left(y^\mu + a^{(1)}(x)y^{\mu-1} + \dots + a^{(\mu)}(x)\right)$. Introduce the parameter $\nu = \min\{\mathrm{mult}\, a^{(i)}/i,\ i=1,\dots,\mu\}$. Obviously, $\nu \in \mathbb{Q}, \nu \geq 1$. The number $-1/\nu$ is the slope of the steepest segment of $N(f)$. By means of the Tschirnhausen transformation $y \mapsto y - a^{(1)}(x)/\mu$ we may consider $a^{(1)}(x) = 0$. Therefore we may restrict ourselves to the case

(1) $\qquad f = y^\mu + a^{(2)}(x)y^{\mu-2} + \dots + a^{(\mu)}(x)$.

In the following we will always presume that $N(f)$ is a straight line segment. This is a necessary condition for f to be irreducible (see [2] lemma 3.2).

LEMMA 2. (a) <u>If f is irreducible, then $\mu\nu \in \mathbb{N}$</u> .
(b) <u>If $\mu\nu \in \mathbb{N}$ with $\mu, \mu\nu$ relatively prime, then f is irreducible.</u>

<u>Proof</u>. (a) Obviously, if $\mu\nu \notin \mathbb{N}$, then $N(f)$ cannot be a segment. (b) Under these conditions $N(f)$ cannot contain the points with integer coordinates other than its two ends, and by the lemma 1 f is irreducible.

The usual method of exploring singularities is the process of blowing-up, locally described by coordinate changes of the type $x=u, y=uv$. Let $\pi: S^* \to S$ be the blowing-up of S centered at P, C^* be the strict transform of C, τ be the number of points laying above P and let the asterisk denote the parameters of these points.

LEMMA 3. (a) <u>If $\nu = 1$ then $\tau > 1$ and all $\mu^* < \mu$</u> .
(b) <u>If $\nu > 1$ then $\tau = 1$ and $\mu^* < \mu$ or $\mu^* = \mu$ but $\nu^* = \nu - 1$</u> .
(c) <u>In the case $\tau = 1$ we have $\mu^* = \mu \Leftrightarrow \nu \geq 2$</u> .

<u>Proof</u>. For a proof of (a) and (b) see [3] p.226. (c) follows from the fact that the local equation of the strict transform C^* is $f_1(u,v) = v^\mu + \frac{a^{(2)}(u)}{u^2}v^{\mu-2} + \dots + \frac{a^{(\mu)}(u)}{u^\mu}$ and $\mathrm{mult}\left(\frac{a^{(i)}(u)}{u^i}v^{\mu-i}\right) = \mu - 2i + \mathrm{mult}\, a^{(i)}$.

Note that if f is irreducible, so is f_1. According to the lemma 3, after a finite sequence of blowing-ups we get $\nu \in (1,2)$. From the lemma 2 it now follows that for irreducible f of degree μ the only admissible values of ν are $\frac{\mu+1}{\mu}, \frac{\mu+2}{\mu}, \dots, \frac{2\mu-1}{\mu}$. Since there is a finite number of them for a given μ , we may try to find conditions for irreducibility of all f with a given μ , starting with $\mu=2$. As an evident corollary to the preceding lemmas we have:

PROPOSITION 1. <u>For the following combinations of</u> μ,ν <u>all Weierstrass polynomials of the type</u> (1) <u>are analytically irreducible</u>:

$\mu=2$ <u>and every admissible</u> ν $(=3/2)$;

$\mu=3$ <u>and every admissible</u> ν $(=4/3,5/3)$;

$\mu=4$ <u>and</u> $\nu=5/4,7/4$;

$\mu=5$ <u>and every admissible</u> ν $(=k/5,k=6,..,9)$;

$\mu=6$ <u>and</u> $\nu=7/6,11/6$;

$\mu=7$ <u>and every admissible</u> $\nu(=k/7,k=8,..,13)$.

The only nontrivial cases are of course the cases with $\mu,\mu\nu$ not relatively prime. For small $\mu<8$ these are only $\mu=4$, $\nu=3/2$ and $\mu=6$, $\nu=4/3,3/2$ and $5/3$. For the first case the complete answer is found. Notice that, since the point $(\mu\nu,0)$ belongs to $N(f)$, $\text{mult}\, a^{(\mu)}=\mu\nu$ and with a coordinate change we can have $a^{(\mu)}(x)=x^{\mu\nu}$.

THEOREM 1. <u>Every Weierstrass polynomial of the type</u> (1) <u>with</u> $\mu=4$, $\nu=3/2$ <u>can be written in the form</u>

$$y^4+a(x)\,x^3y^2+b(x)\,x^5y+x^6$$

<u>after a suitable coordinate transformation. We have:</u>

f <u>is irreducible</u> $\Leftrightarrow$ $a(0)=\pm 2$ <u>and</u> $\text{mult}\,(a-a(0)) > \text{mult}\, b$.

<u>Proof</u>. The first part is obvious since $\text{mult}\, a^{(i)} \geq i\nu = \frac{3}{2}i$ (i=2,3). After one blowing-up and the coordinate change $y \mapsto y-x^2$ we get a singularity with a local equation

$$y^2+\sum_{i\geq 1} a_i\,(y-x^2)^{i+1}x^2 + \sum_{i\geq 0} b_i\,(y-x^2)^{i+2}\,x$$

and the result follows after considering its Newtons diagram and the case $\mu=2$.

THEOREM 2. <u>Let</u> f <u>be of the type</u> (1) <u>with</u> $\mu=6$.

(a) <u>If</u> $\nu=4/3$, f <u>can be written in the form</u>

$$y^6+a(x)\,x^3y^4+b(x)\,x^4y^3+c(x)\,x^6y^2+d(x)\,x^7y+x^8$$

If f is irreducible, then $b(0)=\pm 2$. Let $\alpha = \text{mult}\, a$, $\lambda = \min\{\text{mult}\, c, \text{mult}(a-d), \text{mult}(b-b(0))\}$.

f is irreducible in the case $\lambda < 6\alpha+8$, $\lambda \not\equiv 0 \bmod 2$.

f is reducible in the following three cases:

1) $\lambda > 6\alpha+8$; 2) $\lambda < 6\alpha+8$ and $\lambda \equiv 0 \bmod 2$;

3) $\lambda = 6\alpha+8$, $a_\alpha^2 \neq 4c_\gamma$ ($\gamma = \text{mult}\, c = 2\alpha$).

(b) If $\nu = 5/3$, f can be written in the form

$$y^6 + a(x)x^4y^4 + b(x)x^5y^3 + c(x)x^7y^2 + d(x)x^9y + x^{10}$$

The other conditions are the same as in (a) (except $\gamma = 2\alpha+1$).

(c) If $\nu = 3/2$, f can be written in the form

$$y^6 + a(x)x^3y^4 + b(x)x^5y^3 + c(x)x^6y^2 + d(x)x^8y + x^9$$

If f is irreducible, then $a(0)=3\varepsilon$, $c(0)=3\varepsilon^2$ ($\varepsilon^3=1$). Let $\alpha = \text{mult}(a-a(0))$, $\beta = \text{mult}\, b$, $\lambda = \min\{\text{mult}(b-d), \text{mult}(a-a(0)-c+c(0))\}$.

f is irreducible in the following two cases:

1) $\lambda \not\equiv 0 \bmod 3$; 2) $\lambda \equiv 0 \bmod 3$ and $\lambda < 3\alpha+6$ and $\lambda < 6\beta+9$.

f is reducible in the following two cases:

1) $\lambda \equiv 0 \bmod 3$, $\lambda > 3\alpha+6$ or $\lambda > 6\beta+9$;

2) $\lambda \equiv 0 \bmod 3$, $\lambda = 3\alpha+6$ and $\lambda < 6\beta+9$ or $\lambda < 3\alpha+6$ and $\lambda = 6\beta+9$.

Proof. The first statement of the three parts is obvious since $\text{mult}\, a^{(i)} \geq i\nu$ (i=2,3,4,5).

(a) The blowing-up and the change $y \mapsto y-x^3$ leads to the series

$$y^2 + \sum_{i\geq 0} a_i(y-x^3)^{i+1}x^4 + \sum_{i\geq 1} b_i(y-x^3)^{i+1}x^3 + \sum_{i\geq 0} c_i(y-x^3)^{i+2}x^2 + \sum_{i\geq 0} d_i(y-x^3)^{i+2}x$$

and the result follows from the analysis of the Newton diagram and the case $\mu=2$.

(b) The proof is almost the same as for (a), except that two blowing-ups are required instead of one.

(c) The blowing-up and the change $y \mapsto y-x^2$ leads to the series

$$y^3 + \sum_{i\geq 1} a_i(y-x^2)^{i+1}x^4 + \sum_{i\geq 0} b_i(y-x^2)^{i+2}x^3 + \sum_{i\geq 1} c_i(y-x^2)^{i+2}x^2 + \sum_{i\geq 0} d_i(y-x^2)^{i+3}x$$

and the result follows from the analysis of the Newton diagram and the case $\mu=3$.

Remark. The remaining alternatives ($\lambda=6\alpha+8$ in (a) and (b) and $\lambda=3\alpha+6=6\beta+9$ in (c)) can be treated further in the same way.

From the theorem of Mather ([1]p.478 or [4]p.89) it is easily seen that the described process will finish after a finite number of steps for every $\mu \in \mathbb{N}$, since the singularity (1) is formally isomorfic to the one obtained by cutting the "tails" of the series $a^{(i)}(x)$ at the sufficiently high order. However, as we see from the theorem 2, with increasing of the parameter μ the explicit conditions of irreducibility become very involved. This leads to the conclusion that the classifying parameter μ is not likely to be the natural one. The most of the work in the classification of irreducible elements in the ring $K[[x,y]]$ still remains to be done.

REFERENCES

1. E.Brieskorn, H.Knörrer, Ebene algebraische Kurven, Birkhäuser, Basel-Boston-Stuttgart 1981.
2. A.Lipkovski, On unibranched rings and a criterion for irreducibility in the formal power series ring, Proc. of the Third algebraic conference, Novi Sad 1983, 93-98.
3. Д.Мамфорд, Алгебраическая геометрия I. Комплексные проективные многообразия, Мир, Москва 1979.
4. J.Milnor, Singular points of complex hypersurfaces, Princeton Univ. Press, Princeton 1968.

Institut za matematiku
Prirodno matematički fakultet
Studentski trg 16
11000 Beograd
Jugoslavija

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", ZAGREB 1984

SEMIGROUPS WHOSE SUBSEMIGROUPS ARE PARTIALLY SIMPLE

Todor Malinović

Abstract. In this paper we describe semigroups in which every proper two-sided ideal is partially simple and in this way a generalization of some results of [7] is given. Partially simple semigroups are studied by the author of [7]. Moreover, in this paper semigroups (regular semigroups) in which every subsemigroup (right ideal) is partially right simple are considered. In this case we give some new characterizations of semigroups in which every subsemigroup has a left identity. Also, we describe semigroups in which every proper right ideal has a left identity. Semigroups in which every subsemigroup (right ideal) has a left identity are studied by M. Petrich in [3]. At the end we describe semigroups which contain unique maximal right ideal.

Let S be a semigroup. An element $a \in S$ is a universal left (interior) divisor of S if $aS=S$ ($SaS=S$). A semigroup S is a partial (right) simple if it contains nonempty subset of universal interior (left) divisors.

For nondefinied notions we refer to [1] .

LEMMA 1. *Let S be a semigroup in which every proper two-sided ideal is partially simple. Then*

(i) *Every proper two-sided ideal of S is a principal ideal and for any proper principal ideal* $J(a)$ *of S,* $J(a)=SaS$.

(ii) *Every two-sided ideal of an arbitrary proper two-sided ideal of S is a two-sided ideal of S.*

Proof. (i) Let J be a proper two-sided ideal of S. Then

$$(\exists a \in J)(J=JaJ \subseteq SaS \subseteq J(a)).$$

Moreover $J(a) \subseteq J$ and so $J=J(a)$.

Let M be a union of all proper two-sided ideals of S and let $a \in M$ be an arbitrary element. Then $a \in SaS$. Suppose that $a \notin SaS$ and $A=aS \cup Sa \cup SaS$. From this and by the hypothesis we have that $a \notin aS$ and $a \notin Sa$. Consequently A is a proper two-sided ideal of J(a) and $J(a) \setminus A = \{a\}$. Thus A is a unigue maximal two-sided ideal of J(a) which implies $J(a)=J(a)aJ(a) \subseteq SaS$ (see Theorem 2.1. [7]) and so $a \in SaS$ which is not possible . Hence

$$(\forall a \in M)(a \in SaS)$$

and thus $J(a)=SaS$.

(ii) Let A be a proper two-sided ideal of S, and let B be a two-sided ideal of A. Then ABA is an ideal of S and $ABA \subseteq B$. We prove that $ABA=B$. Really, if $ABA \subset B$, then

$$(\exists b \in B \setminus ABA).$$

It follows from this and from (i) that $J(b)=SbS$. By the hypothesis we have $J(b)=J(b)^3$. Moreover, $SbS\ SbS\ SbS \subseteq SbS\ b\ SbS$, from this we have $J(b)^3 \subseteq J(b)\ b\ J(b)$ and so $J(b) \subseteq ABA$. Thus $b \in ABA$, which is not possible. Hence, B is a two--sided ideal of S.

THEOREM 1. <u>Every proper two-sided ideal of S is partially simple if and only if one of the following conditions holds</u>:

(i) S <u>is semisimple and its every proper two-sided ideal is a principal ideal</u>.

(ii) S <u>contains a unique maximal two-sided ideal which is semisimple and its every two-sided ideal is a principal ideal</u>.

<u>Proof</u>. Let every proper two-sided ideal of S be partially simple and let M be a union of all proper ideals.

If $M=S$, then $J(a)$ is a proper two-sided ideal of S for every $a \in S$ and the principal factor $J(a)/I(a)$ of S is 0-simple or simple (Theorem 2.2. [7]) and so S is semisimple. Moreover, every proper two-sided ideal of S is a principal ideal (Lemma 1 .).

If $M \neq S$, then M is a unique maximal two-sided ideal of S and by Theorem 2.1. [7], $S \setminus M=\{a \in S \mid SaS=S\}$ or $S\setminus M=\{a\}$, $a^2 \in M$. In the case $S\setminus M=\{a \in S \mid SaS=S\}$ we have that S is partially simple and so by Theorem 2.3. [7] we have (i).

Let $S \setminus M= \{a\}$, $a^2 \in M$. Then, by Lemma 1. and by the hypothesis every two-sided ideal of M is partially simple and M is a semisimple semigroup whose two-sided ideals are principal ideals (Theorem 2.3. [7]).

The converse follows by Theorem 2.3. [7] and by Lemma 1.

DEFINITION. [1] A partially ordered set T is downward well ordered if every non-empty subset of T has a greatest element.

THEOREM 2. <u>The following conditions on a semigroup</u> S <u>are equivalent</u>:

(i) <u>Every subsemigroup of S is partially right simple</u>;

(ii) <u>Every subsemigroup of</u> S <u>has a left identity</u>;

(iii) S <u>is a downward well ordered set of periodic right groups</u>.

<u>Proof</u>. (i) $\Rightarrow$(ii). Let A be a subsemigroup of S. Then A is a partially right simple semigroup, which implies that

$$(\exists a \in A)(aA=A).$$

From this we have that $A^2=A$. Thus every subsemigroups of S is globally idempotent. Consequently, every subsemigroup of S is regular (Theorem 2.1. [4]). If $a \in A$, then

$$(\exists x \in A)(a=axa),$$

and thus

$$aA=axaA=axA=A.$$

Since $ax=e$ is an idempotent of A, we have that e is the left identity of A.

(ii) ⇒ (i). It follows immediately.

(ii) ⇔ (iii) By Theorem 6. [3].

THEOREM 3. _The following conditions on S are equivalent:_

(i) S _is regular and every right ideal of S is partially right simple;_

(ii) _Every right ideal of S has a left identity;_

(iii) S _is regular and E is a band which is a downward well ordered set of right zero semigroups._

Proof. (i) ⇒ (ii). Let S be regular and every right ideal R of S is partially right simple. Then

$$(\exists a \in R)(\exists x \in S)(aR=R \wedge a=axa).$$

Consequently, $R=aR=axaR=axR$. From this we have that $ax=e$ is a left identity of R since e is an idempotent.

(ii) ⇒ (i) If (ii) holds and e is a left identity of R(a), then $e=xa=(ex)a$ for some $x \in S$. Thus $a=a(ex)a$. Hence, S is regular. Let R be an arbitrary right ideal of S and e be a left identity of R. Then $eR=R$ which implies that R is partially right simple.

(ii) ⇔ (iii). By Theorem 12. [3].

THEOREM 4. _Every proper right ideal of S has a left identity if and only if one of the following conditions holds:_

(i) S <u>is regular and its every proper right ideal is partially right simple</u>;

(ii) S <u>contains a unique maximal right ideal which is regular and its every right ideal is partially right simple</u>;

(iii) <u>Every right ideal of</u> S <u>has a left identity</u>.

<u>Proof</u>. Let S be a semigroup whose every proper right ideal has a left identity and let R(S) denote the union of all proper right ideals of S. Then we have that every proper right ideal of S is partially right simple. Let R(S)=S and let a be an arbitrary element of S. Then R(a) has a left identity e which implies e=ax and a=ea. Consequently a=axa. Hence, S is a regular semigroup corresponding to case (i).

If $R(S) \neq S$, then M=R(S) is the unique maximal right ideal of S. Let R be an arbitrary right ideal of M. Then

$$a \in R \Rightarrow a=axa \in RSR \subseteq R^2,$$

which implies $R^2=R$. Consequently

$$RS=R^2S=RRS \subseteq RMS \subseteq RM \subseteq R.$$

Hence, every right ideal of M is a proper right ideal of S and thus every right ideal of M has a left identity. Moreover, by Lemma 1.1. [7] we have $S \setminus M=\{a\}$, $a^2 \in M$ or $S \setminus M= \{a \in S \mid aS=S\}$. If $S \setminus M=\{a\}$, $a^2 \in M$, then by Theorem 2. we have that (ii) holds.

Now, we consider the case $S \setminus M=\{a \in S \mid aS=S\}$. Let a be an arbitrary element of $S \setminus M$. Then a=axa and so

$$aS=axaS=axS=S.$$

Since ax=e is an idempotent of S, we have that e is the left identity of S. Thus in this case we have that every right ideal of S has a left identity corresponding to case (iii).

Since the converse is obvious, the theorem is proved.

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

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

(ii) $S \setminus M = T_1 \cup T_2$, where $T_1 = \{a \in S \setminus M \mid aM = M\}$ is a right simple semigroup of S and $T_2 = \{a \in S \setminus M \mid aM = S\}$ is a two-sided ideal of semigroup $S \setminus M$.

Proof. Let M be a unique maximal right ideal of S. Then $S \setminus M = \{a\}$, $a^2 \in M$ or $S \setminus M = \{a \in S \mid aS = S\}$ (Lemma 1.1. [7]). If $S \setminus M = \{a \in S \mid aS = S\}$, then $T = S \setminus M$ is a subsemigroup of S. Let $a \in S \setminus M$. Then we have $aMS \subseteq aM$ and so aM is an right ideal of S. Consequently, $aM \subseteq M$ or $aM = S$. If $aM \subseteq M$, then

$$aS = S \Rightarrow a(M \cup T) = M \cup T \Rightarrow aM \cup aT = M \cup T.$$

From this we have $aM = M$ since $aT \subseteq T$ and $M \cap T = \emptyset$. Hence,

$$(\forall a \in T)(aM = M \vee aM = S).$$

If $T_1 = \{a \in S \setminus M \mid aM = M\}$ and $T_2 = \{a \in S \setminus M \mid aM = S\}$, then

(1) $$S \setminus M = T_1 \cup T_2$$

Let $a, b \in T_1$ then

$$(aM = M \wedge bM = M) \Rightarrow abM = aM = M.$$

From this we have that $ab \in T_1$. Consequently, T_1 is a subsemigroup of S. If $a, b \in T_2$, then

$$(aM = S \wedge bM = S) \Rightarrow abM = aS = S,$$

and so $ab \in T_2$. Thus, T_2 is a subsemigroup of S.

For $a \in T_1$ and $b \in T_2$ we have that $abM = aS = S$ and $baM = bM = S$. Consequently $ab, ba \in T_2$ and we have

$$(2)\qquad T_1T_2 \subseteq T_2 \wedge T_2T_1 \subseteq T_2$$

From (1) and (2), it follows that

$$T_2(S \setminus M)=T_2(T_1 \cup T_2)=T_2T_1 \cup T_2{}^2 \subseteq T_2,$$

$$(S \setminus M)T_2=(T_1 \cup T_2)T_2=T_1T_2 \cup T_2{}^2 \subseteq T_2.$$

Hence, T_2 is a two-sided ideal of $S \setminus M$.

If $a \in T_1$, then $aS=S$ and so

$$a(M \cup T)=M \cup T \Rightarrow aM \cup aT=M \cup T.$$

It follows from this that $aT=T$, since $aM=M$ and $M \cap T=\emptyset$. Consequently we have that

$$(3)\quad a(T_1 \cup T_2)=T_1 \cup T_2 \Rightarrow aT_1 \cup aT_2=T_1 \cup T_2.$$

Moreover $T_1 \cap T_2=\emptyset$ and from (2) and (3) we have that $T_1 \subseteq aT_2$. However, T_1 is subsemigroup and so $aT_1=T_1$. Hence, T_1 is a right simple subsemigroup of S.

Conversely, in the case (i) the assertion follows imediately. Suppose now that (ii) holds. Then, $M \neq S$ and so $S \setminus M \neq \emptyset$. Consequently, at least one of the sets T_1 and T_2 is nonempty. If T_1 and T_2 are nonempty subsets of S, then

$$(a \in T_1 \wedge b \in T_2) \Rightarrow (abM=aS \wedge abM=S),$$

since $ab \in T_2$ and from this $aS=S$. If $a \in T_2$, then $aM=S$ which implies $aS=S$. Let $T_1=\emptyset$, then

$$a \in T_2 \Rightarrow aM=S \Rightarrow aS=S.$$

Assume that $T_2=\emptyset$. Then

$$a \in T_1 \Rightarrow aS=a(M \cup T_1)=aM \cup aT_1=M \cup T_1=S.$$

Hence, in every of the preceding cases we have that

$$(\forall a \in S \setminus M)(aS=S).$$

i.e. $S \setminus M = \{a \in S \mid aS = S\}$, since for $a \in M$, $aS \subseteq MS \subseteq M \neq S$. It follows from this that M is a maximal right ideal of S (Lemma 1.1. [7]).

LEMMA 2. Let M be a unique maximal right ideal of S. Then M is a two-sided ideal if and only if $T_2 = \{a \in S \setminus M \mid aM = S\} = \emptyset$.

Proof. Let M be a unique maximal right ideal of S. which is two-sided. Then $SM \subseteq M \neq S$, which implies $T_2 = \emptyset$.

Conversely, let $T_2 = \emptyset$ and let M be a unique maximal right ideal of S. Then $S \setminus M = \{a\}$, $a^2 \in M$ or $aM = M$ for any $a \in S \setminus M$ (Theorem 5.). If $S \setminus M = \{a\}$, $a^2 \in M$, then $aM \subseteq M$. Really, if we suppose that $aM \nsubseteq M$ holds, we have that $aM = S$, which is not possible. Let $a \in M$, then $aM \subseteq M$, which together with the case $aM = M$ for any $a \in S \setminus M$ implies $SM \subseteq M$ and thus M is a two-sided ideal of S.

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

Proof. Follows immediately from the Theorem 5. and Lemma 2.

R E F E R E N C E S

[1] A.H. Clifford and G.B. Preston: The algebraic theory of semigroups (in Russian) "MIR ", Moskow 1972.

[2] M. Petrich: Introduction to Semigroups, Charles E. Merrill Publishing Co. Columbus, Ohio 1973.

[3] M. Petrich: Semigroups certain of whose subsemigroups have identities, Czesh. Math. 16 (91) 1966, 186-198.

[4] S. Bogdanović: Sur les demi-groupes dans lesquels tous les sous-demi-groups propres Sont idempotents. Math. Seminar Notes 9(1981) 17-24, Kobe University.

[5] Š. Schwarz: O maksimaljnyh idealah v teorii polugrupp I, II, Czechoslovak Math. Jornal, 3(78), (1953) 139-153, 365-385.

[6] T. Malinović: Polugrupe u kojima je svaki pravi desni ideal regularan, Matematički vesnik, 36(1984), 21-34.

[7] T. Malinović: Partially simple semigroups, Matematički vesnik, (tc appear).

Lenjinova 4/16
175oo - Vranje,
Yugoslavia

**PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", ZAGREB 1984**

ON ε-BOUNDED ULTRAPRODUCTS

Žarko Mijajlović

Ultraproducts of models are one of the most important constructions in model theory by which new or nonstandard models of a first order theory are obtained. Such constructions first appeared in [6], where T.Skolem proved the existence of nonstandard models of arithmetic. The definition of ultraproducts of models given by J.Łoš and his fundamental theorem [2] are the main contribution to this subject, but today several modifications of this construction are known. One such recent construction is the bounded ultrapower of the structure of natural numbers [3], which Kochen and Kripke used to give a new proof of the famous result of Paris and Harrington [5], that a form of Ramsey theorem is not provable in formal arithmetic P. In this note we shall unify some of those constructions.

Let $\mathfrak{M}_i$, $i\in I$, be a nonempty family of models of a first-order language L. Further, let B be a Boolean subalgebra of the field of subsets of I, and let D be an ultrafilter over B. Finally, let $\mathcal{F}\subseteq\prod_i M_i$ be a nonempty set of functions. Other model-theoretic notions and symbols we adopt as they appear in [1].

Assume $\varepsilon\in L$ is a binary relation symbol. Instead of εxy we shall write $x\varepsilon y$. A formula φ of L is ε-bounded if ε is built up by use of symbols of L, logical connectives and bounded quantifiers $(\exists x\varepsilon y)$, $(\forall x\varepsilon y)$, where

$(\exists x\varepsilon y)\psi$ stands for $\exists x(x\varepsilon y\wedge\psi)$, and
$(\forall x\varepsilon y)\psi$ stands for $\forall x(x\varepsilon y\rightarrow\psi)$.

If we want to construct an ultraproduct over $\mathcal{F}$, some hypothesis on $\mathcal{F}$ should be made. Such assumptions on $\mathcal{F}$ are stated in the following definition.

DEFINITION 1. Let $\mathcal{F} \leq \prod_i M_i$. Then

1^o $\mathcal{F}$ is ε-convex if for all $f \in \prod_i M_i$, $f \varepsilon g$ and $g \in \mathcal{F}$ implies $f \in \mathcal{F}$.

2^o $\mathcal{F}$ is closed if $\mathcal{F}$ is closed under operaions in $\prod_i \mathfrak{M}_i$.

Thus we see that if $\mathcal{F}$ is closed then $\mathcal{F}$ is a submodel of $\prod_i \mathfrak{M}_i$, therefore $\mathcal{F}$ is a model of the language L. We remind that symbols Σ_n^o, $\prod_n^o$ denote usual proof-theoretical hierarchis. By $\Sigma_n^o(\mathcal{F})$ we denote the set of all $X \subseteq I$ such that for some Σ_n-formula φ and $f_1,\dots,f_m \in \mathcal{F}$, $X = \{i: \mathfrak{M}_i \models \varphi[f_1(i),\dots,f_m(i)]\}$. Now we introduce a relation $\sim$ in $\mathcal{F}$ induced by the ultrafilter D, as in the case of the standard ultraproduct construction:

$f \sim g$ iff $\{i: f(i) = g(i)\} \in D$.

As usual, if $f \sim g$ we shall say that f=g a.e. (almost everywhere). Also, we have an "a.e." refinement of the notion of ε-convexity: in Definition 1, the term $f \varepsilon g$ is replaced by $f \varepsilon g$ a.e., where $f \varepsilon g$ stands for

$\{i \in I: f(i) \varepsilon g(i)\} \in D$.

If $\mathcal{F}$ is closed set and $\Sigma_0^o(\mathcal{F}) \subseteq B$, then the relation $\sim$ is a relation of congruence of the structure $\mathcal{F}$, so as in the case of standard ultraproduct construction we can define the quotient structure which we denote by $\mathcal{F}/D$. If we keep the former meanings of the symbols, we have the following Loš-type theorem:

THEOREM 2. Suppose

1^o $\Sigma_0^o(\mathcal{F}) \subseteq B$, 2^o $\mathcal{F}$ is closed and an a.e. ε-convex set

Then for any ε-bounded formula $\varphi(x_1,\dots,x_n)$ and $f_1,\dots,f_n \in \mathcal{F}$ we have

$\mathcal{F}/D \models \varphi[f_{1D},\dots,f_{nD}]$ iff

$\{i \in I: \mathfrak{M}_i \models \varphi[f_1(i),\dots,f_n(i)]\} \in D$.

<u>Proof</u> The most of the steps of the proof are similar to the proof of classical Loš theorem, thus we shall consider only the bounded quantifier induction step, i.e. when $\varphi(y,x_1,\dots,x_n)$ is of the form $(\exists x \varepsilon y)\psi(x,x_1,\dots,x_n)$.

($\Rightarrow$) Assume $\mathcal{F}/D \models \varphi[g_D, f_{1D}, \dots, f_{nD}]$ i.e.

$$\mathcal{F}/D \models \exists x \varepsilon g_D \psi[x, f_{1D}, \dots, f_{nD}].$$

Then for some $h \in \mathcal{F}$ we have $h \varepsilon g$ a.e. and $\mathcal{F}/D \models \psi[h_D, f_{1D}, \dots, f_{nD}]$. Therefore, by the induction hypothesis

$\{i \in I: \mathfrak{M}_i \models \psi[h(i), f_1(i), \dots, f_n(i)]\} \in D$ and

$\{i \in I: h(i) \varepsilon g(i)\} \in D$ as well, so

$\{i \in I: \mathfrak{M}_i \models h(i) \varepsilon g(i) \wedge \psi[h(i), f_1(i), \dots, f_n(i)]\} \in D$.

Therefore,

$\{i \in I: \mathfrak{M}_i \models (\exists x \varepsilon g(i)) \psi[(h(i), f_1(i), \dots, f_n(i)]\} \in D$, i.e.

$\{i \in I: \mathfrak{M}_i \models \varphi[g(i), f_1(i), \dots, f_n(i)]\} \in D$.

($\Leftarrow$) Assume $\{i \in I: \mathfrak{M}_i \models \varphi[g(i), f_1(i), \dots, f_n(i)]\} \in D$. So $X = \{i \in I: \mathfrak{M}_i \models (\exists x \varepsilon g(i)) \psi[x, f_1(i), \dots, f_n(i)]\}$ belongs to D. For $i \in X$ we can choose $a_i \in g(i)$ such that $\mathfrak{M}_i \models \psi[a_i, f_1(i), \dots, f_n(i)]$. Let $h \in \prod_i M_i$ be a function defined by $h(i) = a_i$ for $i \in X$, and $h(i)$ be an arbitrary element if $i \notin X$. Then $h \varepsilon g$ a.e., thus $h \in \mathcal{F}$ since $\mathcal{F}$ is $\mathcal{E}$-convex. Using the induction hypothesis we have

$\mathcal{F}/D \models h_D \varepsilon g_D \wedge \psi[h_D, f_{1D}, \dots, f_{nD}]$, therefore

$\mathcal{F}/D \models \varphi[g_D, f_{1D}, \dots, f_{nD}]$.

A structure $\mathcal{F}/D$ which satisfies the conditions of Theorem 2, we shall call an $\mathcal{E}$-bounded ultraproduct of models $\mathfrak{M}_i$, $i \in I$. Using this theorem we can derive a number of variants of ultraproduct constructions and corresponding Łoš-type theorems.

1° Let $\mathcal{F} = \prod_i M_i$, and assume that $\mathcal{E}$ is interpreted in each M_i as a full relation, i.e. $\mathcal{E} = M_i^2$ in M_i. Then the bounded quantifiers $(\exists x \varepsilon y)$, $(\forall x \varepsilon y)$ become the standard quantifiers, and $B = \Sigma_0^0(\mathcal{F})$ is the field of all subsets of I. Thus, we obtain then the classical ultraproduct.

2° Let $M = V_\omega(R)$ be the superstructure over the field of real numbers, $\mathcal{F} \subseteq M^\omega$ the set of bounded functions, and $\mathcal{E}$ be the set-theoretical membership relation $\in$. Then

$\mathcal{F}/D$ is a nonstandard model of analyzis, and in this case Theorem 2. gives the Leibniz transfer principle.

3^o Let $\mathfrak{M}$ be the structure of natural numbers, and ε be the standard ordering $\leq$ in that model. Then the ultrapower construction in [3] is a special case of our construction, and Theorem 1 in [3] corresponds to our Theorem 2.

Some theorems about standard ultraproducts have natural transforms to ε-bounded ultraproducts. Such one concerns the saturation of models. A set of formulas $\Sigma(x)$ is ε-bounded if every formula in $\Sigma(x)$ is ε-bounded, and $\Sigma(x)$ contains a formula of the form $x\varepsilon c$, where c is a constant symbol.

THEOREM 3. (cf [1], Theorem 6.1.) Let $\mathcal{F}/D$ be an ε-bounded ultraproduct, and assume there is a sequence of sets $B=J_0 \geq J_1 \geq \dots$ in B such that $\bigcap_n J_n = \emptyset$. Then $\mathcal{F}/D$ is ω_1 ε-saturated, i.e. $\mathcal{F}/D$ realizes every countable ε-bounded type with countably many parameters in $\mathcal{F}/D$.

<u>Proof</u> It is easy to see that for every simple expansion $(\mathcal{F}/D, f_{1D}, f_{2D}, \dots)$ there is a model $\mathcal{F}'$ such that $\mathcal{F}'/D = (\mathcal{F}/D, f_{1D}, f_{2D}, \dots)$. Thus it suffices to realize ε-bounded types without parameters. So let $\Sigma(x) = \{\varphi_1(x), \varphi_2(x), \dots\}$ be a set of ε-bounded formulas such that every finite subset of $\Sigma(x)$ is finitely satisfieble in $\mathcal{F}'/D$. Define

$$X_n = \{i \in J_n : \mathfrak{M}_i \models \exists x(\varphi_1(x) \wedge \dots \wedge \varphi_n(x))\}, \quad n > 0, \quad n \in \omega.$$

Then $\bigcap_n X_n = \emptyset$, and X_n is a decreasing sequence of sets in D, thus for each $i \in I$ there is the greatest n_i such that $i \in X_{n_i}$. Let $g \in \mathcal{F}$ be the interpretation of the constant symbol c, where $x\varepsilon c$ belongs to $\Sigma(x)$. Then we can choose a function $f \in \prod_i M_i$ such that

if $n_i > 0$ then $\mathfrak{M}_i \models (\varphi_1 \wedge \dots \wedge \varphi_{n_i})[f(i)]$.

Thus if $i \in X_n$ then $\mathfrak{M}_i \models \varphi_n[f(i)]$. Therefore we have

1^o $f \in \mathcal{F}$ since $f\varepsilon g$ a.e.
2^o $\mathcal{F}/D \models \varphi_n[f_D]$ by Theorem 2.

Hence, f_D realizes the type $\Sigma(x)$ in $\mathcal{F}'/D$.

There are other variants of ultraproduct construction. Keeping the meaning of the introduced symbols, a such one construction is described in the following proposition.

THEOREM 4. Let the index set I be the domain of a structure $\mathfrak{M}$, and assume

1^o $\Sigma_n^o(\mathcal{F}) \subseteq B$.

2^o $\mathcal{F} \subseteq M^I$ is closed under Skolem functions for Σ_n^o formulas.

Then for each Σ_n^o formula φ and $f_1,\dots,f_n \in \mathcal{F}$ we have

$\mathcal{F}/D \models \varphi[f_{1D},\dots,f_{nD}]$ iff $\{i \in I : \mathfrak{M} \models \varphi[f_1(i),\dots,f_n(i)]\} \in D$.

The proof of this assertion is straightforward so we omit it. This theorem cover many applications of special ultrapower constructions, particularly in formal arithmetic and set theory, cf [4]. We mention the following:

1^o Let $\mathcal{F}$ be the set of arithmetical Σ_n^o definable functions in formal arithmetic **P** ($n \geqslant 1$), and assume B is the Boolean algebra of Σ_n^o definable sets in **P**. Then $\mathcal{F}/D$ is a model for $\mathbf{P} \cap \Sigma_n^o$ but not for **P** (what improves Mostowski's theorem that P does not have a Σ_n^o axiomatization).

2^o Particular ultrapowers give end extensions of models of theories close to P or ZF set theory (for the review see e.g. [4]).

REFERENCES

1. C.C.Chang, H.J.Keisler, <u>Model Theory</u>, North-Holland, Amsterdam, 1973

2. J.Loš, Quelques remarques, théorémes et problémes sur les classes definissables d'algébres, Mathematical Interpretation of Formal Systems, North-Holland, Amsterdam 1955, 98-113.

3. S.Kochen, S.Kripke, Non-standard Models of Peano Arithmetic, Monographie de L'Enseignement Mathématique No.30, Géneve 1982.

4. H.Kotlarski, On Skolem ultrapowers and their non-standard variant, Zeitschrift für Math. Logik und Grundlagen der Math., B.26, 1980, 227-236.

5. J.Paris, L.Harrington, A Mathematical Incompleteness in Peano Arithmetic, Handbook of Mathematical Logic, North-Holland, 1977.

6. T. Skolem, Uber die Nicht-Characterisiebarkeit der Zahlenreiche mittels endlich oder abzählbar unendlich vieler Aussagen mit ausschlieslich Zahlenvariablen, Fund. Math. 23,1934.

University of Belgrade
Faculty of Sciences,
Math. Department,
Studentski tr 16
11000 Belgrade
Yugoslavia

LOGIC OF GUARANTY

Virgilio Muškardin

Abstract. If $p, \cdot p$ range over propositions which are guaranteed, merely hinted at, respectively, by an ethical and mature speaker, we argue that an information of the form $p \vee (p \wedge q)$ is richer than just p /which should be equivalent according to the classical logic/. We give a semantic construction of a logic, termed the logic of guaranty, in which $p \vee (p \wedge q)$ is equivalent to $p \wedge \cdot q$ /" p is guaranteed, but, besides, q is hinted at"/. It is a 3-valued logic in which $\wedge$ /and/ is a straightforward extension of its classical counterpart, but $\vee$ /or/ receives a new interpretation. /Consequently $p \vee q$ is logically equivalent to $(p \wedge \cdot q) \vee (\cdot p \wedge q)$ ./ Some characteristic features of the logic of guaranty are discussed, with some valid logical implications and equivalences exhibited. This logic is free from the deontic paradox /for $p \not\models p \vee q$ / and does not commit the basic relevance paradoxes /since $p \wedge \neg p \not\models q$, $p \not\models q \vee \neg q$ /. A list of problems, concerning possible extensions and improvements, ends the paper.

M o t i v a t i o n

On an earlier occasion I have pointed out that /classical/ logic, although originated by abstraction from situations of human communication /and individual thinking/, treats /factual/ propositions stated by a certain speaker as being objectively true or false /fifty-fifty!/. And yet, a meaningful and purposeful human communication is based on the assumption that the speaker, at least in principle, states true propositions, in spite of the possibility that he might be mistaken or even deliberately cheating us.

We start with a presupposition that the speaker stating propositions is an ethical and mature pearson i.e. he does not lie on purpose and does not make statements on something he cannot judge about. But even then, he does not utter each proposition with the same guaranty: for some of them he guarantees as surely true while others he merely hints at as only likely true. We use propositional variables, e.g. p, for the former, and propositional variables prefixed by the $\bullet$-operator, e.g. $\bullet q$, for the latter.

Consider now a motivating example: Either of

/1/ $$p \wedge (p \vee q) \quad , \quad p \vee (p \wedge q)$$

is classically considered equivalent to

/2/ $$p \; .$$

/Read "$\wedge$" as "and", "$\vee$" as "or"./ But do we not find an information of the form /1/ richer then the corresponding information of the form /2/? Should /1/ not be more adequately understood as

/3/ $$p \wedge \bullet q \quad ?$$

/3/ is interpreted as "p is guaranteed, but, besides, q is hinted at".

In order to get a better grasp of the logic we are about to develop, think, but not as an essential restriction, of propositional variables as ranging over a set of action-describing propositions. Then p corresponds to actions the speaker has decided to perform while $\bullet q$ corresponds to actions he has only given a thought but has not yet decided about. Concerning the latter actions, he may make up his mind later on or may give up thinking about altogether.

Of course, $\neg p$ /read "$\neg$" as "not"/ corresponds to actions he has decided against /i.e. not to be performed/.

S e m a n t i c s

To elucidate the idea it suffices to construct only the propositional semantics. The basic semantic definition, in the table-form, springs from the following analysis.

According to the proposed approach, in decision making on a certain action one can adopt one of the 3 attitudes:

$\top$ = be agreeable to,

$\mid$ = be reserved about,

$\bot$ = be contrary to;

depending on which one of the action-describing propositions A , $\bullet A$, $\neg A$ resp. holds. Thus our semantics will be 3-valued, the values being denoted by $\top$, $\mid$, $\bot$. Of course, there is apparently the 4th attitude, namely not even to consider that action, but then it is beyond one's dispute.

Thus, each entry in the value-table will be one of $\top$, $\mid$, $\bot$ depending on one's mutually consistent attitudes towards the corresponding propositions.

Obviously, the $\neg$-table should read:

	$\neg$
$\top$	$\bot$
$\mid$	$\mid$
$\bot$	$\top$

.

The $\bullet$-table brings in a desired asymmetry / $\bullet p$ and $\bullet\neg p$ are not equivalent!/:

	$\bullet$
$\top$	$\top$
$\mid$	$\mid$
$\bot$	$\mid$

Justification: if one is agreeable to p being guaranteed, he should also be agreeable to p being hinted at; if one is reserved about p being guaranteed /N.B. at a later stage he might make up his mind!/ he cannot but be reserved about p being hinted at; but if one is contrary to p being guaranteed he need not be contrary to p being hinted at, thus he may nevertheless be reserved in this case.

The $\wedge$-<u>table</u> is a straightforward extension of the classical truth-table for $\wedge$:

$\wedge$	T	I	$\bot$
T	T	I	$\bot$
I	I	I	$\bot$
$\bot$	$\bot$	$\bot$	$\bot$

But $\vee$ receives a new interpretation, hence the $\vee$-<u>table</u> requires some more consideration. When we know only that somebody guarantees $p \vee q$, all we know is that he guarantees p or q or both, but we do not know which is the case. In spite of such "imprecise" information, we shall certainly be agreeable to $p \vee q$ if we are agreeable to both p and q ; and we shall certainly be contrary to $p \vee q$ if we are contrary to both p and q . In all other cases we should be reserved, for in neither of those cases are we certain that what is actually the situation when $p \vee q$ is guaranteed /i.e. which of the three possibilities applies/ coincides with our attitude towards p and q . Hence the table:

$\vee$	T	I	$\bot$
T	T	I	I
I	I	I	I
$\bot$	I	I	$\bot$

.

/The "weakness" of the $\vee$-table reflects the "poverty" of the information form $p \vee q$ ./ Observe that in classical logic $\top \vee \bot = \top$, but under our interpretation, being agreeable to p and contrary to q does not entitles us to being agreeable to $p \vee q$, for the situation might be such that $p \vee q$ may be guaranteed <u>via</u> the guaranty of q only.

There is one more operation usually defined in a propositional logic viz. the <u>operation</u> /$\rightarrow$/ <u>of implication</u>; not to mention the operation /$\leftrightarrow$/ of equivalence which is just the two-way implication. We argue that it cannot be defined in terms of the operations defined so far, if it is really going to be a formalization of implication - one which does not commit implicational paradoxes of any sort. /In classical logic, for example, $\alpha \rightarrow \beta$ is just an abbreviation for $\neg\alpha \vee \beta$, but then we have paradoxical tautologies like $\alpha \rightarrow (\beta \rightarrow \alpha)$, where no contextual relevance of β to α is required./ Indeed, $p \rightarrow q$ is of an essentially different nature than $p \wedge q$ or $p \vee q$. Let A , B be two arbitrary action-describing propositions. Then $A \wedge B$ and $A \vee B$ can also be conceived as /somewhat more complex/ action-describing propositions, but it does not seem that $A \rightarrow B$ could be conceived as such; it simply says that the action in B is implied by the action in A . Thus, if $A \rightarrow B$ is to be meaningful, some sort of <u>subordination</u> should hold between A and B , while $A \wedge B$ and $A \vee B$ could be meaningful even if A and B are entirely <u>independent</u>. Furthermore, the values of $A \wedge B$ and $A \vee B$ depends on our attitude towards A and B , while $A \rightarrow B$ is to be accepted or rejected on some internal merits viz. its propositional form if $\rightarrow$ formalizes the /purely/ logical implication, e.g. we accept $A \rightarrow A$ irrespective of our attitude towards A . Because of these distinct features, we shall not attempt to characterize $\rightarrow$-operator here, but shall leave it as a central theme of an subsequent paper.

Nevertheless, since one cannot do logic without implication, we define the <u>relation</u> $\models$ of <u>logical implication</u> by:

$\alpha \models \beta$ if and only if $\alpha^{\tau} \leq \beta^{\tau}$ for all valuations τ;

where $\alpha^{\tau}, \beta^{\tau} \in \{\top, \mid, \bot\}$ and $\bot < \mid < \top$. Thus, the relation $\Dashv\models$ of <u>logical equivalence</u> is defined by:

$\alpha \Dashv\models \beta$ if and only if $\alpha^{\tau} = \beta^{\tau}$ for all valuations τ,

i.e. $\alpha \Dashv\models \beta$ if and only if $\alpha \models \beta$ and $\beta \models \alpha$.

Obviously, these definitions are in conformity with their classical counterparts.

Notice that no formula takes the value $\top$ under all valuations. /No action is <u>a priori</u> supported!/ Indeed, if all propositional variables in a formula take value $\mid$, so does the formula. But, in view of the proposed definition, this is not an obstacle to characterizing valid logical implications.

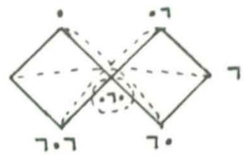
P e c u l i a r i t i e s

Operators $\neg$ and $\cdot$ are the only unary ones. Adopting the term accustomed in modal logic, each consecutive sequence of unary operators will be called a <u>modality</u>. The following table shows that there are exactly <u>7 distinct modalities</u> in the displayed logic of guaranty.

p	$\cdot p$	$\neg p$	$\cdot\cdot p$	$\neg\neg p$	$\cdot\neg p$	$\neg\cdot p$	$\cdot\neg\cdot p$	$\neg\cdot\neg p$	$\cdot\neg\cdot\neg p$	$\neg\cdot\neg\cdot p$
$\top$	$\top$	$\bot$	$\top$	$\top$	$\mid$	$\bot$	$\mid$	$\mid$	$\mid$	$\mid$
$\mid$	$\mid$	$\mid$	$\mid$	$\mid$	$\mid$	$\mid$	$\mid$	$\mid$	$\mid$	$\mid$
$\bot$	$\mid$	$\top$	$\mid$	$\bot$	$\top$	$\mid$	$\mid$	$\bot$	$\mid$	$\mid$

Only 2, $\begin{bmatrix}\top\\ \mid\\ \top\end{bmatrix}$ and $\begin{bmatrix}\bot\\ \mid\\ \bot\end{bmatrix}$, of the 9 variations, when $\mid$'s are fixed in the middle row, cannot be obtained <u>via</u> $\cdot$ and $\neg$

alone; the former appertain to $\neg(p \wedge \neg p)$, the latter to $p \wedge \neg p$. These modalities form an implicational diagram:



/Implication goes along a solid line upwards; dotted lines indicate negation./

From the table we can pick up the <u>reduction rules</u> for modalities:

/i/ of two consecutive •'s delete one,

/ii/ of two consecutive ¬'s delete both,

/So far we are left only with alternating sequences of various lengths, e.g. •¬•¬• or ¬•¬•¬ for length 5./

/iii/ replace an alternating sequence of length greater than 3 by the sequence •¬• .

In particular we have:

$$\cdot\cdot\alpha \mathrel{\vDash\!\dashv} \cdot\alpha \quad ,$$

$$\neg\neg\alpha \mathrel{\vDash\!\dashv} \alpha \quad ,$$

$$\cdot\neg\cdot\neg\alpha \mathrel{\vDash\!\dashv} \cdot\neg\cdot\alpha \mathrel{\vDash\!\dashv} \neg\cdot\neg\cdot\alpha \quad ,$$

for any formula α .

Observe that

/4/ $$\cdot\neg\cdot\alpha \mathrel{\vDash\!\dashv} \cdot\neg\cdot\beta$$

for any pair of formulae α and β . A reflection on the intuitive meaning of •¬• reveals that this equivalence is not as odd as it might appear at first insight.

From the implicational diagram for modalities we see in particular that

$$\alpha \vDash \cdot\alpha \quad \text{and} \quad \neg\cdot\alpha \vDash \neg\alpha \quad .$$

Moreover,

$$\alpha \models \beta \quad \text{if and only if} \quad \neg\beta \models \neg\alpha$$

holds for any α, β.

By inspection of the corresponding tables we find out

/5/ $$\alpha \models \beta \quad \text{if and only if} \quad \alpha \wedge \beta \mathrel{\dashv\vDash} \alpha \quad ,$$

but the replacement of $\wedge$ by $\vee$ in /5/ would not yield a valid conclusion.

It is worth of noticing, though trivial, that

$$\alpha \wedge \cdot\alpha \mathrel{\dashv\vDash} \alpha \quad \text{and} \quad \alpha \vee \cdot\alpha \mathrel{\dashv\vDash} \cdot\alpha \quad ,$$

while

$$\alpha \wedge \cdot\neg\alpha \mathrel{\dashv\vDash} \neg\cdot\neg\alpha \text{ and } \alpha \vee \cdot\neg\alpha \mathrel{\dashv\vDash} \cdot\neg\cdot\alpha \quad .$$

Furthermore we have, in accordance with our motivational paradigm,

$$\alpha \wedge (\alpha \vee \beta) \mathrel{\dashv\vDash} \alpha \wedge \cdot\beta \mathrel{\dashv\vDash} \alpha \vee (\alpha \wedge \beta) \quad .$$

Thus the absorbtivity laws of Boolean algebra /BA/ are not valid here. Nor are De Morgan laws; their invalidity being justifiable in view of our understanding of the operator $\vee$ /see def./. The valid equivalence

$$\alpha \vee \beta \mathrel{\dashv\vDash} (\alpha \wedge \cdot\beta) \vee (\cdot\alpha \wedge \beta) \vee (\alpha \wedge \beta)$$
$$\mathrel{\dashv\vDash} (\alpha \wedge \cdot\beta) \vee (\cdot\alpha \wedge \beta)$$

also complies with our intuition. Concerning other BA-laws we find that idempotency, commutativity, associativity and distributivity are all valid, but

/6/ $$\alpha \wedge \neg\alpha \not\mathrel{\dashv\vDash} \beta \wedge \neg\beta \quad .$$

Still

/7/ $$\alpha \vee \neg\alpha \mathrel{\dashv\vDash} \beta \vee \neg\beta$$

holds for any α, β. Indeed

$$\alpha \vee \neg\alpha \mathrel{\dashv\vDash} \cdot\neg\cdot\alpha \quad ,$$

/cf. /4/ /. This seems right, for by guaranteeing $\alpha \vee \neg\alpha$ one does not really guarantee anything. /He only says a triviality./ Contrasting /6/ and /7/ we may comment that although it is not the same giving a contradictory information about α or about β , it is quite the same giving no information about α or about β . Bearing this in mind it is not surprising that

$$\alpha \vee \neg\alpha \dashv\vDash \neg(\alpha \vee \neg\alpha) \quad .$$

The operation $\bullet$ is distributive over each of the operations $\wedge$ and $\vee$;

$$\bullet(\alpha \wedge \beta) \dashv\vDash \bullet\alpha \wedge \bullet\beta \quad ,$$

$$\bullet(\alpha \vee \beta) \dashv\vDash \bullet\alpha \vee \bullet\beta \quad .$$

Even a stronger connection,

/8/ $$\bullet(\alpha \wedge \beta) \dashv\vDash \bullet(\alpha \vee \beta) \quad ,$$

holds, which nicely confirms our definition of the $\bullet$-operation.

N.B. $$\alpha \wedge \bullet\beta \not\dashv\vDash \bullet(\alpha \wedge \beta) \not\dashv\vDash \bullet\alpha \wedge \beta \quad .$$

As an instance of /8/ we have

$$\bullet(\alpha \wedge \neg\alpha) \dashv\vDash \bullet(\alpha \vee \neg\alpha) \quad ,$$

and each of these is logically equivalent to $\alpha \vee \neg\alpha$, /just poor informations!/.

In the logic of guaranty

$$\alpha \wedge \beta \vDash \alpha \quad ,$$

but

$$\alpha \not\vDash \alpha \vee \beta \quad .$$

The latter fact resolves the so-called <u>deontic paradox</u> /cf. [1, p.21] , where a convincing example,of course using "ought to" instead of "guarantee",reads: "If I ought to mail a letter, I also ought to mail or burn it."/. Naturally

$$\alpha \wedge \beta \vDash \alpha \vee \beta \ .$$

This logic also, to a certain significant degree, avoids some <u>relevance paradoxes</u> /cf. [2, p.111] /, for

$$\alpha \wedge \neg\alpha \not\vDash \beta \quad \text{and} \quad \alpha \not\vDash \beta \vee \neg\beta \quad ,$$

but not entirely, for

$$\alpha \wedge \neg\alpha \models \beta \vee \neg\beta \models \neg(\alpha \wedge \neg\alpha) \quad .$$

In order to resolve these, 2 distinct contexts should be taken into account, as proved in [2] . Hence the task to extend the logic in this direction.

Problems

We end the paper with a list of pertinent problems.

1. Find an adequate formalization of implicational propositions; i.e. define semantically the operation of logical implication.

2. Build in a contextual approach to the logic of guaranty, i.e. one which will also respect different contents of propositions.

3. Consider distinctions between factual and logical truths.

4. Investigate systematically other peculiarities of the logic of guaranty, besides those exhibited.

5. Study an appropriate class of algebras s.t. it contains the corresponding Lindenbaum algebra.

6. Find a sound and complete axiomatization for the logic of guaranty /Hilbert, Gentzen or Smullyan type/.

7. Extend the logic to the first, and perhaps higher, order level; and examine the consequences for set and number theories.

8. Pursue similar constructions starting from different backgrounds, e.g. intuitionistic / $\neg\neg\alpha \not\models\!\!\!\dashv \alpha$ /.

9. Consider possible contributions of the logic of guaranty to the problem of formalizing natural languages.

M e m o r a n d a

This paper was /in essentials/ presented at the symposium "Philosophy of Science and Language" held in Ljubljana on 16th and 17th December 1983.

The author is grateful to N. Miščević who suggested the term "logic of guaranty" and made some useful comments to an early version of the work.

R e f e r e n c e s

1. R. Hilpinen /ed./, DEONTIC LOGIC: INTRODUCTORY AND SYSTEMATIC READINGS, Synthese Library v.33, repr., D. Reidel Publ. Co., Dordrecht 1981.

2. V. Muškardin, QUASI-BOOLEAN ALGEBRAS AND SEMANTICS FOR LOGICAL ENTAILMENT, Ph.D. thesis, University of Bristol, Bristol 1978.

12, S. Kovačevića; 51000 RIJEKA
YUGOSLAVIA

[illegible]

[illegible]

[illegible]

[illegible]

[illegible]

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC“, ZAGREB 1984

LOCALIZATION IN (m,n)-RINGS

Đ. Paunić

Abstract. A universal algebra (R,f,g) is called an (m,n)-ring iff (i) (R,f) is commutative m-group, (ii) (R,g) is an n-semigroup, (iii) for every $a_1,\dots,a_n,b_1,\dots$ $\dots,b_m \in R$

$$g(a_1^{i-1},f(b_1^m),a_{i+1}^n) = f(g(a_1^{i-1},b_1,a_{i+1}^n),\dots,g(a_1^{i-1},b_m,a_{i+1}^n))$$

holds. (m,n)-ring is commutative iff (R,g) is commutative n-semigroup. In this paper only commutative (m,n)-rings will be considered.

If S is an n-subsemigroup of (R,g), then on $R\times S^{n-1}$ an equivalence relation $\sim$ is defined by $(r_1^n)\sim(s_1^n)$ iff there is $t_2^n \in S$ such that

$$g(g(r_1,s_2^n),t_2^n) = g(g(s_1,r_2^n),t_2^n).$$

If $R\times S^{n-1}/\sim$ is denoted by $S^{-1}R$ then in $S^{-1}R$ operations $\overline{f}$, and $\overline{g}$ are defined so that $(S^{-1}R,\overline{f},\overline{g})$ is an (m,n)-ring, such that there is a homomorphism $\pi_S: R \longrightarrow S^{-1}R$ so that $\pi_S(S)$ is contained in n-group $(S^{-1}S,\overline{g})$, and (m,n)-ring is cancellative with respect to the elements of $S^{-1}S$. It is proved that $(S^{-1}R,\overline{f},\overline{g})$ is universal with respect to these properties, and some related results.

First, some basic definitions and notations will be given. General references are [1] and [3] .

The sequence $x_m,x_{m+1},\dots,x_n$ is denoted by $\{x_i\}_{i=m}^n$ or x_m^n. If $m>n$ then x_m^n is considered empty, and if

$x_i = x$ for all $i \in \mathbb{N}_n = \{1,\dots,n\}$ then x^n is denoted by $\overset{n}{x}$. For $n \leqslant 0$ $\overset{n}{x}$ will be considered empty.

An element $e \in Q$ of an n-groupoid (Q,f) is called idempotent iff $f(\overset{n}{e}) = e$.

An element $e \in Q$ of an n-groupoid (Q,f) is an identity element in (Q,f) iff $f(\overset{i-1}{e}, x, \overset{n-i}{e}) = x$, for every $x \in Q$, and every $i \in \mathbb{N}_n$.

An n-groupoid (Q,f) is commutative iff the following identity holds

$$f(x^n) = f(x_{\sigma(1)}^{\sigma(n)}),$$

for every permutation σ of the set $\mathbb{N}_n$.

A mapping $\varphi: Q \to S$ of an n-groupoid (Q,f) into an n-groupoid (S,g) is a homomorphism iff the identity

$$\varphi(f(x_1^n)) = g(\{\varphi(x_i)\}_{i=1}^n)$$

holds.

An n-groupoid (Q,f) is an n-semigroup iff

$$f(x_1^i, f(x_{i+1}^{i+n}), x_{i+n+1}^{2n-1}) = f(x_1^j, f(x_{j+1}^{j+n}), x_{j+n+1}^{2n-1})$$

holds for every $x_1^{2n-1} \in Q$, and every $i,j \in \{0,\dots,n-1\}$.

An n-semigroup is i-cancellative, $i \in \mathbb{N}_n$, with respect to $M \subseteq Q$ iff

$$f(a_1^{i-1}, x, a_{i+1}^n) = f(a_1^{i-1}, y, a_{i+1}^n) \text{ implies } x = y,$$

whenever $a_1^n \in M$. If an n-semigroup (Q,f) is i-cancellative with $M = Q$, for every $i \in \mathbb{N}_n$, then it is called cancellative.

An n-groupoid (Q,f) is an n-quasigroup iff the equation $f(a_1^{i-1}, x, a_{i+1}^n) = b$ has a unique solution x for every $a_1^n, b \in Q$, and every $i \in \mathbb{N}_n$.

An n-group (Q,f) is an n-semigroup which is also an n-quasigroup.

In a commutative n-group (Q,f) an element e is idempotent iff e is identity element.

For every $a \in Q$ in an n-group (Q,f) there is unique $x \in Q$ such that $f(\overset{n-1}{a},x) = a$. That x is denoted by $\bar{a}$ and is called the querelement of a. For every $a,x \in Q$, and every $i \in \{2,\ldots,n\}$, we have

$$f(x,\overset{i-2}{a},\bar{a},\overset{n-i}{a}) = f(\overset{i-2}{a},\bar{a},\overset{n-i}{a},x) = x.$$

It can be proved easily that $\varphi(\bar{a}) = \overline{\varphi(a)}$ for every n-group homomorphism φ, and every $a \in Q$, and that if n-group is commutative then $\overline{f(x_1^n)} = f(\bar{x}_1^n)$ holds.

An algebra (R,f,g) is called an (m,n)-ring iff

(i) (R,f) is a commutative m-group,

(ii) (R,g) is an n-semigroup,

(iii) the following distributive laws hold for every $i \in \mathbb{N}_n$, and every $a_1^n, b_1^m \in R$

$$g(a_1^{i-1},f(b_1^m),a_{i+1}^n) = f(\{g(a_1^{i-1},b_j,a_{i+1}^n)\}_{j=1}^m).$$

Since this notation is rather complicated it will be simplyfied to $f(a_1^m) = a_1+a_2+\ldots+a_m$, and $g(b_1^n) = b_1b_2\ldots b_n$ which is much more suggestive but much more imprecize. $a_1+\ldots+a_k$ makes sense only if $k=1 \bmod(m-1)$, $b_1\ldots b_l$ makes sense only if $l=1 \bmod(n-1)$ and such words are called admissible. Admissible word $b_1\ldots b_l$ where $b_i=b$ for $i \in \mathbb{N}_l$ is denoted by $(b)^l$. $(b)^l$ is considered empty for $l \leq 0$.

The commutative m-group (R,f) of the (m,n)-ring (R,f,g) will be called the additive m-group of (m,n)-ring, and n-semigroup (R,g) will be called the multiplicative n-semigroup of the (m,n)-ring R.

The (m,n)-ring is commutative iff its multiplicative n-semigroup is commutative.

If the multiplicative n-semigroup of an (m,n)-ring (R,f,g) has an n-subsemigroup (S,g), which is an n-group, then the querelement of an element $a \in S$, with respect to the operation g is denoted by $\underline{a}$.

An element 0 (or 0_R when necessary) in an (m,n)-ring R is zero of R iff $g(a_1^{i-1},0,a_{i+1}^n) = 0$ for every $a_1^n \in R$, and every $i \in \mathbb{N}_n$. An (m,n)-ring may have at most one zero. A zero of R is clearly additive and multiplicative idempotent in R but converse does not necessarily hold.

By R^* will be denoted the set of non-zero elements in the (m,n)-ring R.

An (m,n)-ring (R,f,g) is cancellative with respect to $S \subseteq R$, iff the multiplicative n-semigroup of R is cancellative with respect to S. If $S = R^*$ then R is called cancellative. A commutative cancellative (m,n)-ring is called an integral (m,n)-domain.

An (m,n)-subring I of the (m,n)-ring R is an ideal of R iff

(i) (I,f) is an n-subgroup of the additive n-group of R.

(ii) $g(r_1^{i-1},a,r_{i+1}^n) \in I$ for every $r_1^n \in R$, every $a \in I$, and every $i \in \mathbb{N}_n$.

Let $I_1,\dots,I_k$ be ideals of (m,n)-ring R where $k \equiv 1 \bmod(m-1)$. $J = \{x \in R \mid x = a_1+\dots+a_k,\ a_i \in I_i,\ i \in \mathbb{N}_k\}$ is an ideal of R which is denoted by $I_1+\dots+I_k$, and called sum of ideals I_i, $i \in \mathbb{N}_k$.

Let $I_1,\dots,I_l$ be ideals of (m,n)-ring R where $l \equiv 1 \bmod(n-1)$, and $J = \{x \in R \mid x = a_{11}\dots a_{1l}+\dots+a_{k1}\dots a_{kl}$, $a_{ij} \in I_j$, $i \in \mathbb{N}_k$, $j \in \mathbb{N}_l$, $k \equiv 1 \bmod(m-1)$. If R is commutative (m,n)-ring then J is an ideal which is denoted by $I_1\dots I_l$ and called the product of ideals $I_1,\dots,I_l$.

In this paper all (m,n)-rings are commutative.

DEFINITION 1. Let S be an n-subsemigroup of the multiplicative n-semigroup of a commutative (m,n)-ring R. On $R \times S^{n-1}$ define relation $\sim$ by

$(r_1^n) \sim (s_1^n)$ iff there are $t_1^{n-1} \in S$ such that

$r_1 s_2 \dots s_n t_1 \dots t_{n-1} = s_1 r_2 \dots r_n t_1 \dots t_{n-1}$.

THEOREM 1. The relation $\sim$ defined in the definition is an equivalence relation on $R \times S^{n-1}$.

Proof. The proof of reflexivity and symmetry is immediate, and the proof of transitivity will be given for (m,3)-rings since the notation in general case becomes to complicated.

(1) $(r_1, r_2, r_3) \sim (s_1, s_2, s_3)$ iff $r_1 s_2 s_3 t_1 t_2 = s_1 r_2 r_3 t_1 t_2$,

(2) $(s_1, s_2, s_3) \sim (u_1, u_2, u_3)$ iff $s_1 u_2 u_3 v_1 v_2 = u_1 s_2 s_3 v_1 v_2$,

for some $t_1, t_2, v_1, v_2 \in S$, so we have from (1)

$$r_1 u_2 u_3 (s_2 t_1 v_1)(s_3 t_2 v_2) = s_1 r_2 r_3 t_1 t_2 u_2 u_3 v_1 v_2 ,$$

and from (2)

$$s_1 u_2 u_3 v_1 v_2 t_1 t_2 r_2 r_3 = u_1 r_2 r_3 (s_2 t_1 v_1)(s_3 t_2 v_2) ,$$

so we have finally

$$(r_1, r_2, r_3) \sim (u_1, u_2, u_3).$$

Remark. When the n-subsemigroup S is cancellative then the relation $\sim$ is equivalent to the relation introduced in [2] .

DEFINITION 2. The equivalence class of (s_1^n), with respect to $\sim$, will be denoted by $[s_1^n]$. If $T \subseteq R$ then the set of $[s_1^n]$, where $s_1 \in T$, and $s_2^n \in S$ is denoted by $S^{-1}T$.

THEOREM 2. Let in the set $S^{-1}R$, of the equivalence classes of $\sim$ define operations in the following way:

Let $[a_1^n], [b_1^n], [c_1^n], \ldots, [d_1^n], [e_1^n]$ be m elements of $S^{-1}R$, define

(i) $[a_1^n] + [b_1^n] + [c_1^n] + \ldots + [d_1^n] + [e_1^n] =$

$$= [(a_1 b_2 \ldots b_n \ldots e_2 \ldots e_n + b_1 a_2 \ldots a_n c_2 \ldots c_n \ldots e_2 \ldots e_n + \ldots$$

$$\ldots + e_1 a_2 \ldots a_n \ldots d_2 \ldots d_n) x_{12} \ldots x_{1n} \ldots x_{k2} \ldots x_{kn},$$

$$, a_2 b_2 \ldots d_2 e_2 x_{12} \ldots x_{k2}, \ldots, a_n b_n \ldots d_n e_n x_{1n} \ldots x_{kn})] ,$$

where k is a number such that the words $a_i b_i \ldots d_i e_i x_{1i} \ldots x_{ki}$ become admissible for multiplicative n-semigroup, and $x_{ij} \in S$, $i \in \mathbb{N}_k$, $j \in \mathbb{N}_n$.

Let $[a_1^n], [b_1^n], \ldots, [e_1^n]$ be n elements of $S^{-1}R$, define

(ii) $[a_1^n][b_1^n] \ldots [e_1^n] = [a_1 b_1 \ldots e_1, \ldots, a_n b_n \ldots e_n]$.

Then $(S^{-1}R, +, \cdot)$ is an (m,n)-ring.

Proof. Direct verification.

DEFINITION 3. The (m,n)-ring defined in theorem 2. is called the localization of R at S.

COROLLARY 1. For every $a_1^m \in R$, and every $b_2^n \in S$

$$[a_1, b_2, \ldots, b_n] + \ldots + [a_m, b_2, \ldots, b_n] =$$
$$= [a_1 + \ldots + a_m, b_2, \ldots, b_n] .$$

Proof.

$$[a_1, b_2, \ldots, b_n] + \ldots + [a_m, b_2, \ldots, b_n] =$$
$$= [(a_1(b_2 \ldots b_n)^{m-1} + \ldots + a_m(b_2 \ldots b_n)^{m-1}) x_{12} \ldots x_{1n} \ldots x_{k2} \ldots x_{kn},$$
$$, (b_2)^m x_{12} \ldots x_{k2}, \ldots, (b_n)^m x_{1n} \ldots x_{kn}] = [a_1 + \ldots + a_n, b_2, \ldots, b_n]$$

since we have

$$(a_1 + \ldots + a_m)(b_2)^m \ldots (b_n)^m x_{12} \ldots x_{k2} \ldots x_{1n} \ldots x_{kn} =$$
$$= (a_1(b_2 \ldots b_n)^{m-1} + \ldots + a_m(b_2 \ldots b_n)^{m-1}) x_{12} \ldots x_{1n} \ldots x_{k2} \ldots$$
$$\ldots x_{kn} b_2 \ldots b_n .$$

COROLLARY 2. If I is an ideal of an (m,n)-ring R then $S^{-1}I$ is an ideal in $S^{-1}R$.

Proof. It follows immediately from the definition of an ideal and theorem 2.

COROLLARY 3. *If* $I_1, \dots, I_k$ *are ideals of an* (m,n)-*ring* R, *where* $k \equiv 1 \mod(m-1)$, *then*

$$S^{-1}(I_1 + \dots + I_k) = S^{-1}I_1 + \dots + S^{-1}I_k .$$

Proof. It follows from theorem 2 and corollary 1.

COROLLARY 4. *If* I,J *are ideals of an* (m,n)-*ring* R *then* $S^{-1}(I \cap J) = S^{-1}I \cap S^{-1}J$.

COROLLARY 5. *If* $J_1, \dots, J_l$ *are ideals of an* (m,n)-*ring* R, *where* $l \equiv 1 \mod(n-1)$ *then*

$$S^{-1}(J_1 \dots J_l) = (S^{-1}J_1)\dots(S^{-1}J_l) .$$

Proof. It follows from theorem 2, and corollary 1 if $a_1 = i_1 \dots i_l$, $b_1 = j_1 \dots j_l$, $c_1 = k_1 \dots k_l$, ..., $d_1 = p_1 \dots p_l$, $e_1 = q_1 \dots q_l$, where $i_1, j_1, k_1, \dots, p_1, q_1 \in J_1$, ..., $i_l, j_l, k_l, \dots, p_l, q_l \in J_l$.

THEOREM 3. $S^{-1}S$ *is a multiplicative* n-*group*.

Proof. One checks directly that

$$x = [a_1 s_2 \dots s_n \dots t_2 \dots t_n, a_2 s_1 \dots t_1, a_3, \dots, a_n]$$

is a solution of the equation

$$(3) \qquad x[s_1^n]\dots[t_1^n] = [a_1^n] .$$

Since R is commutative (m,n)-ring it follows that $S^{-1}S$ is an n-group ([4], p.217).

THEOREM 4. (m,n)-*ring* $S^{-1}R$ *is cancellative with respect to the elements of* $S^{-1}S$.

Proof. Since R is commutative (m,n)-ring it is sufficient to prove 1-cancellativity. Let

$$[x_1^n][a_1^n]\dots[c_1^n] = [y_1^n][a_1^n]\dots[c_1^n] .$$

Then for some $t_2^n \in S$ we have

$$(x_1a_1\ldots c_1y_2a_2\ldots c_2\ldots y_na_n\ldots c_n)t_2\ldots t_n =$$
$$= (y_1a_1\ldots c_1x_2a_2\ldots c_2\ldots x_na_n\ldots c_n)t_2\ldots t_n \quad ,$$

or

$$(x_1y_2\ldots y_n)a_1\ldots c_1\ldots a_n\ldots c_nt_2\ldots t_n =$$
$$= (y_1x_2\ldots x_n)a_1\ldots c_1\ldots a_n\ldots c_nt_2\ldots t_n \quad .$$

Since $a_1\ldots c_1\ldots a_n\ldots c_nt_2\ldots t_n = u_2\ldots u_n$ it follows that $[x_1^n] = [y_1^n]$.

THEOREM 5. <u>The mapping</u> $\pi_S : R \longrightarrow S^{-1}R$ <u>defined by</u> $\pi_S : a \longmapsto [as_2\ldots s_n, s_2,\ldots,s_n]$, $s_2^n \in S$, <u>is well-defined homomorphism of</u> (m,n)-<u>rings</u>.

<u>Proof</u>. Let $t_2^n \in S$. One checks easily that

$$[at_2\ldots t_n, t_2,\ldots,t_n] = [as_2\ldots s_n, s_2,\ldots,s_n]$$

so π_S is well-defined.

From corollary 1 it follows that

$$\pi_S(a_1 + \ldots + a_m) = \pi_S(a_1) + \ldots + \pi_S(a_m) \; .$$

$$\pi_S(a\ )\ldots\pi_S(a_n) = [a_1s_2\ldots s_n, s_2,\ldots,s_n]\ldots$$
$$\ldots[a_ns_2\ldots s_n, s_2,\ldots,s_n] = [a_1\ldots a_n(s_2)^n\ldots(s_n)^n, (s_2)^n,\ldots$$
$$\ldots,(s_n)^n] = [a_1\ldots a_ns_2\ldots s_n, s_2,\ldots,s_n] = \pi_S(a\ \ldots a_n) \; .$$

THEOREM 6. <u>When</u> $(R,\cdot)$ <u>is cancellative</u> n-<u>semigroup with respect to</u> S, <u>then the homomorphism</u> π_S, <u>defined in theorem</u> 5, <u>is a monomorphism</u>.

<u>Proof</u>. If $[as_2\ldots s_n, s_2,\ldots,s_n] = [bs_2\ldots s_n, s_2,\ldots,s_n]$ then $as_2\ldots s_ns_2\ldots s_nt_2\ldots t_n = bs_2\ldots s_ns_2\ldots s_nt_2\ldots t_n$, for $t_2^n \in S$, and since R is cacellative with respect to S it follows that $a = b$.

THEOREM 7. <u>When</u> S <u>is an</u> n-<u>group then the homomorphism</u> π_S, <u>defined in theorem</u> 5, <u>is an isomorphism</u>.

<u>Proof</u>. Let $[t, u_2,\ldots,u_n]$ be arbitrary element of $S^{-1}R$.

If π_S is onto then there should exist an $[ss_2\dots s_n, s_2,\dots,s_n]$ such that $[ss_2\dots s_n, s_2,\dots,s_n] = [t,u_2,\dots,u_n]$ or equivalently $ss_2\dots s_n u_2\dots u_n x_2\dots x_n = ts_2\dots s_n x_2\dots x_n$ for some $x_2^n \in S$. Since S is an n-group then it suffices that there is an $s \in R$ such that $ss_2\dots s_n u_2\dots u_n = ts_2\dots s_n$. If $s = t(u_2)^{n-3}\underline{u_2}\dots(u_n)^{n-3}\underline{u_n}$ then, because in an n-group $(u_i)^{n-2}\underline{u_i}y = y$ holds for every $y \in S$, it follows that $ss_2\dots s_n u_2\dots u_n = ts_2\dots s_n$ holds and so π_S is surjective. By theorem 6 it is injective.

THEOREM 8. *Let* S *be an n-subsemigroup of the multiplicative n-semigroup of an (m,n)-ring* R, *and let* T *be another (m,n)-ring. If* $\varphi : R \to T$ *is an (m,n)-ring homomorphism such that* $\varphi(S)$ *is an n-group in the multiplicative n-semigroup* $(T^*,\cdot)$ *then there is unique homomorphism* $\overline{\varphi} : S^{-1}R \to T$ *such that* $\overline{\varphi}\pi_S = \varphi$.

Proof. Let us define $\overline{\varphi} : S^{-1}R \to T$ by

$$\overline{\varphi}([r,s_2,\dots,s_n]) = \varphi(r)(\varphi(s_2))^{n-3}\underline{\varphi(s_2)}\dots(\varphi(s_n))^{n-3}\underline{\varphi(s_n)}.$$

Using the fact that $\underline{\varphi(x_1\dots x_n)} = \underline{\varphi(x_1)}\dots\underline{\varphi(x_n)}$ from the definitions of addition and multiplication easily follows that $\overline{\varphi}$ is well-defined homomorphism of rings such that $\overline{\varphi}\pi_S = \varphi$.

Let ψ be an another homomorphism such that $\psi\pi_S = \varphi$. Then for every $s \in S$, $\psi(\pi_S(s))$ has multiplicative querelement in T so $\underline{\psi(\pi_S(s))} = \psi(\underline{\pi_S(s)})$.
$x = [r,s,\dots,s]$ is the solution of the equation

$$x[s_2t_2\dots t_n, t_2,\dots,t_n]\dots[s_nt_2\dots t_n, t_2,\dots,t_n] = [rt_2\dots t_n, t_2,\dots,t_n]$$

which is checked directly. Let us denote $[s_it_2\dots t_n, t_2,\dots,t_n]$ by u_i, $i=2,\dots,n$. If u_i are elements of an n-group then

$$y = [rt_2\dots t_n, t_2,\dots,t_n](u_2)^{n-3}\underline{u_2}\dots(u_n)^{n-3}\underline{u_n}$$

is a solution too so

$$[r,s_2,\dots,s_n] = [rt_2\dots t_n, t_2,\dots,t_n](u_2)^{n-3}\underline{u_2}\dots(u_n)^{n-3}\underline{u_n} \quad .$$

It follows that

$$\Psi([r,s_2,\dots,s_n]) = \Psi([rt_2\dots t_n, t_2,\dots,t_n](u_2)^{n-3}\underline{u_2}\dots(u_n)^{n-3}\underline{u_n}) =$$
$$= \Psi([rt_2\dots t_n, t_2,\dots,t_n])(\Psi(u_2))^{n-3}\underline{\Psi(u_2)}\dots(\Psi(u_n))^{n-3}\underline{\Psi(u_n)}.$$

Using that $u_i = \pi_S(s_i)$, $i=2,\dots,n$, and $\Psi\pi_S = \varphi$ we have

$$\Psi([r,s_2,\dots,s_n]) = \varphi(r)(\varphi(u_2))^{n-3}\underline{\varphi(u_2)}\dots(\varphi(u_n))^{n-3}\underline{\varphi(u_n)} =$$
$$= \overline{\varphi}([r,s_2,\dots,s_n])$$

and so $\Psi = \overline{\varphi}$.

THEOREM 9. <u>Let</u> $S \subseteq T$ <u>be</u> n-<u>subsemigroups</u> <u>of</u> <u>the</u> <u>multiplicative</u> n-<u>semigroup</u> <u>of</u> <u>a</u> <u>commutative</u> (m,n)-<u>ring</u> R. <u>Then</u>

(i) <u>There</u> <u>is</u> <u>a</u> <u>unique</u> <u>homomorphism</u> $\varphi: S^{-1}R \to T^{-1}R$ <u>such</u> <u>that</u> $\pi_T = \varphi\pi_S$.

(ii) $S^{-1}T$ <u>is</u> <u>an</u> n-<u>subsemigroup</u> <u>of</u> <u>the</u> <u>multiplicative</u> n--<u>semigroup</u> <u>of</u> <u>the</u> (m,n)-<u>ring</u> $S^{-1}R$.

(iii) (m,n)-<u>rings</u> $T^{-1}R$ <u>and</u> $(\pi_S(T))^{-1}(S^{-1}R)$ <u>are</u> <u>isomorphic</u>.

(iv) (m,n)-<u>rings</u> $(\pi_S(T))^{-1}(S^{-1}R)$ <u>and</u> $(S^{-1}T)^{-1}(S^{-1}R)$ <u>are</u> <u>isomorphic</u>.

<u>Proof</u>. To prove (i), let $t_2^n \in T$, $s_2^n \in S$, and since $S \subseteq T$ then as in proof of theorem 5 it follows that $\pi_T(s) = [st_2\dots t_n, t_2,\dots,t_n] = [ss_2\dots s_n, s_2,\dots,s_n] \in S^{-1}S$ so by theorem 3 $\pi_T(S)$ is an n-group. By theorem 8 it follows that there is unique homomorphism φ such that $\pi_T = \varphi\pi_S$.

The proof of (ii) is immediate.

The proof of (iii) follows from the fact that $(\pi_S(T))^{-1}(S^{-1}R)$ is obtained as composition of

$$R \xrightarrow{\pi_S} S^{-1}R \xrightarrow{\pi_{\pi_S(T)}} (\pi_S(T))^{-1}(S^{-1}R),$$

so $(\pi_S(T))^{-1}(S^{-1}R)$ also has the universal property from the theorem 8. Since universal objects are unique up to isomorphism it follows that $T^{-1}R$ and $(\pi_S(T))^{-1}(S^{-1}R)$ are isomorphic.

The proof of (iv) is obtained similarly as that of (iii).

ACKNOWLEDGMENT. The author wishes to thank Professor Đ. Čupona and W. Dudek for their very useful suggestions which helped him to improve this paper.

REFERENCES

1. Crombez, G., On (m,n)-rings, Abh. Math. Sem. Univ. Hamburg 37(1972), 180-199.

2. Crombez, G., Timm, J., On (m,n)-quotient rings, Abh. Math. Sem. Univ. Hamburg 37(1972), 200-203.

3. Leeson, J. J., Butson, A. T., On the general theory of (m,n)-rings, Algebra Universalis 11(1980), 42-76.

4. Post, E., Polyadic groups, Trans. Am. Math. Soc. 48(1940), 208-350.

Institute of Mathematics
Faculty of Natural Sciences
21 000 Novi Sad
Dr I. Djuričića 4

[illegible] also has the universal property (from [illegible] the theorem). Since universally [illegible] objects are unique up to isomorphism, it follows that [illegible] and [illegible] are isomorphic.

The proof of (iv) is obtained similarly as that of [illegible].

ACKNOWLEDGMENTS. The author wishes to thank Professor [illegible] and [illegible] for their very useful suggestions which helped him to improve this paper.

REFERENCES

[illegible]

[illegible]

[illegible]

[illegible]

PROCEEDINGS OF THE CONFERENCE „ALGEBRA AND LOGIC", ZAGREB 1984

INDUCTIVE DEFINITIONS IN ML_0

Dean Rosenzweig

Abstract. Sets and predicates defined by ordinary induction are, in a very strong sense, definable in the first layer of Martin-Löf's theory of types without universes or wellorderings, with or without function-types.

INTRODUCTION

Sets and predicates defined by induction can be conveniently constructed in Martin-Löf's theory of types (Martin-Löf (1978), (1984) are general references) using the machinery of "wellorderings", or, far less generally and somewhat less conveniently, using universes, i.e. treating names of types as objects. Both approaches, however, involve considerable strengthening of the basic arithmetical theory ML_0, which is precisely the theory of types without either wellorderings or universes. ML_0 has probably not been intended to stand alone, but it can certainly be viewed as a formalization of a definite body of mathematics; it might even be argued that it is a more suitable (in sense of Beeson (1981)) formalization of the same body of mathematics as, say, HA^{ω} (in some variants).

It encompasses a significant fragment of constructive mathematics including elementary analysis, as well as (or rather undistinguishable from, as argued by Martin-Löf (1978)) a significant part of computing science. This fragment would naturally include a definite class of inductively defined sets and predicates, namely those specified by "ordinary" as opposed to "generalized" induction in sense of Martin-Löf (1971); yet the means for their explicit construction are entirely lacking in ML_0, save for the set of natural numbers.

In this paper we show that they are definable in ML_0 in a very strong sense (as well as in the subsystem of ML_0 without function-types, named SA for "Skolem-arithmetics" by Jervell (1978)). In view of standard facts about

HA, together with results and techniques of Beeson (1982) (see also section 3) the sets and predicates of that class should be somehow definable; if ML_o is to be a suitable formalization of anything, they should be definable in as strong a sense as can be, so the results are anything but unexpected.

In section 1. we redescribe sets and predicates defined by ordinary induction so as to fit together with ML_o. In section 2. we explain what it means for them to be definable and what it means for an extension to be conservative, as ML_o is not an ordinary first-order theory, and show how isomorphism in a category introduced by J.Cartmell (1978) relates to definability. In section 3. we display isomorphs, in ML_o or in SA, of sets and predicates of section 1.

1. SETS AND PREDICATES DEFINED BY ORDINARY INDUCTION

In the theory of types sets exist as types, and predicates as type-valued functions, in view of interpretability of types as propositions. All types of ML_o are defined by means of rules, namely: rules of formation, which specify the conditions for something to be a type, rules of introduction, which specify how objects of a type are to be constructed, as well as what it means for two objects to be equal, rules of elimination, which specify the conditions for introducing functions over a type, and rules of conversion, which define functions introduced by elimination. Inductively defined types shall then be specified by rules of the following general form (we shall suppress their obvious equality-counterparts):

1.1. V - formation

$$\frac{b \in B_i}{V_i(b)\ \text{type}} \qquad\qquad i \in \{1,\dots,n\}.$$

1.2. V - introduction

$$\frac{a \in A_i \ \dots\ a_{rs} \in A_r,\ c_{rs} \in V_r(t_{rs}(a_{rs}))\dots}{c_{ij}(a,\ \dots a_{rs}, c_{rs} \dots\ ) \in V_i(t_{ij}(a))}$$

provided $t_{ij}(x) \in B_i \quad (x \in A_i)$,

$i \in \{1,\dots,n\}$, $j \in \{1,\dots,m_i\}$, $r \in R_{ij} \subseteq \{1,\dots,n\}$, $s \in S_{ijr} \subseteq \{1,\dots,m_r\}$.

1.3. V - elimination

$$\frac{b \in B_i \quad c \in V_i(b) \qquad \text{minor premisses}}{rec(c, \ldots d_{km} \ldots) \in C_i(b,c)}$$

provided $C_i(x,y)$ type $(x \in B_i,\ y \in V_i(x))$,

where $i,k \in \{1,\ldots,n\}$, $m \in \{1,\ldots,m_k\}$, and for any pair k,m there is a minor premiss of form

$$(x_k \in A_k \quad \ldots y_{rs} \in A_r, z_{rs} \in V_r(t_{rs}(y_{rs})),\ w_{rs} \in C_r(t_{rs}(y_{rs}), z_{rs}) \ldots)$$

$$d_{km}(x_k,\ \ldots y_{rs}, z_{rs}, w_{rs} \ldots) \in C_k(t_{km}(x_k), c_{km}(x_k,\ \ldots y_{rs}, z_{rs} \ldots))$$

with $r \in R_{km}$, $s \in S_{kmr}$.

1.4. V - conversion

$$\frac{a \in A_i \quad \ldots a_{rs} \in A_r, c_{rs} \in V_{rs}(t_{rs}(a_{rs})) \ldots \qquad \text{minor premisses}}{\begin{aligned} &rec(c_{ij}(a,\ \ldots a_{rs}, c_{rs} \ldots),\ \ldots d_{km} \ldots) \\ &\quad = d_{ij}(a,\ \ldots a_{rs}, c_{rs}, rec(c_{rs},\ \ldots d_{km} \ldots) \ldots) \\ &\quad\quad \in C_i({}_{ij}(a), c_{ij}(a,\ \ldots a_{rs}, c_{rs} \ldots)) \end{aligned}}$$

where ranges of i,j,r,s are as in V-introduction, and minor premisses and ranges of k,m are as in V-elimination.

1.5. The rules are graphically complicated, and will be, in section 3, reduced to equivalent rules that are simpler to write down in general form; the present form of rules is, however, very easy to recognize in special cases.

1.6. Examples

1.6.1. The set of symbolic expressions over a set Atom is specified by the following rules:

1.6.1.1. Sexp-formation

Sexp type

1.6.1.2. Sexp-introduction

$$\frac{a \in \text{Atom}}{\text{at}(a) \in \text{Sexp}} \qquad \frac{a \in \text{Sexp} \quad b \in \text{Sexp}}{\text{cons}(a,b) \in \text{Sexp}}$$

1.6.1.3. Sexp-elimination

$$\frac{c \in \text{Sexp} \quad \begin{matrix}(x \in \text{Atom}) \\ d(x) \in C(\text{at}(x))\end{matrix} \quad \begin{matrix}(x \in \text{Sexp} \quad y \in C(x) \quad z \in \text{Sexp} \quad w \in C(z)) \\ e(x,y,z,w) \in C(\text{cons}(x,z))\end{matrix}}{\text{Sexprec}(c,d,e) \in C(c)}$$

1.6.1.4. Sexp-conversion

$$\frac{a \in \text{Atom} \qquad \text{minor premisses}}{\text{Sexprec}(\text{at}(a),d,e) = d(a) \in C(\text{at}(a))}$$

$$\frac{a \in \text{Sexp} \quad b \in \text{Sexp} \qquad \text{minor premisses}}{\begin{matrix}\text{Sexprec}(\text{cons}(a,b),d,e) \\ = e(a,\text{Sexprec}(a,d,e),b,\text{Sexprec}(b,d,e)) \in C(\text{cons}(a,b)).\end{matrix}}$$

1.6.2. The predicates of being a list and of being an element of a list are specified by the following rules:

1.6.2.1. Formation

$$\frac{a \in \text{Sexp}}{\text{Listelement}(a)\ \text{type}} \qquad \frac{a \in \text{Sexp}}{\text{List}(a)\ \text{type}}$$

1.6.2.2. Introduction

$$\frac{a \in \text{Atom}}{c_1(a) \in \text{Listelement}(\text{at}(a))} \qquad \frac{a \in \text{Sexp} \quad b \in \text{List}(a)}{c_2(a,b) \in \text{Listelement}(a)}$$

$$c_3 \in \text{List}(\text{at}(\text{nil}))$$

$$\frac{a \in \text{Sexp} \quad b \in \text{Listelement}(a) \quad c \in \text{Sexp} \quad d \in \text{List}(c)}{c_4(a,b,c,d) \in \text{List}(\text{cons}(a,c))}$$

1.6.2.3. Elimination

$$\frac{a \in \text{Sexp} \quad c \in \text{Listelement}(a) \qquad \text{minor premisses}}{\text{rec}(c,e,f,g,h) \in C(a,c)}$$

$$\frac{a \in \text{Sexp} \quad c \in \text{List}(a) \qquad \text{minor premisses}}{\text{rec}(c,e,f,g,h) \in D(a,c)}$$

provided

$C(x,y)$ type $(x \in \text{Sexp},\ y \in \text{Listelement}(x))$

$D(x,y)$ type $(x \in \text{Sexp},\ y \in \text{List}(x))$,

where the minor premisses are:

$$\begin{array}{c} (x \in \text{Atom}) \\ e(x) \in C(\text{at}(x),c_1(x)) \end{array} \qquad \begin{array}{c} (x \in \text{Sexp},\ y \in \text{List}(x),\ z \in D(x,y)) \\ f(x,y,z) \in C(x,c_2(x,y)) \end{array}$$

$$g \in D(\text{at}(\text{nil}),c_3)$$

$$\begin{array}{c} (x \in \text{Sexp} \quad y \in \text{Listelement}(x) \quad z \in C(x,y) \quad u \in \text{Sexp} \quad v \in \text{List}(u) \quad w \in D(u,v)) \\ h(x,y,z,u,v,w) \in D(\text{cons}(x,u),c_4(x,y,u,v) \end{array}$$

1.6.2.4. Conversion

$$\frac{a \in \text{Atom} \qquad \text{minor premisses}}{\text{rec}(c_1(a),e,f,g,h) = e(a) \in C(\text{at}(a),c_1(a))}$$

$$\frac{a \in \text{Sexp} \quad b \in \text{List}(a) \qquad \text{minor premisses}}{\text{rec}(c_2(a,b),e,f,g,h) = f(a,b,\text{rec}(b,e,f,g,h) \in C(a,c_2(a,b))}$$

$$\text{rec}(c_3,e,f,g,h) = g \in D(\text{at}(\text{nil}),c_3)$$

$$\frac{a \in \text{Sexp} \quad b \in \text{Listelement}(a) \quad c \in \text{Sexp} \quad d \in \text{List}(c) \quad \text{minor premisses}}{\begin{array}{c}\text{rec}(c_4(a,b,c,d),e,f,g,h) = h(a,b,\text{rec}(b,e,f,g,h),c,d,\text{rec}(d,e,f,g,h)) \\ \in D(\text{cons}(a,c),c_4(a,b,c,d)).\end{array}}$$

1.6.3. The predicate Eval(x,y,z), meaning "a LISP-evaluator, given the Sexp x with the environment (cf. Allen (1978)) y, terminates yielding value z", can be specified with not many more then twenty introduction-rules, provided the type of environments has already been defined.

1.6.4. Given Eval as above, we can, by standard methods, specify a universal predicate for all one-place recursively enumerable predicates over the type Sexp, with symbolic expressions as r.e. indices.

1.7. The semantics of cannonical objects (Martin-Löf (1978), (1984)) can be straightforwardly extended to rules of form 1.1-1.4.

1.8. Sets specified by rules of form 1.1-1.4. are holomorph (Ger. zahlenartig aufgebaut) in sense of Péter (1967).

1.9. The rules of elimination and conversion can be produced mechanically, as soon as the rules of formation and introduction are given.

In presençe of rules for identity-types, they entail the following statement:

For any system of functions d_{km} which validate the minor premisses of 1.3. there is a unique system of functions

$$f_i(z) \in C_i(y,z)(y \in B_i,\ z \in V_i(y))$$

which satisfy the recursion-equations

$$f_i(c_{ij}(x, \ldots y_{rs}, z_{rs} \ldots)) = d_{ij}(x, \ldots y_{rs}, z_{rs}, f_r(z_{rs}) \ldots)$$
$$\in C_i(t_{ij}(x), c_{ij}(x, \ldots y_{rs}, z_{rs} \ldots))(x \in A_i,\ \ldots y_{rs} \in A_r, z_{rs} \in V_r(t_{rs}(y_{rs}))),$$
$$i \in \{1,\ldots,n\},\quad j \in \{1,\ldots,m_i\}.$$

1.1o. The rules 1.6.1. and 1.6.2. may be seen as proof-theoretic unwinding of "domain equations"

$$\text{Sexp} \simeq \text{Atom} + \text{Sexp Sexp},$$

$$\text{Listelement}(x) \simeq \text{Isatom}(x) + \text{List}(x) \quad (x \in \text{Sexp})$$

$$\text{List}(x) \simeq \text{Isnil}(x) + (\exists u \in \text{Sexp}\cdot\text{Sexp})((x = \text{cons}(p(u),q(u)))\ \text{Listelement}(p(u))\cdot\text{List}(q(u))) \quad (x \in \text{Sexp}),$$

with the obvious predicates Isatom, Isnil, while $(a = b)$ is shorthand for $I(A,a,b)$, to be used when no ambiguity as to type can arise. The rules are indeed determined by the equations in a sense which will be made precise in the next section.

2. DEFINABILITY AND CONSERVATIVITY

2.1. T will in the sequel denote a subsystem of ML_0 containing all of its rules except perhaps those for function-types (in that case possibly some of their instances), and perhaps some rules of form 1.1-1.4. We shall say that a system of unary type-valued functions $\ldots V_i \ldots$, $i \in \{1,\ldots,n\}$, validates the rules 1.1-1.4. in T if types $\ldots A_i, B_i \ldots$, functions $\ldots t_{ij}, c_{ij} \ldots$ and a functional rec can be defined so that the rules 1.1.-1.4. are derived rules of T. We shall also say that predicates specified by those rules are definable in T if there are type-valued functions which validate them in T.

2.1.1. Weaker notions, such as existence of logically equivalent type-valued functions (predicates), would be grossly inadequate for the theory of types; extending T by rules for a predicate which is only definable in such a weak sense can be very nonconservative (see 2.5.).

In view of the formulae-as-types interpretation of proof-theory, this suggests a notion of deductive definability of predicates and connectives in a system of natural deduction which is stronger then the usual notion of logical definability. Deductive definability would preserve some proof-theoretic results, such as normal-form theorems. Disjunction is for instance definable deductively in intuitionistic arithmetic, while only logically in classical logic. The Shaeffer-operation, introduced by K. Došen in this volume, defines all operations of intuitionistic propositional logic only logically, its rules do not suffice to define the rules of introduction and elimination of other propositional constants so as to validate the inversion principle in form of standard rules of reduction.

2.1.2. If $\ldots V_i \ldots$ validate the rules 1.1.-1.4. we can, assuming $y \in B_i$ and using 1.9. with appropriate choices of d_{km}, define functions which extract the following information form a $z \in V_i(y)$:

a) $ind1(z) \in N_n$, so that $ind1(z) = i \in N_n$

b) $ind2(z) \in N_{m_i}$, so that for some j $ind2(z) = j \in N_{m_i}$

c) $a(z) \in A_i$, so that $y = t_{ij}(a(z)) \in B_i$

d) $\ldots$
$a_{rs}(z) \in A_r$, $r \in R_{ij}$, $s \in S_{ijr}$
$\ldots$

e) $\dots$
$c_{rs}(z) \in V_r(t_{rs}(a_{rs}(z))), \quad r \in R_{ij}, \; s \in S_{ijr}$
$\dots$

so that

f) $z = c_{ij}(a(z), \dots a_{rs}(z), c_{rs}(z) \dots) \in V_i(t_{ij}(a(z)))$

is derivable in T.

Equalities c),f) are proved by 1.3. or 1.9. using appropriate identity-types for C_i (and a function $t(i,j,x)$ defined by rules for finite types so as to take the same values as $t_{ij}(y)$).

2.2. The fact that each object of a $V_i(y)$ is completely determined by information 2.1.2. invites category-theoretic formulation.

Objects of the category C_T will be contexts, i.e. sequences of assumptions

$$x_1 \in A_1,\; x_2 \in A_2(x_1), \dots, x_n \in A_n(x_1, \dots, x_{n-1})$$

such that the judgements

A_1 type

$\dots$

$A_n(x_1, \dots x_{n-1})$ type $(x_1 \in A_1, \dots, x_{n-1} \in A_{n-1}(x_1, \dots, x_{n-2}))$

are all derivable in T; if

$\underline{A} \equiv x_1 \in A_1, \dots, x_n \in A_n(x_1, \dots, x_{n-1})$

$\underline{B} \equiv y_1 \in B_1, \dots, y_m \in B_m(y_1, \dots, y_{m-1})$

are contexts, morphisms form $\underline{A}$ to $\underline{B}$ will be realizations of $\underline{B}$ in $\underline{A}$, i.e. sequences of n-ary functions $f_1, \dots, f_m$ such that the judgements

$f_1(x_1, \dots, x_n) \in B_1 \quad (\underline{A})$

$\dots$

$f_m(x_1, \dots, x_n) \in B_m(f_1(x_1, \dots, x_n), \dots, f_{m-1}(x_1, \dots, x_n)) \quad (\underline{A})$

are all derivable in T; objects and morphisms will be equal in C_T if the appropriate judgements of equality are derivable in T.

With the obvious composition and identities, C_T is a contextual category of Cartmell (1978), essentially a subcategory of the initial "strong Martin-Löf structure".

We shall say that an isomorphism $f_1, \dots, f_n$ of two contexts of equal length is structure-preserving if f_i is a function of $x_1, \dots, x_i$ only, and the inverses $g_1,\dots,g_n$ have the same property. It namely preserves the tree-structure of contexts (cf. Cartmell (1978)).

We shall say that a morphism of two contexts with the common initial segment $\underline{Q}$ is <u>above</u> $\underline{Q}$ if its first length($\underline{Q}$) components are the projections. To morphisms of $\underline{Q}$, $y \in A(x_1,\dots,x_n)$ to $\underline{Q}$, $z \in A'(x_1,\dots,x_n)$ above $\underline{Q}$ we shall simultaneously refer as morphisms from A to A' above $\underline{Q}$.

<u>2.3.</u> The information contained in 2.1.2. can now be expressed by a "domain-equation"

$$V_i \simeq (y)\ \dots+(\exists x \in A_i)((y=t_{ij}(x)) \times V_{ij})+\dots \qquad i \in \{1,\dots,n\},\ \ j \in \{1,\dots,m_i\},$$

where

$$V_{ij} \equiv \dots \times(\exists x \in A_{rs})V_r(t_{rs}(x))\times \dots,\quad r \in R_{ij},\ s \in S_{ijr},$$

$\simeq$ means isomorphism above $y \in B_i$, and the finite sums and products are obvious iterates of binary sums and products as type-constructors of T.

<u>2.3.1.</u> By 1.9. $\dots V_i \dots$ is a <u>minimal solution</u> of equations 2.3., i.e. for any other system of type-valued functions $\dots V_i' \dots$ over $\dots B_i \dots$ which solve the equations, there is a unique system of monomorphisms from V_i to V_i' above $y \in B_i$ which commute with the equations.

The domain-equations namely suggest recursion-equations for functions $h_i(y,z) \in V_i'(y)(y \in B_i, z \in V_i(y))$: from $\dots h_r(y_{rs},z_{rs})\dots$ reconstruct the r.h.s., map to $V_i'(y)$ by inverse-isomorphism and equate to $h_i(y,z)$; by 1.9. such $\dots h_i \dots$ exist and are unique, by the equations they are monomorphisms.

<u>2.4.</u> THEOREM. <u>If $\dots V_i, V_i' \dots$ are unary type-valued functions over $\dots B_i \dots$ in T, and $\dots V_i \dots$ validate the rules 1.1-1.4. in T, the following statements are equivalent for $\dots V_i' \dots$ in</u> T:

a) <u>they are isomorphic to $\dots V_i \dots$ above $\dots B_i \dots$</u>

b) <u>they form a minimal solution to equations 2.3.</u>

c) <u>they validate the rules 1.1-1.4.</u>

<u>2.4.1.</u> <u>Proof</u>. We have already checked that c) implies b). Given b), the composition of monomorphisms from V_i to V_i' and back will commute with the equations, so, being unique, it must be the identity; hence a).

To prove that a) implies c), we must, given the isomorphism $\dots f_i \dots$, construct c_{ij}' and rec'.

The information contained in introduction-rules and 1.9. is "category-theoretic" above B_i, what is claimed is existence of morphisms and a universal property, so 1.2. and 1.9. will hold for $\ldots V'_i \ldots$ if a) holds. This entails the choice

$$c'_{ij}(x, \ldots y_{rs}, z_{rs} \ldots) \equiv f_i(t_{ij}(x), c_{ij}(x, \ldots y_{rs}, f_r^{-1}(t_{rs}(y_{rs}), z_{rs}) \ldots),$$

where f_i is the isomorphism of V_i and V'_i above $y \in B_i$. What remains to be proved is precisely what 1.3. and 1.4. say more compared to 1.9., and that is a linguistic statement: there is a functional which solves the recursion-equations uniformly in $\ldots d_{km} \ldots$. Given the minor premisses

$$(x_k \in A_k \ldots y_{rs} \in A_r, z'_{rs} \in V'_r(t_{rs}(y_{rs})), w_{rs} \in C'_r(t_{rs}(y_{rs}), z'_{rs}) \ldots)$$

$$\ldots \qquad d'_{km}(x, \ldots y_{rs}, z'_{rs}, w_{rs} \ldots) \in C'_r(t_{rs}(y_{rs}), z'_{rs}) \qquad \ldots,$$

we can define

$$C_i(y,z) \equiv C'_i(y, f_i(y,z))$$

$$d_{km}(x, \ldots y_{rs}, z_{rs}, w_{rs} \ldots) \equiv d'_{km}(x, y_{rs}, f_r(t_{rs}(y_{rs}), z_{rs}), w_{rs} \ldots),$$

$$i,k \in \{1,\ldots,n\}, \ m \in \{1,\ldots,m_k\}.$$

Given $b \in B_i$, $c \in V'_i(b)$, by 1.3.

$$rec(f_i^{-1}(b,c), \ldots d_{km} \ldots) \in C'_i(b,c) \equiv C_i(b, f_i^{-1}(b,c)).$$

As $\ldots d_{km} \ldots$ can be defined uniformly in $\ldots d'_{km} \ldots$, and i,b can be, by 2.1.2. (which holds by 1.9., so holds for $\ldots V'_i \ldots$) extracted uniformly from c, we can define the functional

$$rec'(z', \ldots d'_{km} \ldots) \equiv rec(h(z'), \ldots d_{km} \ldots)$$

where

$$h(z') \equiv g(ind\,1(z'), t(ind\,1(z'), ind\,2(z'), z'))$$

and $g(i,y,z')$ is defined so as to take the same values as $f_i^{-1}(y,z')$ for $i \in N_n$, $y \in B_i$, $z' \in V'_i(y)$.

2.4.2. The same kind of theorem (stating the equivalence of a) and c), since in most other cases it does not make sense to claim anything like b)) holds for all (instances of) type-constructors of ML_o, by the same kind of proof.

2.5. Extending T by rules for a type-valued function which is definable in T, i.e. by rules which are already present in T in disguise, should be as conservative as possible. Although such a theorem is entirely trivial in case of first-order logic, for the theory of types it requires some care.

New types assume there the role not only of new formulae, but of new <u>sorts</u> as well, over which yet new predicates may be defined, which will themselves produce yet new sorts etc. The very notion of conservativity requires reformulation, as Martin-Löf's notion of judgement, and that is what we derive in the theory of types, is relative not only to language but to deductive apparatus as well. A derivation of a judgement in a context must contain derivations of all judgements which are needed to establish the context and some more, if it for instance derives $a = b \in A$, it must contain derivations of A type, $a \in A$, $b \in A$, these are the things we must know before we can meaningfully assert that $a = b \in A$. If T is extended to T^+ we can in that sense, among the judgements derivable in T^+, distinguish those for which it is meaningful to ask whether they are derivable in T already, namely those that presuppose only judgements which are derivable in T. We are thus compelled to an inductive definition.

<u>2.5.1.</u> We shall say that

- a judgement of form A type $(\underline{Q})$, derivable in T^+, is <u>of</u> $\underline{T}$ if all judgements required to establish $\underline{Q}$ as a context are T-derivable; it is <u>T-derivable</u> if for some A' $T^+ \vdash A = A'$ $(\underline{Q})$ and $T \vdash A'$ type $(\underline{Q}')$;

- a judgement of form $A = B$ $(\underline{Q})$, derivable in T^+, is of T if the judgements A type $(\underline{Q})$, B type $(\underline{Q})$ are both T-derivable; it is T-derivable if it is of T and $T \vdash A' = B'$ $(\underline{Q}')$;

- a judgement of form $a \in A$ $(\underline{Q})$, derivable in T^+, is of T if the judgement A type $(\underline{Q})$ is T-derivable; it is T-derivable if it is of T and for some a' $T^+ \vdash a = a' \in A$ $(\underline{Q})$ and $T \vdash a' \in A'$ $(\underline{Q}')$;

- a judgement of form $a = b \in A$ $(\underline{Q})$, derivable in T^+, is of T if the judgements A type $(\underline{Q})$, $a \in A$ $(\underline{Q})$, $b \in A$ $(\underline{Q})$ are all T-derivable; it is T-derivable if it is of T and $T \vdash a' = b' \in A'$ $(\underline{Q}')$.

<u>2.5.2.</u> If ML_0 is extended by the rules for the type of Brouwer's ordinals, $W(N_3,(x)(I(N_3,x,1)+I(N_3,x,2)\times N))$, or if SA is extended by the rules for $N \to N$, it is easy to concoct judgements of form $f(x) \in N$ $(x \in N)$ or $f(x) = g(x) \in N$ $(x \in N)$, which are derivable in T^+, of T but not T-derivable.

T-derivability of all judgements, derivable in T^+, which are of T, will be our notion of conservativity. Use of new types, if it is to be conservative, may not create new objects at old types, at most new names for old objects. Theorem 2.6. will verify that it relates to definability as it should. If the formulae-as-types interpretation of proof-theory is to make sense, this should be a way towards "more delicate proof-theoretic cosure conditions involving the deductions themselves" for systems of natural deduction, hinted at by Troelstra (1973, p.90); the conditions might require conservation not only of the class of (hypothetical) theorems under logical equivalence, but of classes (types or type-valued functions) of their proofs under type-theoretic isomorphism as well.

2.6. THEOREM. *If T^+ is T extended by rules for a system of type-valued functions ...V_i... which are definable in T, any judgement, derivable in T^+, which is of T is also T-derivable.*

2.6.1. *Proof*. A precise description of the self-suggesting transformation of derivations ("choose an inference by a V-rule such that above it there are no inferences by V-rules and which is not an assumption to be cancelled by V-elimination or V-conversion; replace it with an inference by a derived V'-rule; propagate the effect by substituting defined V'-constants for all occurences of V-constants originating from that inference throughout the rest of the derivation (essentially by Cartmell's pullback-mechanism, (1978)); do some other things, or more of the same, to ensure that you still have a derivation; continue") and a verification of its effects require induction over derivations. As is often the case, it seems that we have to prove a stronger statement in order to prove the induction-step.

In terms of contextual categories, derivations of the four forms of judgements establish contexts, equality of contexts, morphisms and equality of morphisms. Let Con(α) and Hom(α) be the classes of all contexts and morphisms which are established by (subderivations of) α. Closing Con(α) and Hom(α) under application of general rules of equality and substitution (hence under Cartmell's pullbacks) and imposing equalities as inherited from C_{T^+}, we obtain well-behaved compositions and identities, thus a (contextual) subcategory C_α of C_{T^+}. An induction-hypothesis which goes through is then the following statement about a derivation α:

Stat(α) There is a contextual functor (Cartmell (1978)) $F : C_\alpha \to C_T$ such that

a) for any object $\underline{A} \equiv x_1 \in A_1, \ldots, x_n \in A_n(x_1, \ldots, x_{n-1})$ of C_α there is a structure-preserving isomorphism $f_{\underline{A}} : \underline{A} \to F(\underline{A})$ of C_{T^+}, and $F(\underline{A})$ is of form

$$y_1 \in F(A_1), \ldots, y_n \in F(A_n)(y_1, \ldots, y_{n-1}) \quad \text{so that}$$

$$T^+ \vdash F(A_i)(y_1, \ldots, y_{i-1}) = F(A_i(f_1^{-1}(y_1), \ldots, f_{i-1}^{-1}(y_1, \ldots, y_{i-1}))$$

$(y_1 \in F(A_1),\dots,y_{i-1} \in A_{i-1}(y_1,\dots,y_{i-2}))$, $i \in \{1,\dots,n\}$,

where $f_1,\dots,f_n$ are the components of $f_{\underline{A}}$;

b) for any morphism $h : \underline{A} \to \underline{B}$ of C, $F(h) = f_{\underline{B}} \cdot h \cdot f_{\underline{A}}^{-1}$ in C_T+;

c) whenever the subderivation of α establishing $\underline{A}$ is a derivation in T, $F(\underline{A}) = \underline{A}$ and $f_{\underline{A}} = id_{\underline{A}}$ in C_T+.

Contextuality of a functor essentially means that it preserves the tree-structure of contexts, substitution and the type-forming operations of ML_o. If Stat(α) holds for arbitrary α, the functors generated by different derivations can be so chosen, by specifying $F(V_i)$, $i \in \{1,\dots,n\}$, as to agree on intersections of respective subcategories; we would thus have a functor from C_T+ to C_T which is a left adjoint, even a reflection, of the inclusion. Application of that functor would then produce the A', B', a',b' as required by the theorem.

Proof of Stat(α). By induction over α. We shall adopt the usual convention of suppressing all assumptions not explicitly shown in the rules of inference, what enforces the following definition:

$F(A) \equiv A$, $f_A(x) \equiv x$ for A a finite type or N;

$F(\Sigma(A,B)) \equiv \Sigma(F(A),F(B))$;

$f_{\Sigma(A,B)}(z) \equiv (f_A(p(z)),f_B(p(z),q(z)))$;

$F(\Pi(A,B)) \equiv \Pi(F(A),F(B))$;

$f_{\Pi(A,B)}(z) \equiv \lambda((x)f_B(f_A^{-1}(x),Ap(z,f_A^{-1}(x))))$;

$F(A+B) \equiv F(A) + F(B)$;

$f_{A+B}(z) \equiv D(z,(x)i(f_A(x)),(y)j(f_B(y)))$;

$F(I(A,a,b)) \equiv I(F(A),f_A(a),f_A(b))$;

$f_{I(A,a,b)}(z) \equiv r$;

$F(V_i) \equiv V_i'$, $f_{V_i} \equiv$ the isomorphism of 2.4.a), $i \in \{1,\dots,n\}$.

It remains to check the rules of inference.

In the case of general rules of equality and substitution, the induction-step follows immediately.

In the case of rules specifying type-forming operations, the subcase of Σ-rules will show all the essential points; the rest is then a straightforward, though tedious, adaptation of that proof to remaining subcases.

Σ-formation. If α is formed by inferring $\Sigma(A,B)$ type from subderivations of A type and of $B(x)$ type $(x \in A)$, by induction-hypothesis we already know what $F(A)$, f_A, $F(B)$, f_B are, as well as their properties listed in Stat. If $T^+ \vdash A = A'$ and $T^+ \vdash B(x) = B'(x)$ $(x \in A)$ for some A', B' established in α, we know that $T \vdash F(A) = F(A')$ and $T \vdash F(B)(x) = F(B')(x)$ $(x \in F(A))$. Then Σ-formation infers $T \vdash F(\Sigma(A,B))$ type, and $T \vdash F(\Sigma(A,B)) = F(\Sigma(A',B'))$. As a judgement of form $\Sigma(A,B) = C$ can be derived in T^+ by Σ-formation or by a general rule only, F is functional on objects. If f_A, f_B are structure-preserving isomorphisms, so is $f_{\Sigma(A,B)}$ by identity-rules, which completes verification of a). As C_α contains no new morphisms except for identity of $\Sigma(A,B)$, b) holds; c) then holds by identity-rules.

Σ-introduction. If α is formed by inferring $(a,b) \in \Sigma(A,B)$ from subderivations of $a \in A$ and $b \in B(a)$, it must contain a subderivation of $\Sigma(A,B)$ type and, since the last judgement can only be inferred by Σ-formation, subderivations of A type and $B(x)$ type $(x \in A)$. We thus already know what $F(A)$, f_A, $F(B)$, f_B, $f(\Sigma(A,B))$, $f_{\Sigma(A,B)}$ are, as well as their properties listed in Stat; in particular we know that for some a',b'

$$T \vdash a' \in F(A), \qquad T^+ \vdash f_A(a) = a' \in F(A),$$

$$T \vdash b' \in F(B)(a'), \qquad T^+ \vdash f_B(a,b) = b' \in F(B)(a').$$

By the same rule we can then infer

$$T \vdash (a',b') \in \Sigma(F(A),F(B)),$$

and by identity-rules

$$T^+ \vdash f_{\Sigma(A,B)}((a,b)) = (a',b') \in \Sigma(F(A),F(B));$$

since we can treat the corresponding judgements of equality in exactly the same way, the functor F can be extended to new morphisms of C_α so as to satisfy a), b) and c).

Σ-elimination. If α is formed by inferring $E(c,d) \in C(c)$ from subderivations of $c \in \Sigma(A,B)$ and $d(x,y) \in C((x,y))$ $(x \in A,\ y \in B(x))$, it must contain a subderivation of $C(z)$ type $(z \in \Sigma(A,B))$. We then already know what $F(A)$, f_A, $F(B)$, f_B, $F(\Sigma(A,B))$, $f_{\Sigma(A,B)}$, $F(C)$, f_C are, as well as their properties listed in Stat; in particular we know that for some c',d'

$$T \vdash c' \in \Sigma(F(A),F(B)), \qquad T^+ \vdash f_{\Sigma(A,B)}(c) = c' \in \Sigma(F(A),F(B)),$$

$$T \vdash d'(x,y) \in F(C)((x,y)) \ (x \in F(A),\ y \in F(B)(x)),$$

$$T^{+} \vdash f_C((f_A^{-1}(x), f_B^{-1}(x,y)), d(f_A^{-1}(x), f_B^{-1}(x,y)) = d'(x,y) \in F(C)((x,y))$$

$$(x \in F(A),\ y \in F(B)(x)).$$

By the same rule we can infer

$$T \vdash E(c',d') \in F(C)(c'),$$

and we have to verify that

$$T^{+} \vdash f_C(c, E(c,d)) = E(c',d') \in F(C)(c').$$

The function $h(z) \equiv f_C(f^{-1}_{\Sigma(A,B)}(z), E(f^{-1}_{(A,B)}(z), d))$ has the properties

$$T^{+} \vdash h(z) \in F(C)(z) \quad (z \in \Sigma(F(A), F(B))$$

$$T^{+} \vdash h((x,y)) = d'((x,y)) \in F(C)((x,y)) \quad (x \in F(A), y \in F(B)(x)).$$

A statement analogous to 1.9. holds for disjoint unions as well, i.e. by Σ-elimination, Σ-conversion and identity-rules we can derive that $(z)E(z,d')$ is the unique function over $\Sigma(F(A),F(B))$ with these properties, thus

$$T^{+} \vdash h(z) = E(z,d') \in F(C)(z) \quad (z \in \Sigma(F(A), F(B)),$$ but

$$T^{+} \vdash h(c') = f_C(c, E(c,d)) \in F(C)(c).$$

Since we can treat the corresponding equality-judgements in exactly the same way, the functor F can be extended to new morphisms of C_{α} so as to satisfy a), b) and c).

<u>Σ-conversion</u> is now immediate by combining the above constructions, since

$$T^{+} \vdash f_{\Sigma(A,B)}((a,b)) = (a',b') \in \Sigma(F(A), F(B))$$ and

$$T \vdash E((a',b'), d') = d'(a',b') \in F(C)((a',b')).$$

By previous remarks, this concludes the proof of Stat(α) and of the theorem.

<u>2.6.2.</u> Since we have not really used the theory of categories here, category-theoretic language was not necessary; as used above, it may be taken for a system of convenient abbreviations.

3. ARITHMETICAL DEFINITIONS OF INDUCTIVELY DEFINED PREDICATES

3.1. Predicates specified by rules of form 1.1-1.4. can be represented by their "graphs", i.e. by sets of pairs (object of A_i, proof of $V_i(t_{ij}(\text{object})))$. For the graphs, however, rules of particularly simple form will suffice:

3.1.1. Formation.

$$W_i \text{ type}$$

provided A_i type, $i \in \{1,\dots,m\}$.

3.1.2. Introduction.

$$\frac{a \in A_i \quad \dots b_k \in W_k \dots}{c_i(a, \dots b_k \dots) \in W_i}\ ,$$

where $i \in \{1,\dots,m\}$ and k ranges over a (multi)set K_i of values from $\{1,\dots,m\}$.

3.1.3. The rules of elimination and conversion stipulate the existence of a functional which solves the recursion-equations

$$\dots f_i(c_i(x, \dots y_k \dots)) = d_i(x, \dots y_k, f_k(y_k) \dots)$$
$$\in C_i(c_i(x, \dots y_k \dots))\ (x \in A_i, \dots y_k \in W_k \dots) \dots$$

uniformly in $\dots d_i \dots$, provided $\dots C_i(x)$ type $(x \in W_i)\dots$ and the minor premisses

$$\dots d_i(x, \dots y_k, z_k \dots) \in C_i(c_i(x, \dots y_k, z_k \dots))$$
$$(x \in A_i, \dots y_k \in W_k, z_k \in C_k(y_k) \dots) \dots$$

3.1.4. The stipulation of 3.1.3. establishes $\dots W_i \dots$ as a minimal solution of domain-equations

$$W_i \simeq A_i \times \dots \times W_k \times \dots, \quad i \in \{1,\dots,m\},$$

i.e. as a system of sets of nested sequences or lists of elements of A_i's, in an arrangement recursively prescribed by the choice of $\dots K_i \dots$ (with a natural ordering on K_i's that we shall assume fixed in the sequel). A type--constructor to that effect may (but will not) be introduced, parameterized by the choice of m and $\dots K_i \dots$.

We are going to prove that rules 1.1-1.4. are validated in T if rules 3.1.1-3.1.3. are, and show how the latter can be validated in SA and in ML_o for any $\dots A_i \dots$.

3.2. Let $n, \ldots m_i \ldots, \ldots R_{ij} \ldots, \ldots S_{ijr} \ldots$ be as in 1.1-1.4. Define

$$m \equiv \sum_{i=1}^{n} m_i ;$$

$k(i,j)$ - a bijective pairing function such that $k(i,j) \in \{1,\ldots,m\}$ for $i \in \{1,\ldots,n\}$, $j \in \{1,\ldots,m_i\}$;

$$K_i \equiv \bigcup_j \bigcup_{r \in R_{ij}} S_{ijr} ;$$

$$A'_{k(i,j)} \equiv A_i .$$

Let $\ldots W_i \ldots$ be a system of types specified by 3.1.1-3.1.3. with A'_i for A_i, m and $\ldots K_i \ldots$ as above. Let

$$lab(v) \equiv rec(v, \ldots(x, \ldots y_k, z_k \ldots)x \ldots),$$

$$V'_i(y) \equiv \ldots+(\exists v \in W_{k(i,j)})(y = t_{ij}(lab(v))+\ldots,$$

$$val_i \equiv \ldots+(z)p(z)+\ldots,$$

$$c'_{ij}(x, \ldots y_{st}, z_{st} \ldots) \equiv i_j((c_{k(i,j)}(x, \ldots val_s(z_{st}) \ldots),r))$$

where rec is the functional of 3.1.3., sum of functions over the summands denotes the eliminatory function of m_i-1 times iterated binary sum, whose inclusions are denoted by $\ldots i_j \ldots$. By +-rules, $\ldots+(z)i_j((p(z),r))+\ldots$ will be the identity-function of $V'_i(y)$, and $\ldots c'_{ij} \ldots$ will validate the introduction-rules 1.2. for $\ldots V'_i \ldots$. Given the recursion-equations of 1.9., we may define

$$D_{k(i,j)}(y) \equiv C_i(t_{ij}(lab(y)), i_j((y,r))$$

$$e_{k(i,j)}(x, \ldots y_{k(s,t)}, w_{k(s,t)} \ldots)$$
$$\equiv d_{ij}(x, \ldots lab(y_{k(s,t)}), i_t((y_{k(s,t)},r)), w_{k(s,t)} \ldots),$$
$$i \in \{1,\ldots,n\},\ j \in \{1,\ldots, m_i\}.$$

If $\ldots d_{ij} \ldots$ validate the minor premisses of 1.3. for $\ldots C_i \ldots$, it is straightforward to verify that $\ldots e_{k(i,j)} \ldots$ validate the minor premisses of 3.1.3. for $\ldots D_{k(i,j)} \ldots$. Let $\ldots g_{k(i,j)} \ldots$ be the solutions of recursion-equations 3.1.3. for $\ldots e_{k(i,j)}, D_{k(i,j)} \ldots$, which may be obtained uniformly by an application of rec; let

$$f_i = \ldots+(z)g_{k(i,j)}(val_i(z))+\ldots, \qquad i \in \{1,\ldots,n\};$$

we may then derive the judgements

$$f_i(z) = g_{k(i,j)}(val_i(z)) \in D_{k(i,j)}(val_i(z)) \ (x \in A_i, z \in V'_i(t_{ij}(x)).$$

Using this equality, it is straightforward to verify that $\ldots f_i \ldots$ solve the equations 1.9. The recursor for $\ldots V_i' \ldots$ may then be obtained by encoding the above uniform construction from $\ldots d_{ij} \ldots$.

3.3. If restricted to SA, Beeson's (1982) model-construction would go through with primitive recursive functions instead of indices. Formalizing the construction in SA instead of HA, we might use functional expressions instead of pseudoterms, obtaining the following fact for $T = SA$:

3.3.1. For any context $\underline{A} \equiv x_1 \in A_1, \ldots, x_n \in A_n(x_1, \ldots, x_{n-1})$ established in T, functions $\mathrm{num}A_i(x_1, \ldots, x_i)$, $\mathrm{is}A_i\mathrm{num}(y_1, \ldots, y_i)$, $i \in \{1, \ldots, n\}$, may be defined so that

a) the judgements

$$\ldots \mathrm{num}A_i(x_1, \ldots, x_i) \in N \; (x_1 \in A_1, \ldots, x_i \in A_i(x_1, \ldots, x_{i-1})) \ldots$$

are all derivable in T;

b) the judgements

$$\ldots \mathrm{is}A_i\mathrm{num}(y_1, \ldots, y_i) \in N \; (y_1 \in N, \ldots, y_i \in N) \ldots$$

are all derivable in SA;

c) the functions $\ldots (x_1, \ldots, x_i)(\mathrm{num}A_i(x_1, \ldots, x_i), r)) \ldots$ form a structure-preserving isomorphism of $\underline{A}$ and

$$N\underline{A} \equiv z_1 \in NA_1, \ldots, z_n \in NA_n(z_1, \ldots, z_{n-1})$$

in C_T, where $NA_i(z_1, \ldots, z_{i-1}) = \Sigma(N, (z)(\mathrm{is}A_i\mathrm{num}(z_1, \ldots, z_{i-1}, z) = 0))$;

d) N as defined in c) is a contextual functor from C_T to C_{SA}.

3.3.2. The functions $\ldots \mathrm{num}A_i \ldots$ are Gödel-numberings, and $\ldots NA_i \ldots$ may be seen as sets of appropriate Gödel-numbers defined by their characteristic functions $\ldots \mathrm{is}A_i\mathrm{num} \ldots$.

3.3.3. If T is SA extended by (some) rules of form 3.1., the statement 3.3.1. is readily extended to T, using primitive recursive surjective coding of finite sequences of numbers $\langle \ldots \rangle$ strictly increasing in all variables (cf. Troelstra (1973)). Let lth be the length-function, and $(x)_i$ the i-th projection for $i \leq \mathrm{lth}(x)$; let $\mathrm{eq}(x,y)$ be the arithmetical characteristic function of equality on N. By 3.1.3. we may define $\ldots \mathrm{num}W_i \ldots$ so as to satisfy the equations

$$\cdots$$

$$\mathrm{num}W_i(c_i(x, \ldots y_k \ldots)) = \langle i, \mathrm{num}A_i(x), \langle \ldots \mathrm{num}W_k(y_k) \ldots \rangle\rangle \in N \quad (x \in A_i, \ldots y_k \in W_k \ldots).$$

If n_i is the size of K_i, functions ...$isW_i num$... should satisfy the equations

. . .

$$isW_i num(z) = eq(lth(z),3) \cdot eq(lth((z)_3),n_i) \cdot eq((z)_1,i) \cdot$$
$$\cdot isA_i num((z)_2) \cdot \ldots \cdot isW_k num(((z)_3)_k) \cdot \ldots \in N \ (z \in N).$$

Since $z > (z)_j$ for any $j \leq lth(z)$, these equations are readily solved by formalizing the appropriate functional of simultaneous course-of-values recursion (cf. Péter (1967)) in SA. The introductory constants may then be defined by

$$\ldots c_i'(x, \ldots y_k \ldots) \equiv \langle i, p(x), \langle \ldots p(y_k) \ldots \rangle\rangle \ \ldots ,$$

and the recursor may be defined by simultaneous course-of-values recursion. The types ...NW_i..., defined as in 3.3.1., validate the rules 3.1. with ...NA_i... for ...A_i... and with the constants defined as above, so the rest of 3.3.1. follows by (proof of) 2.6.

3.4. Our notion of definability implies type-theoretic isomorphism of the definiendum and its definiens, so Gödel-numberings will not suffice when function-types are involved (because of well known metamathematical reasons).

A list of complicated objects of different sorts, and that is what objects of W_i's specified by 3.1. in general are, may be represented as a pair of two objects: a list of same shape containing only place-holders, which indicate the place and the sort of object to be put in its place, and a system of function-tables, one for each sort, associating complicated objects to place-holders. Lists of same shape containing only simple place-holders may be readily defined in ML_o by 3.3. Function-tables are simple to construct as soon as we

a) know how to count the number of place-holders of the same sort;

b) specify a strategy for traversing the list, i.e. associate table-locations to list-locations in an unambiguous way (it may be already encoded by a suitable choice of place-holders), uniformly for all lists and tables of that kind.

Integers may serve as place-holders; given a) and b), $\Sigma(N,(n)(n < size_i(z))) \rightarrow A_i$ may represent the i-th function-table, where $size_i(z)$ is the number of atoms of i-th sort in the list z. The introductory constants may then be defined by encoding the appropriate operations of updating both the list and the function-tables; the recursor will recur over the list and will use the tables to fetch atomic values when they are needed.

The preceding sentences are essentially to be understood only as what they sound like: as hints for an exercise in programming, which we leave for the reader to complete.

3.5. The relation of the definiendum to its definiens is what is in computing science understood as the relation of an "abstract data-type" to its "implementation". Thus interpreted, the "implementation" of 3.3. turns out to be terribly inefficient. If we, however, admit the type of symbolic expressions of 1.6.1. above a suitable type Atom as primitive, an "efficient" implementation may be effected, paralelling that of 3.3. very closely, although function-types will be needed to implement simultaneous course-of--values recursion. Definability of types specified by rules 3.1. in ML_o would nevertheless be preserved, meaning now "efficient implementability" as well.

Corrigendum. The conclusion of the third rule of conversion in 1.6.2.4. should stand under minor premisses.

REFERENCES

1. J. Allen, Anatomy of LISP, McGraw-Hill, New York 1978.
2. M. Beeson, Formalizing Constructive Mathematics: Why and How?, in: F.Richman, ed., Constructive Mathematics, LNM 873, Springer, Berlin 1981, 146-190.
3. M. Beeson, Recursive Models for Constructive Set Theories, Annals of Mathematical Logic 23(1982), 127-178.
4. J. Cartmell, Generalized Algebraic Theories and Contextual Categories, Thesis, Oxford University 1978.
5. H.R. Jervell, Constructive Universes I, in: Higher set theory (Proc. Conf. Math. Forschungsinst. Oberwolfach, 1977), LNM 669, Springer, Berlin 1978, 73-98.
6. P. Martin-Löf, Constructive mathematics and computer programming, Preprint No 11, University of Stockholm 1978.
7. P. Martin-Löf, Intuitionistic Type Theory, Notes by G.Sambin of a series of lectures given in Padova, June 1980, Stockholm 1984.
8. R. Péter, Recursive functions, Akadémiai Kiadó, Budapest 1967.
9. A.S. Troelstra, Metamathematical Investigation of Intuitionistic Arithmetic and Analysis, LNM 344, Springer, Berlin 1973.

Mr Dean Rosenzweig
Fakultet strojarstva i brodogradnje
Sveučilišta u Zagrebu
41ooo Zagreb, Đure Salaja 5

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", ZAGREB 1984

CONTRAINTUITIONIST LOGIC AND SYMMETRIC SKOLEM ALGEBRAS

Kajetan Šeper

Abstract. Intuitionist logic, formulated e.g. by natural deduction, if algebraically reformulated, leads to Heyting algebras (i.e. absolute implicative lattices with zero element), and these, if algebraically dualized, lead to Brouwer algebras (i.e. absolute subtractive lattices with the unit element). For both kinds of these absolute Skolem algebras, implicative and subtractive, their topological interpretation is well-known, and their unification resulting in absolute implicative-subtractive Skolem algebras was studied by Rauszer under the name of semi-Boolean algebras.

We established a contraintuitionist system of logic, which is logically dual to the intuitionist one, where the dual ⊥-connectives replace the ordinary ones. Thus we obtained a logical interpretation of Brouwer algebras. We wish to contrast it to Goodman's interpretation. Also, as a result of another kind of unification of the both asymmetric intuitionist systems, we established a symmetric intuitionist system, which, if algebraically reformulated, leads to absolute symmetric Skolem algebras. We wish to contrast them to Rauszer's algebras.

Contents.

0. Strong truth and strong falsity. Symmetric logic

Under the classical viewpoint any statement is considered a priori as being true or false but not both. Under the constructive attitude the truth and the falsity of a statement are of a posteriori character, each one is to be established by constructive reasoning - the truth by a proof and the falsity by a ⊥-proof or refutation -, otherwise the statement is to be considered as problematic. Such truth and falsity are called strong. So, constructive logic may be divided into the following kinds: ⊤(truth)-oriented, if its main concern is the study of strong truth; $\bot$(falsity)-oriented, if this holds for strong falsity instead; and $\top$-$\bot$- or S-oriented, or simply symmetric, if both these species, that of strong truth and that of strong falsity, are studied together with no priority of each to the other.

The most natural way to get a symmetric system of logic, e.g. from a $\top$-oriented one, is to unify the both asymmetric systems, the $\top$-oriented system and the corresponding $\bot$-oriented one, into a new complex system. The both disconnected parts may be well mutually connected by several laws. Now, the unification may proceed directly or by means of a new connective, called strong negation, which is to express strong falsity. Then, another new connective, called strong (or two-sided) implication, or simply biplication, may be considered in addition, or, moreover, may replace implication. Consequently, symmetric constructive logic may be divided into the following kinds: semi-symmetric, if the unification is realized directly; pre-symmetric, if the unification is realized solely by means of strong negation; and (strongly) symmetric, if, in addition, biplication replaces implication.

1. Intuitionist logic, JL

Historically, the first constructive logic was developed and applied by Brouwer in his intuitionist mathematics or intuitionism. This intuitionist logic, JL, was formalized by Heyting in the form of a Hilbert-style axiomatic system. JL is $\top$-oriented. However, it contains also a specific notion of falsity, called absurdity in intuitionist jargon. The falsity (or absurdity) of a statement is established by deducing a contradiction (or absurd), $\bot$, from that statement as assumption. This kind of falsity may be called not-truth or weak falsity, and is, as usually, reffered to by negation, $\neg$. It is expressible by implication, $\supset$, and $\bot$: $\neg A \equiv A \supset \bot$. Thus one may say JL is weakly $\bot$-oriented. Then, for any statement A, $A \supset \neg\neg A$ holds, but not conversely. Therefore $\neg\neg A$, if asserted, may be understood as a new kind of truth of A, weaker than the assertion of A. This kind of truth may be called not-weak-falsity of quasi-truth. Thus one may say JL is quasi-$\top$-oriented. So, intuitionistically, one may distinguish four kinds of statements: strongly true, weakly false, quasi-true, and problematic. (A quasi-true statement may count, if one wishes, as problematic in the narrower sense.)

Gentzen formalized JL in the form of a natural deduction system. The notion of proof in tree form is defined by the following natural rules:

$\wedge$ $\qquad \wedge I \ \dfrac{A \quad B}{A \wedge B} \qquad\qquad \wedge E \ \dfrac{A_1 \wedge A_2}{A_i}$

$\vee$ $\quad \vee I \dfrac{A_i}{A_1 \vee A_2} \qquad \vee E_m \dfrac{A \vee B}{A \quad B}$

$\bot$ $\quad \text{efq} \dfrac{\bot}{B}$

$\supset$ $\quad \supset I \dfrac{\begin{matrix}[A]\\ B\end{matrix}}{A \supset B} \qquad \supset E \dfrac{A \quad A \supset B}{B}$

Here $i=1$ or 2, and the "multiple" $\vee E_m$ rule is considered to abbreviate the ordinary "singular" $\vee E$ one i.e.

$$\vee E_m \text{ abbreviates } \vee E \frac{A \vee B \quad \begin{matrix}[A]\\ C\end{matrix} \quad \begin{matrix}[B]\\ C\end{matrix}}{C}$$

(For a properly multiple formulation cf. 5 or 7 .) As mentioned above,

$\neg$ $\qquad \neg A$ will abbreviate $A \supset \bot$.

The I(introduction) rules state conditions under which a compound statement may be infered from its components, and the E(elimination) rules state conditions under which a statement may be infered from a compound one. The ex falso quodlibet rule, efq, adds to the precision of intuitionist implication and enables the $\supset$ rules to be so simple as above; especially, it enables the $\supset$ E rule to be in the form of the modus ponens, mp. The rules fix very clearly the meaning of each connective and so replace their textual explanation.

Then, one easily defines the notion of deducibility of the conclusion B from the assumptions A_i i.e. the (n+1)-ary deducibility relation $A_1, \ldots, A_n \vdash B$, for each natural n. Obviously, $A \vdash A$ i.e. $\vdash A \supset A$ holds, for any A. So, if $\top$ abbreviates $A_o \supset A_o$, for a fixed A_o, then $\vdash \top$ holds, and hence $C \vdash \top$ does, for any C, too.

From the natural deduction formulation of JL one easily obtains its Gentzen sequent calculus reformulation: a sequent $A_1, \ldots, A_n \rightarrow B_1, \ldots, B_m$ is interpreted as standing for the implication $A_1 \wedge \ldots \wedge A_n \supset B_1 \vee \ldots \vee B_m$ i.e. for a deduction of $B_1 \vee \ldots \vee B_m$ from A_i. (For various sequent formulations cf. 5 or 7 .)

2. Heyting algebras, HA

If algebraically formulated, the system of JL leads to Heyting algebras (or pseudo-Boolean algebras according to Rasiowa and Sikorski 1963, or absolute implicative lattices with the zero element according to Curry 1963), HA. The simplest way to formulate JL algebraically and so to obtain a system for HA is to get it from the natural deduction system by means of the 2-ary deducibility relation, $A \vdash B$, which is to be considered as the sole basic relation in HA. Then, this basic relation, denoted $a \leq b$, is a partial order. Concerning the 2-ary operations $\wedge$, $\vee$, and $\supset$, and the 0-ary operation or zero element 0 (which replaces $\perp$) the relation satisfies the following axioms and rules:

$\wedge$	$c \leq a \ \& \ c \leq b \Rightarrow c \leq a \wedge b$	$a_1 \wedge a_2 \leq a_i$
$\vee$	$a_i \leq a_1 \vee a_2$	$a \leq c \ \& \ b \leq c \Rightarrow a \vee b \leq c$
0		$0 \leq b$
$\supset$	$a \wedge c \leq b \Rightarrow c \leq a \supset b$	$a \wedge (a \supset b) \leq b$

Here the small letters are used to emphasize the algebraic character of the system. The 1-ary operation $\neg a$ may be defined by $a \supset 0$, and the 0-ary operation or unit element 1 (which replaces $\top$, and satisfies $c \leq 1$) by $a_o \supset a_o$, for a fixed a_o.

Both systems for JL, that of natural deduction and that of partial order relation, are equivalent:

$$A_1, \ldots, A_n \vdash B \quad \text{iff} \quad A_1 \wedge \ldots \wedge A_n \leq B$$
$$\text{iff} \quad 1 \leq A_1 \wedge \ldots \wedge A_n \supset B.$$

3. Contraintuitionist logic, $\perp$JL

Brouwer's intuitionism greatly influenced further investigations into the mathematical and logical reasoning by constructive methods. Regardless of the critique of and arguments against the intuitionist (weak) falsity and the intuitionist implication as well, and of the further development in this direction, several authors studied the constructive (strong) falsity on a par with constructive (strong) truth.

So, by means of a suitable modification of the Kleene realizability notion, Nelson 1949, 1959 studied constructive falsity closely in parallel to constructive truth, and established some symmetric constructive systems of logic with strong connectives. Fitch 1952, 1963 also studied similar systems. Independently, Markov 1950, 1970 did so by means of intuitive logical explanations; especially, he introduced the notions of strong negation and strong equivalence. This influenced further detailed investigations into the subject by logical and algebraic methods. We mention but the following: Vorob'jev's 1952, 1964 papers on a pre-symmetric system, the "constructive propositional calculus with strong negation", and Zaslavskiĭ's 1978 monograph on a (strongly) symmetric system, the "symmetric constructive logic". If algebraically reformulated, the systems are studied under the name of "Nelson algebras".

However, the semi-symmetric systems of logic were completely ignored.

It seems that the main reason for that resides in the absence of a logical interpretation of "Brouwer algebras" i.e. of a logic proper that would correspond to them as JL does to HA. (Cf. discussion in sec.5.) Another reason seems to be the presence of "semi-Boolean algebras" and the corresponding "Heyting-Brouwer logic". (Cf. also discussion in sec.8.)

As a symmetric counterpart corresponding to the ordinary JL, we established in 4 a contraintuitionist logic, ⊥JL, where the new logically dual ⊥-connectives replace the ordinary ones. For formulae in ⊥JL that symmetry suggests right-to-left reading. Especially, the ⊥-contradiction (or ⊥-absurd), ⊤ , the ⊥-implication or explication, $\not\subset$, read as "is explied by" if the ordinary left-to-right reading is applied, and the ⊥-negation or affirmation, $\llcorner$, read as "not false", replace the ordinary contradiction (absurd), implication, and negation, respectively. The affirmation $A\llcorner$, denoted also $\llcorner A$ or $\lrcorner A$ if the ordinary left-to-right reading is applied, is expressible by $\not\subset$ and ⊤ : $A\llcorner \equiv \top \not\subset A$. Contraintuitionistically, we may distinguish four kinds of statements: strongly false, not-false or weakly true, not-weakly-true or quasi-false, and ⊥-problematic. (Quasi-falsity may count as ⊥-problematic in the narrower sense.) Also, we may say ⊥JL is ⊥-oriented, weakly ⊤-oriented, and quasi-⊥-oriented.

To get the natural deduction formulation for ⊥JL the ⊥-proof or refutation trees will be, for reasons of symmetry, treated as directed upwards, and so as generated by the following natural, upwards applicable, ↑-rules:

$$\wedge E_m \equiv \wedge I \text{ in JL} \qquad \wedge I \equiv \wedge E \text{ in JL} \qquad \wedge$$

$$\vee E \equiv \vee I \text{ in JL} \qquad \vee I \equiv \vee E_m \text{ in JL} \qquad \vee$$

$$\frac{B}{\top}\ \text{evq (ex vero quodlibet)} \qquad \top$$

$$\frac{B}{B \not\subset A \quad A} \not\subset E \text{ (or ⊥-mp)} \qquad \frac{B \not\subset A}{\underset{[A]}{B}} \not\subset I \qquad \not\subset$$

where

$$\wedge E_m \text{ abbreviates } \frac{C}{\underset{[B]}{C} \quad \underset{[A]}{C} \quad B \wedge A} \wedge E$$

(For a properly multiple formulation cf. 5 or 7 .) As mentioned above

$A\llcorner$ will abbreviate $\top \not\subset A$. $\llcorner$

Then, the notion of ⊥-deducibility, $B \dashv A_n, \ldots, A_1$, of the ⊥-conclusion B from the ⊥-assumptions A_i is defined analogously. If ⊥ abbreviates $A_o \not\subset A_o$, for a fixed A_o, then ⊥⊣ holds, and hence ⊥⊣ C does, for any C, too.

The $\bot$-sequent formulation of $\bot$JL is obtained from the natural deduction one by interpreting a $\bot$-sequent $B_m,\ldots,B_1 \leftarrow A_n,\ldots,A_1$ as standing for the explication $B_m \wedge\ldots\wedge B_1 \nsubset A_n \vee\ldots\vee A_1$ i.e. for a $\bot$-deduction of $B_m \wedge\ldots\wedge B_1$ from A_i. (For various sequent formulations cf. 5 or 7 .)

4. Brouwer algebras, BA

If algebraically formulated, the system of $\bot$JL leads to Brouwer algebras (i.e. absolute subtractive lattices with the unit element), BA, where the operation of explication (i.e. subtraction or pseudo-difference) replaces that of implication.

Now, to reformulate the natural deduction system for $\bot$JL algebraically so as to obtain a system for BA we proceed similarly as above for HA, i.e. replace $B \dashv A$ by $b \geqslant a$, and cosider $\geqslant$ as the sole basic relation in BA. Then again $\geqslant$ is a partial order relation that satisfies the following axioms and rules:

$$c \geqslant b \wedge a \Leftarrow c \geqslant b \;\&\; c \geqslant a \qquad a_2 \wedge a_1 \geqslant a_i \qquad\qquad \wedge$$

$$a_i \geqslant a_2 \vee a_1 \qquad b \vee a \geqslant c \Leftarrow b \geqslant c \;\&\; a \geqslant c \qquad\qquad \vee$$

$$b \geqslant 1 \qquad\qquad 1$$

$$b \geqslant (b \nsubset a) \vee a \qquad b \nsubset a \geqslant c \Leftarrow b \geqslant c \vee a \qquad\qquad \nsubset$$

The affirmation $a\llcorner$, denoted also $\llcorner a$ or $\lrcorner a$, may be defined by $1 \nsubset a$, and the zero element 0 (which replaces $\bot$, and satisfies $0 \geqslant c$) by $a_o \nsubset a_o$, for a fixed a_o.

The both systems for JL are equivalent:

$$B \dashv A_n,\ldots,A_1 \quad \text{iff} \quad B \geqslant A_n \vee\ldots\vee A_1$$

$$\text{iff} \quad B \nsubset A_n \vee\ldots\vee A_1 \geqslant 0.$$

5. Discussion I

The systems JL (logic) and HA (algebra) correspond each to other, and the systems HA and BA are algebraically dual each to other. Now, two questions arise. Which system is logically dual to JL? Which system (logic) corresponds to BA (algebra) as JL does to HA? By $\bot$JL we obtained the logical dual to JL and (unintended) the logical interpretation of BA as well. The topological interpretation of each absolute Skolem algebras, HA and BA, by open and, respectively, closed sets of a topological space, or more abstractly, of a topological Boolean algebra, was well-known from the papers of Stone 1937 and of McKinsey and Tarski 1946.

With respect to $\bot$JL (and BA) a comparison with Goodman's 1981 paper

1 was suggested to the author. We wish to discuss this matter now. Goodman tried to interprete BA logically, and so to establish the "logic of contradiction" or "anti-intuitionistic logic". However, this logic actually lacks a proper logical interpretation. What is effected is but an equivalent sequentcalculus reformulation of BA. First, the connective "pseudo-difference", $\dot{-}$, that corresponds to the equally named algebraic operation, suggested to be read as "but not", is in general not logically interpreted at all, only its special instance, "negation", $\neg A \equiv \top \dot{-} A$, suggested to be read as "not", is introduced. Second, the suggested readings "and" and "or" for the other connectives "conjunction", $\wedge$, and "disjunction", $\vee$, respectively, seem to indicate their usual $\top$-interpretation. Thus, by their suggested readings, the connectives seem to be $\top$-connectives. So, on these "grounds" $A \wedge \neg A$ appears as a contradiction, but is in fact a $\bot$-tnd (tertium non datur) $A \wedge \llcorner A$, and $A \vee \neg A$ appears as a tnd, but is in fact a $\bot$-contradiction $A \vee \llcorner A$. Such readings seem to us logically unsatifactory. Formally, if suitably modelled by sequents, the system $\bot$JL may lead exactly to Goodman's sequentcalculus, indeed. (However, for the same purpose we would prefer $\bot$-sequents.)

6. Symmetric intuitionist logic, SJL

When $\bot$JL was established, the idea of a direct unification of both asymmetric logical systems, JL and $\bot$JL, so as to form a new symmetric intuitionist logic, SJL, appeared clearly. For the preference of such unification by means of the strong negation, the system SJL was but mentioned in 4 . It was discussed to some extent in 6 .

We will give here only a simple fragment of SJL containing neither $\supset$ as a $\bot$-connective nor $\not\subset$ as a $\top$-connective, or containing them but not in full generality. The full system would require more technical details i.e. the notion of S-deducibility involving $\top$- as well $\bot$-assumptions symultanously.

To get the natural deduction formulation for SJL we define: (a) the formulae - these are formed as usually from the atomic formulae by means of the connectives $\wedge$, $\vee$, $\supset$, and $\not\subset$; the other connectives $\top$, $\bot$, $\neg A$, and $\llcorner A$ are considered as abbreviations for $A_0 \supset A_0$, $A_0 \not\subset A_0$, for a fixed A_0, $A \supset \bot$, and $\top \not\subset A$, respectively, as indicated above for JL and $\bot$JL; (b) the rules - these are all JL$\downarrow$-rules and $\bot$JL$\uparrow$-rules; the other rules are given in (c); (c) the deducibility relations - these are all $\top$-deducibility relations generated by the $\downarrow$-rules alone, i.e. by proofs in $\downarrow$-tree form, and all $\bot$-deducibility relations generated by the $\uparrow$-rules alone, i.e. by refutations in

$\uparrow$-tree form, both kinds extended by the additional simple SL-rules as follows:

$\llcorner$ $\quad \vdash A \Rightarrow \dashv A$ (i.e. $\llcorner A \dashv$),

$\neg$ $\quad A \dashv \Rightarrow A \vdash$ (i.e. $\vdash \neg A$).

The simple $\bot\supset$ and $\top\not\subset$ rules may well be added:

$\bot\supset$ $\quad \vdash A \,\&\, B \dashv B_n, \ldots, B_1 \Leftrightarrow A \supset B \dashv B_n, \ldots, B_1$,

$\top\not\subset$ $\quad A_1, \ldots, A_n \vdash A \,\&\, B \dashv \Leftrightarrow A_1, \ldots, A_n \vdash A \not\subset B$.

The natural deduction formulation is easily reformulated to obtain the corresponding S-sequent formulation.

7. Symmetric Skolem algebras, SA

If algebraically formulated, the system of SJL leads to a new algebraic system which we call simple absolute symmetric Skolem algebras, SA. (Previously, in 6 , we called it "half-Boolean algebras", the prefix "half" being the English translation of the Croatian "polu" to contrast it to Rauszer's Greek "semi".)

Now, to formulate SJL algebraically to obtain SA, we proceed as above for HA and BA. Thus we obtain a system with two basic 2-ary relations $\leq$ and $\geqslant$ and four 2-ary operations $\wedge, \vee, \supset$, and $\not\subset$ such that $\leq, \wedge, \vee, \supset$ satisfy all the axioms and rules of HA, $\geqslant, \wedge, \vee, \not\subset$ satisfy all those of BA, and $\leq$, $\geqslant$ satisfy the following simple SA-rules in addition:

$\llcorner$ $\quad 1 \leq a \Rightarrow 1 \geqslant a$ (i.e. $\llcorner a \geqslant 0$),

$\neg$ $\quad a \geqslant 0 \Rightarrow a \leq 0$ (i.e. $1 \leq \neg a$),

$\bot\supset$ $\quad 1 \leq a \,\&\, b \geqslant b_1 \Leftrightarrow a \supset b \geqslant b_1$,

$\top\not\subset$ $\quad a_1 \leq a \,\&\, b \geqslant 0 \Leftrightarrow a_1 \leq a \not\subset b$,

where the operations $1, \neg a$ and $0, \llcorner a$ are defined as in HA and BA, respectively.

Both systems for SJL are obviously equivalent as above.

The algebraic formulations for JL, $\bot$JL, and SJL make it possible to define the corresponding abstract (set-theoretic) algebraic systems immediately.

8. Discussion II

With respect to SJL (and SA) it was suggested to the author to compare it with Rauszer's 1974, 1980 papers 2 and 3 . A few remarks will suffice here. Rauszer developed the theory of "semi-Boolean algebras" (i.e.

absolute implicative-subtractive Skolem algebras or lattices, in fact complete lattices) by algebraic and model-theoretic methods. Also, she established and studied the corresponding "Heyting-Brouwer logic" by means of two Hilbert-style axiomatic systems. However, it is hard to say for any of these systems to be properly a logic at all. The reasons are the same as those in sec.5.

REFERENCES

1. N.D. Goodman, The logic of contradiction, Zeitschr. f. math. Logik und Grundlagen d. Math. 27 (1981), 119-126.

2. C. Rauszer, Semi-Boolean algebras and their application to intuitionistic logic with dual operations, Fundamenta Mathematicae 83 (1974), 219-249.

3. C. Rauszer, An algebraic and Kripke-style approach to a certain extension of intuitionistic logic, Dissertationes Mathematicae 167 (1980), 1-62.

4. K. Šeper, Symmetry in logic, The 7th Congress of Balkan Mathematicians, Athens, December 19-26, 1983.

5. K. Šeper, Sequent modelling of various logical systems, The Seminar of Foundations of Mathematics and Mathematical Logic, Zagreb University, February 14, 1984.

6. K. Šeper, Logic and algebra - Logical interpretation of Brouwer algebra and algebraic interpretation of symmetric intuitionist logic, (abstract, in Croatian), The 4th Conference "Algebra and Logic", Zagreb, June 07-09, 1984.

7. K. Šeper, Symmetry in logic (Towards a systematics of logical genealogy), I Conceptual symmetry, II Presentational symmetry, The 7.1.4. SIZ I 1984. project "Mathematical structures, models and applications", Zagreb University.

Prof. dr Kajetan Šeper
Fakultet strojarstva i brodogradnje
Sveučilišta u Zagrebu
Salajeva 5, 41ooo Zagreb

Institut za strojarstvo - Strojarski fakultet
u Slavonskom Brodu Sveučilišta u Osijeku
Trg maršala Tita 18, 55ooo Slavonski Brod

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", ZAGREB 1984

PEACOCK'S PRINCIPLE AND EULER'S EQUATION

Zvonimir Šikić

Abstract. The exponentiation is never extended from the real to the complex domain in accordance with Peacock's principle of permanence, although it is the best way of extending the other operations. But we show that we are almost compelled to Euler's equation by Peacock's principle of permanence and also the we are definitely compelled to it if we accept the principle of permanence of differentiability.

C.B. Allendoerfer dedicated his [1] to those authors whose papers on Euler's equation had been rejected by American Mathematical Monthly. He emphasized that the expression $e^{i\omega}$ has to be defined, in order to prove Euler's equation, but his criteria for accepting a definition of the expression as a good one (rigor, simplicity and intuition) are quite vague. We can not be satisfied with such a vague criteria because excellent criteria have existed for a long time. Such is G.Peacock's principle of permanence of equivalent forms announced already in 1833.

A definition of on operation should be extended from a restricted domain to a wider one in such a way as to conserve the crucial algebraic properties of the operation.

The crucial algebraic properties of addition multiplication and exponentiation are as follows

$$\# \begin{cases} a+b=b+a & a\cdot b=b\cdot a \\ (a+b)+c=a+(b+c) & (a\cdot b)\cdot c=a\cdot(b\cdot c) \\ a\cdot(b+c)=a\cdot b+a\cdot c & \\ a^{b+c}=a^b\cdot a^c \quad (a^b)^c=a^{b\cdot c} & (a\cdot b)^c=a^c\cdot b^c, \end{cases}$$

and the extensions of these operations (from the domain of natural numbers to the domain of complex numbers) were uniquely determined by the principle, in all cases except one. The one with which Euler's equation is concerned.

Mus it be so? Are we compelled by Peacock's principle to define $e^{i\omega}$ as $\cos\omega + i\sin\omega$ (as we are compelled to define $a^{1/n}$ as $\sqrt[n]{a}$ or a^{-n} as $1/a^n$

etc.)? We shall show, that we almost are.

We obtain complex numbers by adding the imaginary unit i to the reals and by combining the old reals with the new unit i using the operations $+$ and $\cdot$ uniquely extended in accordance with Peacock's principle. We immediately realize that any element of the new complex domain is of the form $x+iy$ for real x and y (because of the defining property of i: $i^2=-1$) and that the totality of all new numbers forms a field. But what about exponentiation in the new complex domain? Is it possible to define exponentiation of complex numbers (determined by reals, i, $+$ and $\cdot$) in accordance with Peacock's principle, so as to remain within the complex domain?[1] We shall show it is.

Notice first that $-i$ has the same defining property as i: $(-i)^2=-1$. So, any calculation with i which ends with the result

$$R(i) = x + iy$$

when performed on $-i$ will end with the result

$$R(-i) = x - iy.$$

But we want to treat exponentiation as a calculation process in the complex domain, so if for real a and ω

$$R(i) = a^{i\omega} = x + iy \qquad \text{then}$$

$$R(-i) = a^{-i\omega} = x - iy.$$

This is also a kind of permanence principle. But then

$$a^{i\omega} \cdot a^{i\omega} = (\text{retaining } \# \text{ by Peacock's principle}^{2)}) = a^{i\omega - i\omega} =$$

$$= a^0 = 1 = (x+iy)\cdot(x-iy) = x^2 + y^2 \qquad \text{i.e.}$$

$$a^{i\omega} = \cos\phi + i\sin\phi .$$

It remains to find out how ϕ depends on a and ω.
$\phi(a,\omega)$ has to be continuous in a and ω if continuity of exponentiation is to be preserved in the complex domain. Hence, the continuity will be presupposed in the sequel. By Peacock's principle we shall in the sequel understand the principle of conservation of continuity and the crucial algebraic properties $\#$.

LEMMA 1. <u>The function</u> $\phi(a,\omega)$ <u>is linear in the second argument</u>:

$\phi(a,k\cdot\omega) = k\cdot\phi(a,\omega)$.

Proof.

$\cos\phi(a,\omega_1+\omega_2)+i\sin\phi(a,\omega_1+\omega_2) = a^{i\cdot(\omega_1+\omega_2)} = (Pp) =$

$= a^{i\omega_1}\cdot a^{i\omega_2} = (\cos\phi(a,\omega_1)+i\sin\phi(a,\omega_2))\cdot$

$\cdot(\cos\phi(a,\omega_2)+i\sin\phi(a,\omega_2) = \cos(\phi(a,\omega_1)+ \quad (a,\omega_2)) +$

$+ i\sin(\phi(a,\omega_1)+\phi(a,\omega_2))$ i.e.

(1) $\phi(a,\omega_1+\omega_2) = \phi(a,\omega_1) + \phi(a,\omega_2)$.

Linearity follows from additivity (1) and continuity of ϕ.

LEMMA 2. The function $\phi(a,\omega)$ is linear in the logarithm of the first argument:

$\phi(a^k,\omega) = k\cdot\phi(a,\omega)$.

Proof.

$\cos\phi(a_1\cdot a_2,\omega)+i\sin\phi(a_1\cdot a_2,\omega) = (a_1\cdot a_2)^{i\omega} = (Pp) = a_1^{i\omega}\cdot a_2^{i\omega} =$

$= (\cos\phi(a_1,\omega)+i\sin\phi(a_1,\omega))\cdot(\cos\phi(a_2,\omega)+i\sin\phi(a_2,\omega) =$

$= \cos(\phi(a_1,\omega)+\phi(a_2,\omega))+i\sin(\phi(a_1,\omega)+\phi(a_2,\omega))$ i.e.

(2) $\phi(a_1\cdot a_2,\omega) = \phi(a_1,\omega) + \phi(a_2,\omega)$.

Linearity in logarithm follows from (2) and continuity of ϕ.

If follows from LEMMA 1. that

(3) $\phi(a,\omega) = k(a)\cdot\omega$

and from LEMMA 2. that

(4) $\phi(a,\omega) = \ln a\cdot h(\omega)$.

From (3) and (4) we have

$$k(a)\cdot\omega = \ln a \cdot h(\omega)$$

that is

$$\frac{k(a)}{\ln a} = \frac{h(\omega)}{\omega} \qquad \text{for any } a \text{ and } \omega$$

that is

$$\frac{k(a)}{\ln a} = \frac{h(\omega)}{\omega} = c = \text{const.}$$

Hence

$$\phi(a,\omega) = c\cdot\omega\cdot\ln a .$$

So, the only possible definition of exponentiation in the complex domain, which is in accordance with Peacock's principle, is the following one

$$a^{i\omega} = \cos(c\cdot\omega\cdot\ln a) + i\sin(c\cdot\omega\cdot\ln a).$$

It is also easy to see that the crucial algebraic properties # are realy preserved by this definition (for any choice of c).

In particular, we are compelled by Peacock's principle to define

$$e^{i\omega} = \cos(c\cdot\omega) + i\sin(c\cdot\omega),$$

i.e. we are <u>almost</u> compelled to Euler's equation (up to the constant c, which we can choose arbitrarily).

Are we compelled to choose $c=1$ if we want to define exponentiation of complex base with complex exponent in accordance with Peacock's principle? No, we are not:

Let

$$z_1 = r\cdot(\cos\phi + i\sin\phi)$$

and let

$$z_2 = x + iy.$$

Then

$$z_1^{z_2} = (r\cdot(\cos\phi + i\sin\phi))^{(x+iy)} = (Pp) =$$

$$= r^{(x+iy)}\cdot(\cos\phi + i\sin\phi)^{(x+iy)} = (Pp) =$$

$$= r^x \cdot r^{iy} \cdot (\cos\phi + i\sin\phi)^x \cdot (\cos\phi + i\sin\phi)^{iy} =$$

$$= r^x \cdot (\cos(c\cdot y\cdot \ln r) + i\sin(c\cdot y\cdot \ln r))\cdot(\cos(x\cdot\phi) + i\sin(x\cdot\phi))\cdot$$

$$\cdot(\cos\phi + i\sin\phi)^{iy} = r^x\cdot(\cos(x\cdot\phi + c\cdot y \ln e) + i\sin(x\cdot\phi + c\cdot y\cdot \ln r))\cdot$$

$$\cdot(\cos(c\cdot\frac{\phi}{c}\cdot \ln e) + i\sin(c\cdot\frac{\phi}{c}\cdot \ln e))^{iy} =$$

$$= r^x(\cos(x\cdot\phi + c\cdot y\cdot \ln r) + i\sin(x\cdot\phi + c\cdot y\cdot \ln r))\cdot(e^{i\,\phi/c})^{iy} =$$

$$= (Pp) = r^x\cdot e^{-y\cdot\phi/c}\cdot(\cos(x\cdot\phi + c\cdot y\cdot \ln r) + i\sin(x\cdot\phi + c\cdot y\cdot \ln r)),$$

and it is easy to see that the crucial algebraic properties # are preserved by the definition:

$$(r\cdot(\cos\phi + i\sin\phi))^{(x+iy)} = r^x\cdot e^{-y\cdot\phi/c}\cdot(\cos(x\cdot\phi + c\cdot y\cdot \ln r) + i\sin(x\cdot\phi + c\cdot y\cdot \ln r))$$

for any choice of c.

So, Peacock's principle does not compell us to choose (Euler's) $c=1$.

If we add the principle of permanence of diferentiability we are compelled to choose $c=1$. Namely the function $f(z) = a^z$ is diferentiable only for $c=1$. We shall prove this:

The function

$$u + iv = a^{x+iy} =$$

$$= a^x\cdot\cos(c\cdot y\cdot \ln a) + i\, a^x\cdot \sin(c\cdot y\cdot \ln a)$$

is diferentiable only if

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y} \quad \text{and} \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}$$

i.e. only if

$$a^x\cdot \ln a\cdot\cos(c\cdot y\cdot \ln a) = c\cdot a^x\cdot \ln a\cdot\cos(c\cdot y\cdot \ln a)$$

i.e. only if

$$c = 1.$$

<u>Conclusion</u>. We are <u>almost</u> compelled to Euler's equation by Peacock's principle. We are <u>definitely</u> compelled to it if we also accept the principle of permanence of <u>diferentiability</u>. So, Allendoerfer's condition: $d/d\omega(e^{i\omega}) = i\,e^{i\omega}$, or the Curtiss' condition (cf. p.51): $d/dz(e^z) = e^z$

are unnecesarily strong concerning the diferentiation. Besides, they do not take into consideration the most fundamental principle of permanence - Peacock's principle - which has to remain our guide in extending all the operations, as much as it can.

---

1) Notice, that this is not possible for rational numbers. If we define $2^{1/2}$ in accordance with Peacock's principle as $\sqrt[2]{2}$ we do not remain within rationals.

2) In what follows we shall write (for brevity) "Pp" instead of "retaining # by Peacock's principle".

REFERENCES

1. Allendoerfer, C.B., Editorial - The Proof of Euler's Equation, American Mathematical Monthly, vol.55, 1948.

2. Curtiss, D.R., Analytic Functions of a Complex Variable, MAA, 1926.

Zvonimir Šikić
Fakultet strojarstva i brodogradnje
41000 Zagreb, Đ.Salaja 5

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", ZAGREB 1984

ON SOME PROPERTIES OF THE MARTIN-LÖF'S MEASURES OF RANDOMNESS OF FINITE BINARY WORDS

Branislav D.Vidaković

Abstract. In this paper we shall discuss some basic properties of measure of randomness of the binary word x, of the function KB(x), connected with the tests of P.Martin--Löf [1]. Marks and definitions are similar to those in [2].

1. Marks and Definitions. We shall mark the set of all the finite binary words with an X, and the words alone with x,y,z,u,v, etc. With l(x) we shall mark the length of the word x, and $y \subset x$ will mean that y is the beginning piece of the word x. We shall not differentiate the notions "number" and "the finite binary word", because we join the number $x=2^{l(x)}-1+\sum_{i=1}^{l(x)} x_i 2^{l(x)-i}$ to the word $x=x_1x_2\ldots x_n$, $x_i \in \{0,1\}$. We shall mark the set of infinite words with an Ω, and the words alone with $\alpha, \beta, \gamma, \rho, \omega$, etc. The word ω^n is the beginning piece of the word ω which has the length of an n, and the symbol ω_n is the n-th symbol of the word ω. Set Γ_x is the set of all ω which begin with x, i.e. $\{\omega \mid \omega^{l(x)}=x\}$. We think that on the set Ω constructive measure $\mathbb{P}$, (for example by using the sets Γ_x and $P(\Gamma_x)=2^{-l(x)}$) has been introduced. The partially recursive function $\mathcal{F}$, which

is defined on words , we shall call "a process" if $y \subset x$ and $x \in Dom(\mathcal{F}) \Rightarrow y \in Dom(\mathcal{F})$ and $\mathcal{F}(y) \subset \mathcal{F}(x)$. Let the function $\mathcal{U}^2(i,x)$ be universal for the class of all one-dimensional partially recursive functions. Let $F(x) \preccurlyeq G(x)$ be substitute for the predicate $(\exists C)(\forall x)F(x) \leq G(x)+C$, and let $F(x) \asymp G(x)$ be supstitute for the predicate $(\exists C)(\forall x)F(x)=G(x)+C$.

Let the set Ω be given and a constructive measure $\mathbb{P}$ on it. The Martin-Löf test (ML test) is a general recursive function $F(x,y_1,\ldots,y_k)$ with the property

$$\mathbb{P}\{\omega | \omega \in \Omega, F(\omega, y_1,\ldots,y_k) \geq m\} \leq 2^{-m}, \tag{1.1}$$

where $F(\omega, y_1,\ldots,y_k) = \sup_n F(\omega^n, y_1,\ldots,y_k)$.

The word $\omega \in \Omega$ is random with respect to function F if $F(\omega, ,y_1,\ldots,y_k)$ is finite. There is an universal ML test, function U, with the property that $U(x) \succcurlyeq F(x)$ goes for any other ML test F and every $x \in X$.

In 1965. Kolmogorov [3] defined the measure of complexity of the word x with respect to partial recursive function F as

$$K_F(x) = \begin{cases} \min_p \{l(p) \mid F(p)=x\} \\ \infty, (\forall p \in X)\ F(p) \neq x \end{cases} \tag{1.2}$$

There is an optimal function F^o so that for any other function G and every x goes

$$K_{F^o}(x) \preccurlyeq K_G(x). \tag{1.3}$$

The measure $K_{F^o}(x) \equiv K(x)$ is known as Kolmogorov's complexity of the word x. Basic properties of this measure are given in papers [2],[3] and [4] .

In his paper [1] Martin-Löf introduces the measure of randomness of the word x with respect to the assigned ML test F as

$$KB_F(x|y_1,\dots,y_k)= l(x) - \inf_{z \supset x} F(z,y_1,\dots,y_k). \quad (1.4)$$

We introduce the measure $KB_F(x)$ as $KB_F(x|\wedge,\dots,\wedge)$.

2. Basic properties of the measure KB(x)

(i) There is an universal ML test $U(x,y_1,\dots,y_k)$ so that for any other ML test $F(x,y_1,\dots,y_k)$ and every word $x \in X$ goes

$$KB_U(x|y_1,\dots,y_k) \leqslant KB_F(x|y_1,\dots,y_k) \quad (2.1)$$

The proof for this theorem is standard for this theory and is similar to the proof of Theorem 4.1 in [2],page 112. We shall mark the measure $KB_U(x|y_1,\dots,y_k)$ more simply as $KB(x|y_1,\dots,y_k)$.

(ii) Let $G_x(i,y)$ be to result of application of $l(x)$ step of alghoritm which calculates the function $\mathcal{U}(i,y)$, in that case

$$l(x) - \max_{i \leqslant l(x),\, y \subset x} G_x(i,y) \leqslant KB(x) \leqslant l(x) \quad (2.2)$$

The proof follows directly from the construction of universal test U in the proof [2], which has already been mentioned.

(iii) Function KB(x) is "smooth", a.e.

$$KB(xy)-KB(x) \leqslant l(y) \quad (2.3)$$

This property is a direct consequence of inequality $\inf_{z \supset xy} U(z) \geqslant \inf_{z \supset x} U(z)$. But, $\lim_{x \to \infty} KB(x)$ does not exist because $(\forall n)(\exists x)(l(x) \geqslant n)\ KB(x) \asymp 0$. For example $(\forall n)\ KB(\overbrace{00\dots0}^{n}) \asymp 0$. (Picture 1.)

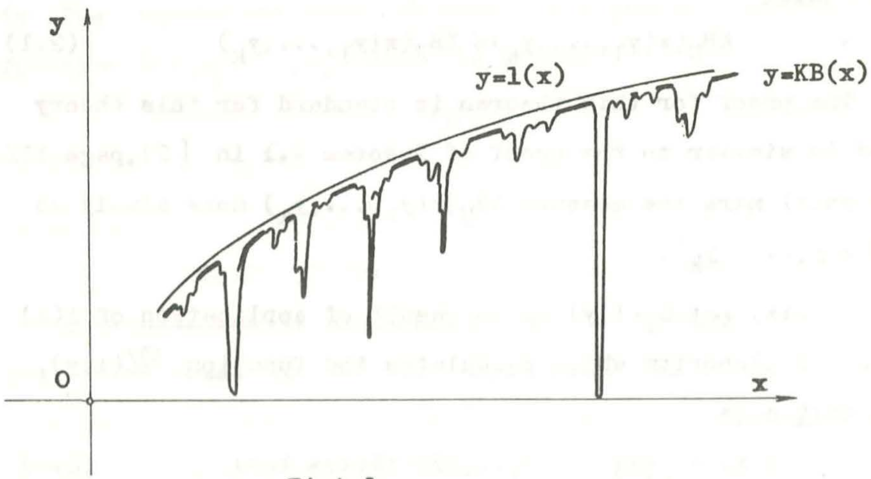
(iv) There is a general recursive function

$\Phi(t,x,y_1,\dots,y_k)$ <u>with the following properties:</u>

$$\Phi(t,x,y_1,\dots,y_k) \leq KB(x\ y_1,\dots,y_k) \tag{2.4}$$

$$\lim_{t\to\infty} \Phi(t,x,y_1,\dots,y_k) = KB(x\ y_1,\dots,y_k) \tag{2.5}$$

The test $U(x,y_1,\dots,y_k)$ is a general recursive function. For every $n\in N$ we form the set $I_n = \{\Lambda,0,1,00,01,10,11,000,\dots$ $\dots,n\}$.



Pict.1.

We define $\Psi(t,x,y_1,\dots,y_k)$ as $\min\limits_{p\in I_n} U(xp,y_1,\dots,y_k)$.

In that case $\Phi(t,x,y_1,\dots,y_k) = l(x) - \Psi(t,x,y_1,\dots,y_k)$.

(v) <u>The function</u> KB(x) <u>is not effective, but a predicate</u>

$$\Pi(x,a) \equiv (KB(x) < a) \tag{2.6}$$

<u>is partially recursive, and set</u>

$$\{x \mid (\exists a)(KB(x)<a) \tag{2.7}$$

<u>is recursively enumerable.</u>

Recursivity of the predicate (2.6) is the result of the recursivity of the the predicate $(\exists t)(\Phi(t,x)<a)$, and

that, in turn, is a result of recursive enumerableness of the set (2.7).

(vi) <u>There are only "a few" words without random, i.e.</u>

$$\mathbb{P}\{\ \Gamma_x \mid KB(x) \leqslant l(x)-m\} \leqslant 2^{-m} \qquad (2.8)$$

$$\mathbb{P}\{\ \Gamma_x \mid KB(x) \leqslant l(x)-m\} = \mathbb{P}\{\ \Gamma_x \mid \inf_{y \supset x} U(y) \geqslant m\} <$$

$$\mathbb{P}\{\ \Gamma_x \mid U(x) \geqslant m\} \leqslant 2^{-m}.$$

So, KB(x) l(x) goes for almost all words x, which justifies the introduction of the measure KB as the measure of the randomness of the word.

(vii) [2]

$$|KB(x) - K(x)| \preccurlyeq (2+\varepsilon)l(l(x)) \qquad (2.9)$$

(viii) <u>Let</u> $\delta(\mathcal{F}(x)) = l(x) - l(\mathcal{F}(x))$. <u>In that case</u>

$$KB(x) - KB(\mathcal{F}(x)) \preccurlyeq \delta(\mathcal{F}(x)) \qquad (2.10)$$

$$KB_{G\circ\mathcal{F}}(x) - KB_G(\mathcal{F}(x)) = \delta(\mathcal{F}(x)) \qquad (2.11)$$

(ix) <u>If</u> ω <u>is a recursive sequence, in that case</u>

$$(\forall n)\ KB(\omega^n) \asymp 0$$

The sequence ω is characteristical for the set $A=\{n_1, n_2, \ldots\} \subseteq N$ if n_1-st, n_2-nd, ... figure in ω is "1" and all other figures are "0". With ω_A we shall mark that the sequence ω is characteristical for the set A. If A is recursive, let's form a function

$$F(\Lambda) = 0$$

$$F(\omega^n) = \sum_{i=1}^{n} \text{ind}\left\{ \left| \frac{W^A(\omega^i)}{i} - \frac{1}{2} \right| \geqslant \frac{1}{2} \right\} \qquad (2.\ 12)$$

where ind S is the indicator of the set S, and $W^A(\omega^i)$ is the number of those ones in the word ω^i which are on the same position as the ones in the sequence ω_A. $F(\omega^n)$ is ML test , and critical set of the test contains only the word ω_A.

So,

$$0 \leqslant KB(\omega_A^n) \preccurlyeq KB_F(\omega_A^n) = 0.$$

(x) <u>For every word</u> $x \in X$

$$KB(x|x) \asymp 0 \tag{2.13}$$

We form the function $F^2(z,x) = \begin{cases} l(x), & x \subset z \\ \Lambda, & \text{otherwise} \end{cases}$

Function F^2 is ML test. $\mathbb{P}\{\omega \mid F(\omega,x) \geqslant m\} = \mathbb{P}\{\omega \mid x \subset \omega, l(x) \geqslant m\} = 2^{-m} + 2^{-m-1} + \ldots = 2^{-m+1}$

$$KB(x|x) \preccurlyeq KB_F(x|x) = 0 .$$

3. References

[1] Martin-Löf, Per, The definition of random seqences, Information and Control 9 (1966).

[2] Звонкин, А.К., Левин, Л.А., Сложность конечных объектов и обоснование понятий информации и случайности с помощу Т-ии алгоритмов, УМН вып. 6 (1956) том XXV ст. 85-127

[3] Колмогоров, А.Н., Три подхода к определению понятия "количество информации", Пробл. пер. инф. 1:1 (1965) 3-7

[4] Banjević, Dragan, On some basic properties of the Kolmogorov complexity, Publ.L'Inst.Math. 30 (44) 1981.

Branislav D.Vidaković,

ul.Nake Spasića br.2/a

11000 BEOGRAD

PROCEEDINGS OF THE CONFERENCE
„ALGEBRA AND LOGIC", ZAGREB 1984

ON ONE DECOMPOSITION OF FUZZY SETS AND RELATIONS

Vojvodić G., Šešelja B.

Abstract. It is known that a fuzzy set $\overline{A}$ on an unempty set S, as a mapping from S to the complete lattice L, uniquely determines the family $\{A_p | p \in L\}$ of subsets of S, such that $\overline{A} = \bigcup_{p \in L} p \cdot A_p$. In |4|, it is proved that $(\{A_p | p \in L\}, \subseteq)$ is a lattice isomorphic to the quotient relative to one closure operation in L.

Here we prove that $\overline{A}$ uniquely determines one family $\{\overline{A}p | p \in L\}$ of fuzzy sets on S, and vice-versa, proving the theorems of decomposition and synthesis. This decomposition preserves the properties of fuzzy congruence relation (defined in |2|) on algebras, and using this we prove some relations in the class of factor algebras modulo fuzzy congruence relation, defined in |3|.

The main definitions and the notation are the same as in |3| and |4|.

1. Let $S \neq \emptyset$ and let $L = (L, \wedge, \vee, 0, 1)$ be a complete lattice. Let $\overline{A} : S \to L$ be a fuzzy set on S, and for every $p \in L$, let $\overline{A}p : S \to L$ be a fuzzy set on S, such that for every $x \in S$

$$\overline{A}p(x) = \begin{cases} \overline{A}(x), & \text{if } \overline{A}(x) \geq p \\ 0, & \text{otherwise.} \end{cases} \qquad (*)$$

PROPOSITION 1.1.

(1) $\overline{A}p(x) \in \{0\} \cup [p)$, <u>for every</u> $x \in S$, <u>where</u> $[p)$ <u>is a principal filter in</u> L, <u>generated by</u> p.

(2) <u>If</u> $s, t \in L$, <u>and</u> $s \leq t$, <u>then</u>:

(2.1) $\overline{A}t(x) \neq 0$ <u>implies</u> $\overline{A}s(x) = \overline{A}t(x)$.

(2.2) <u>If</u> $\overline{A}s(x) = t$, <u>then</u> $\overline{A}t(x) = t$.

<u>Proof.</u> Directly from (*) □

THEOREM 1.2. (<u>DECOMPOSITION</u>) <u>If</u> $\overline{A} : S \to L$ <u>is a fuzzy set on</u> S, <u>then</u>

$$\overline{A} = \bigcup_{p \in L} \overline{A}p \quad .$$

(The union is a fuzzy one, see for example |1|).

<u>Proof.</u> Let $\overline{A}(x) = q$, $x \in S$. Then

$$(\bigcup_{p \in L} \overline{A}p)(x) = \bigvee_{p \in L} \overline{A}p(x) = \bigvee_{p \leq q} \overline{A}p(x) \vee \bigvee_{p \not\leq q} \overline{A}p(x) = \bigvee_{p \leq q} q \vee 0 = q. \ \square$$

PROPOSITION 1.3. <u>If</u> $\overline{A} : S \to L$, <u>is a fuzzy set on</u> S, <u>then</u>

(3) $\overline{A} = \overline{A}0$

(4) $\overline{A} = \bigcup_{p>0} \overline{A}p$

<u>Proof.</u>

(3) Directly from (*) .

(4) Let $\overline{A}(x) = q$, $x \in S$. Then, if $q \neq 0$, the proof is similar to the one of Proposition 2, and if $q = 0$ then it follows from (*) that for every $p \neq 0$, $\overline{A}p(x) = 0$. Then also

$$(\bigcup_{p>0} \overline{A}p)(x) = 0 \ . \qquad \square$$

PROPOSITION 1.4. <u>Let</u> $\overline{A} : S \to L$ <u>be a fuzzy set on</u> S. <u>Then for every</u> $x \in S$:

(5) <u>If</u> $s,t \in L$ <u>and</u> $s \leq t$, <u>then</u> $\overline{At} \subseteq \overline{As}$ (<u>the inclusion is a fuzzy one |1|</u>).

(6) <u>If</u> $s,t \in L$ <u>then for</u> $x \in S$
$\overline{As}(x) \neq 0$ <u>and</u> $\overline{At}(x) \neq 0$ <u>imply</u> $\overline{As}(x) = \overline{At}(x)$.

Proof. (5) Directly from (2.1).

(6) If $x \in S$, from $s \wedge t \leq t$, it follows that $\overline{A}(s \wedge t)(x) = \overline{A}t(x)$, and $s \wedge t \leq s$ imply $\overline{A}(s \wedge t)(x) = \overline{A}s(x)$ (all because of (2.1)).
Thus, $\overline{A}t(x) = \overline{A}s(x)$, for every $x \in S$. □

Remark. (6) is equivalent with $\bigcup_{q \geq p} \overline{Aq} = \overline{Ap}$.

THEOREM 1.5. (SYNTHESIS) Let $S \neq \emptyset$ and let $L = (L, \wedge, \vee, 0, 1)$ be a complete lattice. Also let $\{\overline{A}p \mid p \in L\}$ be a family of fuzzy sets on S (for $p \in L$, $\overline{A}p : S \to L$) satisfying the conditions (1) and (2) from Proposition 1.1.

Then, if $\overline{A} \overset{def}{=} \overline{A}0$, the following is satisfied.

(i) $$\overline{A} = \bigcup_{p>0} \overline{Ap} .$$

(ii) If $x \in S$, then for every $p \in L$

$$\overline{A}p(x) = \begin{cases} \overline{A}(x), & \text{if } \overline{A}(x) \geq p \\ 0, & \text{otherwise .} \end{cases}$$

Proof. (i) Let $\overline{A}(x) = t \in L$. We shall consider two cases:

I $t = 0$. Then, $\overline{A0}(x) = 0$, and by (5), for every $p \in L$ $\overline{Ap}(x) = 0$, and hence

$$\bigvee_{p>0} \overline{Ap}(x) = 0 = t .$$

II $t \neq 0$. Then, because of (2.2), $\overline{A0} = t$ implies $\overline{At}(x) \neq 0$. Now, since for every $s \in L$, $\overline{A}s(x) \neq 0$ (by (2.1)). it follows by (6) that $\overline{A}s(x) = t$.
(We may use (5) and (6) since those are the consequences of (2.1)).

Thus, for every $s > 0$, $s \in L$,

$$\overline{As}(x) = \overline{A0}(x) = \overline{At}(x) = t ,$$

and hence, again

$$\bigvee_{p>0} \overline{Ap}(x) = t.$$

(ii) If $\overline{A}(x) = 0$, for $x \in S$, the equality is obvious. Suppose now that $\overline{A}(x) = \overline{A0}(x) = s \neq 0$. Here, again, we have two cases:

a) $s \geq p$, where $\overline{Ap}$ is given in (ii). By (2.2), $\overline{As}(x) = s$, and since $p \leq s$, by (2.1)

$$\overline{Ap}(x) = \overline{A}s(x) = \overline{A}0(x) = \overline{A}(x).$$

b) $s \not\geq p$. Now, by (6), $\overline{A0} = s$ implies

$$\overline{Ap}(x) = 0 \quad \text{or} \quad \overline{Ap}(x) = s .$$

Because of (1), $\overline{Ap}(x) \neq s$, and hence $\overline{Ap}(x) = 0$. ⊓

PROPOSITION 1.6. _Let_ $\overline{A} : S \to L$, _and for_ $p \in L$ _let_ $\overline{Ap} : S \to L$, _defined by (*). Then the following is satisfied:_

(a) _If_ $q \in L$ _and_ $q \neq 0$, _then_ $Ap_q = A_{p \vee q}$

(b) $Ap_o = A_o = S$.

Here we use the definition: If $p \in L$, _then_ $A_p \subseteq S$ _such that for_ $x \in S$

$$x \in A_p \quad \text{iff} \quad \overline{A}(x) \geq p \quad (\text{see } |1|) .$$

Proof. (a) The equality $A_{p \vee q} = A_p \cap A_q$ (proved in |4|) imply:

$$
\begin{aligned}
x \in A_{p \vee q} \quad & \text{iff} \quad x \in A_p \cap A_q , \\
& \text{iff} \quad x \in A_p \ \text{ and } \ x \in A_q , \\
& \text{iff} \quad \overline{A}(x) \geq p \ \text{ and } \ \overline{A}(x) \geq q , \\
& \text{iff} \quad \overline{A}(x) = \overline{Ap}(x) \geq q , \\
& \text{iff} \quad x \in Ap_q .
\end{aligned}
$$

$$
\begin{aligned}
\text{(b)} \quad x \in Ap_o \quad & \text{iff} \quad \overline{A}p(x) \geq 0 , \\
& \text{iff} \quad \overline{A}(x) \geq 0 , \\
& \text{iff} \quad x \in A_o = S. \quad ⊓
\end{aligned}
$$

Thus we have proved that the usual decomposition of the fuzzy set $\overline{Ap}$, $p \in L$, is the same as the one of $\overline{A}$ for all $q \geq p$ and is the restriction to $p \vee q$ otherwise. Ap_o is, for every p, equal S.

2. The definition (*), when applied on the fuzzy equivalence relations (defined in |1|), preserves their properties. Moreover, if $\overline{\rho}$ is a fuzzy congruence relation on an algebra A (see |3|), $\overline{\rho p}$ is for every $p \in L$ a fuzzy congruence relation on A, as well.

Let $A = (A,F)$ be an algebra, $L = (L, \wedge, \vee, 0, 1)$ a complete lattice, and $\overline{\rho} : S^2 \to L$ a fuzzy congruence relation on A |2| (that is:

For all $x,y \in A$ $\quad \overline{\rho}(x,x) = 1$,

$$\overline{\rho}(x,y) = \overline{\rho}(y,x) \ ,$$

$$\overline{\rho}(x,y) \geq \bigvee_{z \in A} (\overline{\rho}(x,z) \wedge \overline{\rho}(z,y)), \text{ and}$$

if $\overline{\rho}(x_i,y_i) = p_i$, $i = 1,\dots,n$, then for $f \in F$

$$\overline{\rho}(f(x_1,\dots,x_n),f(y_1,\dots,y_n)) \geq \bigwedge_{i=1}^{n} p_i) \ .$$

If $\overline{\rho}$ is a fuzzy congruence relation on A, and $p \in L$, the definition (*) has the following form:

$\overline{\rho}p : A^2 \to L$, and if $(x,y) \in A^2$

$$\overline{\rho}p(x,y) = \begin{cases} \overline{\rho}(x,y) & \text{if } \overline{\rho}(x,y) \geq p \\ 0 & \text{otherwise} \ . \end{cases} \qquad (**)$$

PROPOSITION 2.1. <u>If $\overline{\rho} : A^2 \to L$ is a fuzzy congruence relation on A, then for every $p \in L$ $\overline{\rho p}$ (defined in (**)) is a fuzzy congruence relation on A, as well.</u>

<u>Proof</u>. $\overline{\rho}p$ is reflexive, since $\overline{\rho}(x,x) = 1$ for all $x \in A$, and thus $\overline{\rho}p(x,x) = 1$.

$\overline{\rho}p$ is obviousli symmetric.

To prove that $\overline{\rho}p$ is transitive, we shall consider two cases.

I If for $x,y,z \in A$ $\bar{\rho}p(x,z) = 0$ or $\bar{\rho}p(z,y) = 0$, then, clearly,

$$\bar{\rho}p(x,y) \geq \bar{\rho}p(x,z) \wedge \bar{\rho}p(z,y) .$$

II Let $\bar{\rho}p(x,z) \neq 0$ and $\bar{\rho}p(z,y) \neq 0$, $x,y,z \in A$. Then,

$$\bar{\rho}p(x,z) = \bar{\rho}(x,z) \geq p, \text{ and}$$

$$\bar{\rho}p(z,y) = \bar{\rho}(z,y) \geq p .$$

Hence,

$$p \leq \bar{\rho}p(x,z) \wedge \bar{\rho}p(z,y) = \bar{\rho}(x,z) \wedge \bar{\rho}(z,y) \leq \bar{\rho}(x,y) .$$

Thus, $\bar{\rho}p(x,y) \geq p$, and $\bar{\rho}p(x,y) = \bar{\rho}(x,y)$, i.e.

$$\bar{\rho}p(x,y) \geq \bar{\rho}p(x,z) \wedge \bar{\rho}p(z,y) .$$

Since this inequality holds for every $z \in A$, it follows that $\bar{\rho}p$ is transitive.

Let now f be an n-ary operation from F, and for $x_1,\dots,x_n,y_1,\dots,y_n \in A$, let $\bar{\rho}p(x_i,y_i) = p_i \in L$. Then again we have two cases:

i) $p_i = 0$, for some $i \in \{1,\dots,n\}$. Then clearly $\bigwedge_{i=1}^{n} p_i = 0$, and

$$\bar{\rho}p(f(x_1,\dots,x_n),f(y_1,\dots,y_n)) \geq \bigwedge_{i=1}^{n} p_i .$$

ii) $p_i \neq 0$, for every $i \in \{1,\dots,n\}$. Then,

$$p_i = \bar{\rho}p(x_i,y_i) = \bar{\rho}(x_i,y_i) \geq p , \quad i = 1,\dots,n .$$

Hence

$$p \leq \bigwedge_{i=1}^{n} \bar{\rho}p(x_i,y_i) = \bigwedge_{i=1}^{n} \bar{\rho}(x_i,y_i) \leq \bar{\rho}(f(x_1,\dots,x_n),f(y_1,\dots,y_n)).$$

Thus,

$$\bar{\rho}p(f(x_1,\dots,x_n),f(y_1,\dots,y_n))=\bar{\rho}(f(x_1,\dots,x_n),f(y_1,\dots,y_n))\geq\bigwedge_{i=1}^{n} p_i .$$

This proves that $\bar{\rho}p$ is a fuzzy congruence relation on A. □

COROLLARY 2.2. _If $\overline{\rho} : A^2 \to L$ is a fuzzy congruence relation on the algebra_ A, _then_

$$\overline{\rho} = \bigcup_{p>0} \overline{\rho p} \quad .$$

Proof. By Proposition 1.3 and Proposition 2.1. □

COROLLARY 2.3. _Let_ $\{\overline{\rho p} \mid p \in L\}$ _be a family of fuzzy congruence relations on algebra_ $A = (A,F)$, _where_ $L = (L, \wedge, \vee, 0, 1)$ _is a complete lattice._

Now, if $\{\overline{\rho p} \mid p \in L\}$ _satisfy the conditions of Proposition 1.5, then_

$$\overline{\rho} = \bigcup_{p>0} \overline{\rho p}$$

is a fuzzy congruence relation on A.

Proof. By Proposition 1.5, since $\overline{\rho} = \overline{\rho}0$. □

The following definitions are from |3|.

If $\overline{\rho}$ is a fuzzy congruence relation on $A = (A,F)$, then

$$A/\overline{\rho} \stackrel{\text{def}}{=} \{[x]_{\overline{\rho}} \mid x \in A\} \ , \quad \text{where}$$

$[x]_{\overline{\rho}} : A \to L$, such that $[x]_{\overline{\rho}}(a) \stackrel{\text{def}}{=} \overline{\rho}(x,a)$, $a \in A$.

Now, if $f \in F$, then

$$\overline{f}([x_1]_{\overline{\rho}},\ldots,[x_n]_{\overline{\rho}}) \stackrel{\text{def}}{=} \bigcup_{p \in L} (p \cdot f([x_1]_{\rho_p},\ldots,[x_n]_{\rho_p})), \text{ where}$$

$\overline{\rho} = \bigcup_{p \in L} p \cdot \rho_p$ is the usual decomposition of a fuzzy set $\overline{\rho}$.

Thus, $A/\overline{\rho} = (A/\overline{\rho}, F)$. For $p \in L$ A/ρ_p is the factor algebra modulo ρ_p, which is an ordinary congruence relation on A.

PROPOSITION 2.4. _Let_ $\overline{\rho}$ _be a fuzzy congruence relation on_ $A = (A,F)$. _Then, for_ $p \in L$,

1° $A/\overline{\rho}p \cong A/\overline{\rho}$.

2° $(A/\rho p_q)/(\rho_q/\rho p_q) \cong A/\rho_q$, for every $q \in L$.

Proof. By the definition of $A/\overline{\rho}$, and by Proposition 1.6. □

REFERENCES

|1| Kaufmann, A., Introduction a la theorie des sous-ensembles flous, Paris, 1973.

|2| Vojvodić, G., Šešelja, B., O strukturi slabih relacija ekvivalencije i slabih relacija kongruencije, Matematički Vesnik 1(14)(29)1974, 147-152.

|3| Vojvodić, G., Šešelja, B., On Fuzzy Quotient Algebras, Zbornik radova PMF, Novi Sad, (to appear).

|4| Šešelja, B., Vojvodić, G., Fuzzy Sets on S as Closure Operations on P(S), Zbornik radova PMF, Novi Sad, (to appear).

Institute of Mathematics
University of Novi Sad
Dr Ilije Djuričića 4
21000 Novi Sad
Yugoslavia

THE RELATIONS BETWEEN THE ASSOCIATOR, THE DISTRIBUTOR AND THE COMMUTATOR AND A RADICAL PROPERTY OF A NEAR-RING

Veljko Vuković

Abstract. The concepts of (in general nonassociative and nondistributive) near-ring S, a left (a right) near-ring, a d.g. near-ring, the associator, the distributor, an ideal of S, the relative distributor (r.d.) of a subset T of S, an S-subgroup of (S,+), the normal associator (distributor) subgroup of (S,+), the associator (the distributor) ideal of S etc. are defined in [1]. The radical J(S), the quasiradical Q(S) and the radical subgroup N(S) of a near-ring S and a small ideal of S are defined in [2].

In this paper we have examined the relations between the associator, the distributor and the commutator of a near-ring, respectively of a left (a right) near-ring and of a d.g. near-ring and the necessary and sufficient conditions that the associator (the distributor) be an ideal (Th. 1.-7.), the sufficient conditions that the radical J(S) of a left unitary near-ring S coincides with the quasiradical Q(S) and with the radical subgroup N(S) of S (Th.8.)

THE CONDITIONS THAT THE ASSOCIATOR (THE DISTRIBUTOR) BE AN IDEAL OF A NEAR-RING S

Let A(S) be the associator of a near-ring S. Denote the set $\{x\pm a-x / x\in S,\ a\in A(S)\}$ by B, the set ${}_{L}D\cup{}_{d}D=\{d_1=s((s_1s_2)s_3-s_1(s_2s_3))+s(s_1(s_2s_3))-s((s_1s_2)s_3)/s,s_1,s_2,s_3\in S\}\cup\{d_2=((ss_1)s_2)s_3-(s(s_1s_2))s_3+(s(s_1s_2)-(ss_1)s_2)s_3/s,s_1,s_2,s_3\in S\}$ by $D_S^{S^3}$ and the identity of (S,+) by o. The set ${}^{L}D=\{d=s(x\pm a-x)-s(\pm a-x)-sx/ s,\ x\in S,\ a\in A(S)\}$ (${}^{d}D=\{\overline{d}=-(\pm a-x)s-xs+(x\pm a-x)s/x,s\in S,\ a\in A(S)\}$) is called the left distributor (l.d.) (the right distributor (r.d.)) of the set B in S and ${}^{L}D\cup{}^{d}D$ the distributor (d.) of the set B in S.

THEOREM 1. <u>The normal associator subgroup</u> $\overline{A}(S)$ <u>of a near-ring S is an ideal of S if it is a right (or a left) S-subgroup, contains its own r.d.</u> D_r <u>in</u> S, <u>the distributor of the set</u> B <u>in</u>

S and $D_S^{S^3}$. Conversely, if the normal associator subgroup $\overline{A}(S)$ is an ideal of S and o·s, s·o $\in \overline{A}(S)$, for all $s\in S$ then it is an S-subgroup, contains its own r.d. in S, the d. of the set B in S and $-{}_LD+{}_dD=\{-d_1+d_2/d_1\in {}_LD,\ d_2\in {}_dD\}$. If A(S) contains ${}_LD$ or ${}_dD$ then it contains $D_S^{S^3}$.

Proof. Let $\overline{A}(S)$ be a right S-subgroup, let it contains its own r.d. in S, ${}^LD$ and $D_S^{S^3}$. Then, since $a\in A(S)$ if and only if there exist $s_1,s_2,s_3\in S$ such that $a=(s_1s_2)s-s_1(s_2s_3)$, $xa=x((s_1s_2)s_3-$ $-s_1(s_2s_3))=d_1+x((s_1s_2)s_3)-x(s_1(s_2s_3))=d_1+\overline{a}+(x(s_1s_2))s_3-x(s_1(s_2s_3))$, where $d_1=x((s_1s_2)s_3-s_1(s_2s_3))+x(s_1(s_2s_3))-x((s_1s_2)s_3)$ and $\overline{a}=$ $=x((s_1s_2)s_3)-(x(s_1s_2))s_3$. Hence, $x((s_1s_2)s_3)=\overline{a}+(x(s_1s_2))s_3$. Since $(x(s_1s_2)-(xs_1)s_2)s_3 = a's_3\in\overline{A}(S)$ respectively $(x(s_1s_2))s_3-$ $-((xs_1)s_2)s_3+d_2=a's_3$ (where $d_2=((xs_1)s_2)s_3-(x(s_1s_2))s_3+(x(s_1s_2)-$ $-(xs_1)s_2)s_3$) and from here $(x(s_1s_2))s_3=a's_3-d_2+((xs_1)s_2)s_3)$ and since $((xs_1)s_2)s_3-(xs_1)(s_2s_3)=\overline{\overline{a}}\in\overline{A}(S)$ respectively $((xs_1)s_2)s_3=$ $=\overline{\overline{a}}+(xs_1)(s_2s_3)$, then $xa=d_1+\overline{a}+a's_3-d_2+\overline{\overline{a}}+(xs_1)(s_2s_3)-x(s_1(s_2s_3))=$ $=d_1+\overline{a}+a's_3-d_2+\overline{\overline{a}}+a''\in\overline{A}(S)$, for all $x\in S$.

Since for arbitrary $a_1,a_2\in A(S)$ and $s\in S$, there exist $d',d''\in D_r$ such that $s(a_1+a_2)=d'+sa_1+sa_2\in\overline{A}(S)$ and $(a_1+a_2)s=a_1s+a_2s+d''\in\overline{A}(S)$, inductively one can obtain that $s\sum_i\pm a_i\in\overline{A}(S)$, for all $a_i\in A(S)$, all $s\in S$ and $i\in N$.

Since, by the definition of $\overline{A}(S)$, $\overline{a}\in\overline{A}(S)$ if and only if there exist $a_i\in A(S)$, $x_i\in S$ and $i\in N$ such that $\overline{a}=\sum_{i=1}^{n}(x_i\pm a_i-x_i)$ then for arbitrary $x\in S$ and $\overline{a}\in\overline{A}(S)$ there exist $\overline{d}_L$, $d_i\in D_r$ and $d^i\in {}^LD$ such that $x\overline{a} = \overline{d}_L+\sum_i x(x_i\pm a_i-x_i)) = \overline{d}_L+\sum_i(d^i+xx_i+d_i\pm xa_i-xx_i)\in\overline{A}(S)$ (respectively $\overline{a}x=(\sum_i(x_i\pm a_i-x_i))x=\sum_i(x_ix\pm a_ix-x_ix+\overline{d}_i+d_d^i)+\overline{d}_d\in\overline{A}(S)$, for all $\overline{a}\in\overline{A}(S)$, all $x\in S$, some $\overline{d}_d,\overline{d}_i\in D_r$ and some $d_d^i\in {}^dD$).

Since for any $s,s_1 \in S$ and for any $\bar{a} \in \bar{A}(S)$ there exist $d_L, d_d \in D_r$ such that $s_1(s+\bar{a})-s_1 s = d_L + s_1 s + s_1\bar{a} - s_1 s \in \bar{A}(S)$ and $(s+\bar{a})s_1 - ss_1 = ss_1 + \bar{a}s_1 + d_d - ss_1 \in \bar{A}(S)$ then $\bar{A}(S)$ is an ideal of S.

If $(S,+,\cdot)$ is an associative near-ring with zero then ${}_LD = {}_dD = o$.

Conversely, let $\bar{A}(S)$ be an ideal of a near-ring S and $o\cdot s$, $s\cdot o \in \bar{A}(S)$. Then, $\bar{A}(S)$ is an S-subgroup, i.e. $ax, xa \in \bar{A}(S)$, for all $a \in \bar{A}(S)$ and all $s \in S$ by the definition. Also, $x(s+a)-xs = d_L + xs + xa - xs \in \bar{A}(S) \Longrightarrow d_L \in \bar{A}(S)$, for all $x,s \in S$ and all $a \in \bar{A}(S)$. Similarly, $d_d \in \bar{A}(S)$.

Likewise, from $s\bar{a} = s(x\pm a-x) = d+sx+s(\pm a-x) = d+sx+d_r \pm sa - sx \in \bar{A}(S)$ follows $d \in \bar{A}(S)$ for (some $d_r \in D_r$, some $d \in {}^LD$ and) all $s,x \in S$ and all $a \in A(S)$. Similarly, from $\bar{a}s = (x\pm a-x)s = (x\pm a)s - xs + \bar{d}_d \in \bar{A}(S)$ follows $\bar{d}_d \in \bar{A}(S)$, for all $x,s \in S$, all $a \in A(S)$ and some $\bar{d}_d \in {}^dD$.

Since $xa = d_1 + \bar{a} + a's_3 - d_2 + \bar{\bar{a}} + a'' \in \bar{A}(S)$, for all $x \in S$ and $a \in A(S)$, where $\bar{a} = x((s_1 s_2)s_3) - (x(s_1 s_2))s_3$, $a' = x(s_1 s_2) - (xs_1)s_2$ and $d_1, d_2, \bar{\bar{a}}, a'', a'$ as above, then $d_1 + \bar{a} + a's_3 - d_2 \in \bar{A}(S)$. Hence, $-d_1 + (d_1 + \bar{a} + a's_3 - d_2) + d_1$ from $\bar{A}(S)$ and $\bar{a} + a's_3 - d_2 + d_1 \in \bar{A}(S)$ ......(+). From (+) follows that $-d_2 + d_1 \in \bar{A}(S)$ ....(-).

If $\bar{A}(S)$ contains ${}_LD$ or ${}_dD$ then from (-) follows that it contains $D_S^{S^3}$.

COROLLARY. *If the normal associator subgroup $\bar{A}(S)$ of a near-ring S with zero is an ideal of S then it is an S-subgroup, contains its own r.d. in S, the set $-{}_LD + {}_dD = \{-d_1+d_2 \,/\, d_1$ $d_1 \in {}_LD$, $d_2 \in {}_dD\}$ and the distributor of the set B in S.*

THEOREM 2. *The normal associator subgroup A(S) of a right (a left) near-ring S is an ideal of S if it is a right (a left) S-subgroup, contains its own r.d. in S, the left d. (the r.d.) of the set B in S and the distributor ${}_LD$ (${}_dD$). Conversely,* if the normal associator subgroup $\bar{A}(S)$ of a right (a left) near-ring S is an ideal and $s\cdot o\in\bar{A}(S)$ ($o\cdot s\in A(S)$) then it is an S-subgroup and contains its own r.d. in S, the distributor $_LD$ ($_dD$) and the d. of the set B in S.

Proof. This theorem follows from Th. 1.

COROLLARY 1. The normal associator subgroup $\bar{A}(S)$ of a right (a left) near-ring S with zero is an ideal if and only if it is a right (a left) S-subgroup, contains its own r.d. in S, the d. of the set B in S and the distributor $_LD$ ($_dD$).

COROLLARY 2. If the normal associator subgroup A(S) of a right near-ring S contains its own r.d. in S, the l.d. of the set B in S, the distributor $_LD$ and it is a right S-subgroup then S/A(S) is an associative near-ring.

THEOREM 3. Let S be a d.g. right (or left) near-ring. Then, the normal associator subgroup $\bar{A}(S)$ is an ideal of S if it is a left (or a right) S-subgroup and $S'S^3$ (or S^3S') is additively commutative. ($(S',\cdot)$ is a subgroupoid of the left (right) distributive elements of S which additively generate S).

Proof. If the normal associator subgroup $\bar{A}(S)$ of a right d.g. near-ring S is a left S-subgroup then for each $\bar{a}=\sum_{i=1}^{n}(x_i\pm a_i-x_i)$ of $\bar{A}(S)$ holds $\bar{a}x=\sum_{i=1}^{n}(x_ix\pm a_ix-x_ix)$. It remains to prove that $ax\in\bar{A}(S)$ for all $a\in A(S)$ and all $x\in S$. If $S'S^3$ is additively commutatitive then, for any $s_1,s_2,s_3,x\in S$, $a=(s_1s_2)s_3-s_1(s_2s_3)$ from A(S) and $ax=((s_1s_2)s_3-s_1(s_2s_3))x=$(Since $((s_1s_2)s_3)x-(s_1s_2)(s_3x)=\tilde{a}$ then $((s_1s_2)s_3)x=\tilde{a}+(s_1s_2)(s_3x))=\tilde{a}+(s_1s_2)(s_3x)-(s_1(s_2s_3))x=$(Since $(s_1s_2)(s_3x)-s_1(s_2(s_3x))=\tilde{\tilde{a}}$ then $(s_1s_2)(s_3x)=\tilde{\tilde{a}}+s_1(s_2(s_3x))$) $=\tilde{a}+\tilde{\tilde{a}}+s_1(s_2(s_3x))-(s_1(s_2s_3))x=$ (Since $s_1(s_2(s_3x)-$

$-(s_2s_3)x)=s_1a_1$ and since $s_1a_1=s_1(s_2(s_3x)-(s_2s_3)x)=\sum_i \pm s^i(s_2(s_3x)-$
$-(s_2s_3)x) = \pm s^1(s_2(s_3x)-(s_2s_3)x)\pm \dots \pm s^n(s_2(s_3x)-(s_2s_3)x) =$
$=\pm s^1(s_2(s_3x))\mp s^1((s_2s_3)x)\pm \dots \pm s^n(s_2(s_3x))\mp s^n((s_2s_3)x =$
$=(\pm s^1\pm \dots \pm s^n)(s_2(s_3x))-(\pm s^1\pm \dots \pm s^n)((s_2s_3)x)=s_1(s_2(s_3x))-$
$-s_1((s_2s_3)x)$, then $s_1(s_2(s_3x))=s_1a_1+s_1((s_2s_3)x)\ ) = \tilde{a}+\tilde{\tilde{a}}+s_1a_1+$
$+s_1((s_2s_3)x)-(s_1(s_2s_3))x = \tilde{a}+\tilde{\tilde{a}}+s_1a_1+a_2 \in \bar{A}(S)$, where $a_2=$
$=s_1((s_2s_3)x)-(s_1(s_2s_3))x$ and $s^i \in S'$, $i=1,\dots,n$.
Similarly, $x(s+a)-xs=\sum_i \pm x^i(s+a)-\sum_i \pm x^i s = \pm x^1(s+a)\pm \dots \pm$
$\pm x^k(s+a)-(\pm x^1 s\pm \dots \pm x^k s)=\pm x^1 s\pm x^1 a\pm \dots \pm x^k s\pm x^k a\mp x^k s\mp \dots \mp x^1 s\in A(S)$
for all $x,s\in S$ and $a\in\bar{A}(S)$.

COROLLARY. _If S is a right d.g. near-ring, the associator normal subgroup $\bar{A}(S)$ of S is a left S-subgroup and $S'S^3$ is additively commutative then $S/\bar{A}(S)$ is an associative near-ring._

THEOREM 4. _The normal associator subgroup $\bar{A}(S)$ of a right (a left) d.g. near-ring S is an ideal of S if and only if it is a right (a left) S-subgroup and contains the distributor $_LD$ ($_dD$)._

Proof. If $\bar{A}(S)$ is a right (a left) S-subgroup of (S,+) and contains the distributor $_LD$ ($_dD$) then we conclude as in the proof of Th. 1. that $xa\in\bar{A}(S)$, for all $a\in A(S)$ and all $x\in S$. But since S is a right d.g. near-ring we have $x\bar{a}=\sum_i s^i\bar{a} =$ $=\sum \pm(\sum_j (s^i x_j \pm s^i a_j - s^i x_j)) \in \bar{A}(S)$ for all $x\in S$ and all $\bar{a}\in\bar{A}(S)$. As in the proof of Th. 3. we see now that $A(S)$ is an ideal of S.

COROLLARY. _If the normal associator subgroup $\bar{A}(S)$ of a right d.g. near-ring contains the distributor $_LD$ and it is a right S-subgroup then $S/\bar{A}(S)$ is a right distributively generated associative near-ring._

THEOREM 5. <u>If the left (the right) normal distributor subgroup</u> $\overline{D}_L$ ($\overline{D}_d$) <u>of a near-ring</u> S <u>contains the associator</u> A(S) <u>of</u> S <u>then it is a left (a right) ideal of</u> S.

<u>Proof</u>. Next we prove that $\overline{D}_L$ ($\overline{D}_d$) is a left (a right) S-subgroup. Since, by the definition of $\overline{D}_L$ ($\overline{D}_d$), $\overline{d}_L \in \overline{D}_L$ ($\overline{d}_d \in \overline{D}_d$) if and only if there exist $d_L^i \in D_L$ ($d_d^i \in D_d$) and $x_i \in S$ such that $\overline{d}_L = \sum_{i=1}^n (x_i \pm d_L^i - x_i)$) then $x\overline{d}_L = x\sum_{i=1}^n (x_i \pm d_L^i - x_i) = d + \sum_{i=1}^n (xx_i \pm xd_L^i - xx_i)$, for some $d \in \overline{D}_L$ and some $n \in N$) ($d_d x = (\sum_{i=1}^n (x_i \pm d_d^i - x_i))x = \sum_{i=1}^n (x_i x \pm d_d^i x - x_i x) + \overline{d}$, for some $\overline{d} \in \overline{D}_d$, some $n \in N$ and all $x \in S$. It remains to prove that $xd_L^i \in \overline{D}_L$ ($d_d^i x \in \overline{D}_d$), for all $x \in S$ and all $d_L^i \in \overline{D}_L$ (respec. $d_d^i \in \overline{D}_d$).

By the definition of D_L, $d_L \in D_L$ if, and only if there exist $s_1, s_2, s \in S$ such that $d_L = s(s_1+s_2) - ss_2 - ss_1$. Then, for every $x \in S$ $xd_L = x(s(s_1+s_2)-ss_2-ss_1) = d'_L + x(s(s_1+s_2)) - x(ss_2) - x(ss_1) =$ (Since $x(s(s_1+s_2)) - (xs)(s_1+s_2) = -a$ then $x(s(s_1+s_2)) = -a + (xs)(s_1+s_2)$; $x(ss_2) - (xs)s_2 = -a_1 \Longrightarrow x(ss_2) = -a_1 + (xs)s_2$ and $x(ss_1) - (xs)s_1 = -a_2 \Longrightarrow x(ss_1) = -a_2 + (xs)s_1$) $= d'_L - a + (xs)(s_1+s_2) - (xs)s_2 + a_1 - (xs)s_1 + a_2 = d'_L - a + (xs)(s_1+s_2) - (xs)s_2 - (xs)s_1 + a'_1 + a_2 = d'_L - a + d''_L + a'_1 + a_2 \in \overline{D}_L$, because $d''_L = (xs)(s_1+s_2) - (xs)s_2 - (xs)s_1$, $a_1 - (xs)s_1 = -(xs)s_1 + a'_1$ and, from here, $a'_1 = (xs)s_1 + a_1 - (xs)s_1 \in \overline{D}_L$

Also, $x(s+d_L) - xs = \tilde{d}_L + xs + xd_L - xs \in \overline{D}_L$, for all $x, s \in S$ and all $d_L \in \overline{D}_L$. (Similarly, $d_d x \in \overline{D}_d$ and $(s+d_d)x - sx \in \overline{D}_d$, for all $d_d \in \overline{D}_d$ and all $x, s \in S$).

THEOREM 6. <u>The left (the right) normal distributor subgroup</u> $\overline{D}_L$ ($\overline{D}_d$) <u>of a right (a left) associative near-ring</u> S <u>is an ideal of</u> S.

<u>Proof</u>. We prove that $\overline{D}_L$ ($\overline{D}_d$) is a right (a left) S-subgroup.

For any $d_L \in D_L$ and any $s, s_1 \in S$ $d_L x = (s(s_1+s_2)-ss_2-ss_1)x = (s(s_1+s_2))x - (ss_2)x - (ss_1)x = s((s_1+s_2)x) - s(s_2x) - s(s_1x) = s(s_1x+s_2x)-s(s_2x)-s(s_1x) \in D_L$; $\overline{d}_L x = (\sum_i (x_i \pm d_L^i - x_i))x = \sum_i (x_i x \pm d_L^i x - x_i x) \in \overline{D}_L$, for all $\overline{d}_L \in \overline{D}_L$ and all $x \in S$.

But $\overline{D}_L$ ($\overline{D}_d$) is by Th.5. also a left (a right) ideal of S.

THEOREM 7. <u>Let E_o be the set of all endomorphisms of a group</u> $(G,+)$, $E(G)$ <u>the set of all maps of the group</u> $(G,+)$ <u>which is additively generated by all elements of</u> E_o ; $\overline{A}$, C, D_d <u>the normal associator subgroup of the near-ring</u> $(E(G)xG,+,x)$, <u>the commutator subgroup of</u> $(G,+)$, <u>the normal right distributor subgroup of</u> $(E(G)xG,+,x)$ <u>respectively, where</u> $+,x$ <u>are point-wise addition in</u> $E(G)xG$ <u>and affine multiplication:</u> $(f,g)x(f_1,g_1) = ((ff_1, fg_1+g)$, $(f,g),(f_1,g_1) \in E(G)xG$. <u>Then,</u> 1. $\{o\}xC$ <u>is an ideal of</u> $E(G)xG$, 2. $\overline{A} = \{o\}xC = D_d$ <u>and</u> 3. $E(G)xG/\{o\}xC$ <u>is a ring.</u>

Proof. 1. For every $(f,g),(f_1,g_1) \in E(G)xG$ and every $\overline{g} \in C$

$((f,g)+(o,\overline{g}))(f_1,g_1)-(f,g)(f_1,g_1) = (f, g+\overline{g})(f_1,g_1)-(f,g)(f_1,g_1) = (o, fg_1+g+\overline{g}-g-fg_1) \in \{o\}x\,C$ and

$(f_1,g_1)((f,g)+(o,\overline{g})) - (f_1,g_1)(f,g) = (f_1,g_1)(f,g+\overline{g})-(f_1f, f_1g+g_1) = (f_1f, f_1(g+\overline{g})+g_1)-(f_1f, f_1g+g_1) = (o, f_1(g+\overline{g})-f_1g) =$ (For any $f_1 \in E(G)$ there exist $f^i \in E_o$; $i=1,\ldots,n$; such that $f_1 = \sum_{i=1}^n \pm f^i$) $= (o, (\sum_i \pm f^i)(g+\overline{g}) - \sum_i \pm f^i g) = (o, \pm f^1(g+\overline{g}) \pm \ldots \pm f^n(g+\overline{g}) \mp f^n g \mp \ldots \mp f^1 g = (o, c \pm f^1 g \pm \ldots \pm f^n g \mp f^n g \mp \ldots \mp f^1 g = (o,c) \in \{o\}xC$ and $\{o\}xC$ is an ideal of $E(G)xG$.

2. The associator of $E(G)xG$ is the set of all elements of the form $((f,g)(f_1,g_1))(f_2,g_2) - (f,g)((f_1,g_1)(f_2,g_2)) = (o, ff_1g_2+fg_1-f(f_1g_2+g_1))$, $(f,g),(f_1,g_1),(f_2,g_2) \in E(G)xG$.

It follows that the normal associator subgroup $\overline{A}$ is contai-

ned in $\{o\}\times C$. Namely $ff_1g_2+fg_1-f(f_1g_2+g_1) = \sum_i \pm f^i f_1 g_2 + \sum_i \pm f^i g_1 - \sum_i \pm f^i(f_1g_2+g_1) \in C$, since the sumands of $-\sum_i \pm f^i(f_1g_2+g_1)$ are of the form $\mp f^i(f_1g_2)$, $\mp f^i g_1$ and we have $x+y-x+z = x-x+y+(-y+x+y-x)+z = y+z+c$ for all $x,y,z \in G$ and some $c \in C$.
Conversely, if we take $f=-e$, $f_1=e$, then from $(o, ff_1g_2+fg_1-f(f_1g_2+g_1)) \in A$ we have $(o,-g_2-g_1+g_2+g_1) \in \overline{A}$. Hence, $\{o\}\times C \subseteq \overline{A}$.
So, $\overline{A} = \{o\}\times C$.

Further, for every $(f,g),(f_1,g_1),(f_2,g_2) \in E(G)\times G$ the right distributor: $((f_1,g_1)+(f_2,g_2))(f,g)-(f_2,g_2)(f,g)-(f_1,g_1)(f,g) = (o,f_1g+f_2g+g_1-f_2g-g_1-f_1g) \in \{o\}\times C$ ....(++) and follows $D_d \subseteq \{o\}\times C$. If put that $f_2=e$ (identity of $E(G)$) and $f_1=o$ in (++) then $(o,g+g_1-g-g_1) \in D_d$. Thus, $D_d = \overline{A}$.

3. The proof is straightfarward and we omit it.

A near-ring $(S,+,\cdot)$ is said to be solvable if and only if $(S,+)$ has a solvable sequence of S-subgroups.

A right S-subgroup P of $(S,+)$ is said to be a right small S-subgroup if and only if S=B for each other right S-subgroup B of S such that S=P+B.

THEOREM 8. <u>Let S be a left unitary near-ring with the distributor ideal D and the associator ideal A which are small right ideals and $(S,+,\cdot)$ is solvable. Then, the radical J(S) of S coincides with the quasiradical Q(S) and S/J(S) is a ring. If J(S) is a small right S-subgroup, then it coincides with the radical subgroup N(S) also.</u>

<u>Proof</u>. Since A and D are small right ideals of S they are contained in every maximal right ideal M of S. Hence, for every maximal right ideal M the near-ring S/M is an associative and distributive near-ring. We prove that S/M is a ring and that M is a modu-

lar ideal of S .
Since (S,+,·) is solvable then there exists a solvable series
of S-subgroups: $S=S_o \; S_1 \; \dots \; S_n = o$. If M is a maximal
right ideal then S M o is a normal series of S-subgroups
since o·s(D M, for each s(S, and hence M is a S-subgroup .
Namely, os=(o+o)s=os+os+d , i.e. os=d(D, for each s(S and for
some d(D. Now, ms=((o+m)s-os)+os (M for all m(M and s(S. This
have equivalent refinements which are solvable (see (1.3 3).
If (S/M,+) isn't commutative then there exists a solvable se-
ries of S-subgroups: S K ... M ... o . Since K M A(S) ,
K M D and K is a normal S-subgroup then K is right ideal.
This is a contradiction. Hence, (S/M,+) is a commutative group
and S/M is a ring. From this fact it falows that M is a modu-
lar right ideal. Hence, J(S) = Q(S). But S/J(S) = S/ M is a
subdirect sum of the rings S/M (M runing over all maximal
ideals). Hence S/J(S) is also a ring.
Since N(S) is the intersection of all maximal right S-subgroups,
and J(S) is contained in every such S-subgroup we have also J(S)=
=N(S). Namely, S/J(S) is a ring, and every S-subgroup G of S
containing J(S) is a right ideal of S.

R E F R E N C E S

1. V. Vuković : (Nonassociative) Near-Ring , to appear .
2. " : Prstenoidne strukture, doktorska disertacija, Univerzitet u Prištini, 1984.
3. J. C. Beidleman: Distributively Generated Near-Ring with Descending Chain Condition, Math. Z. 91, 65-69 (1966).

Vojvode Mišića 54
18000 Niš
Yugoslavia