MATEMATICKO-FYZIKÁLNY ČASOPIS
ROČNÍK IV ČÍSLO 4

O ROZKLADE JEDNODUCHÝCH POLOGRÚP NA DIREKTNÝ SÚČIN

JÁN IVAN, Bratislava

ÚVOD

Predložená práca nadväzuje na autorovu prácu [1], ktorej obsahom je vyšetrovanie vlastností direktného súčinu pologrúp, najmä jednoduchých. Cieľom tejto práce je nájsť nevyhnutné a postačujúce podmienky k tomu, aby sa konečná jednoduchá pologrupa bez nuly dala rozložiť na direktný súčin iných pologrúp.

Úvodom si pripomenieme základné definície a vety z teórie pologrúp. Podrobnejšie poučenie o tom čitateľ nájde napr. v práci Schwarz [1].

Pologrupou nazývame každú neprázdnu množinu S elementov $a, b, c, \ldots$, ktorá je uzavretá vzhľadom na nejakú jednoznačnú asociatívnu operáciu (násobenie): $(ab)\,c = a(bc)$.

Každú neprázdnu podmnožinu S_1 pologrupy S, ktorá pri tej istej definícii násobenia tvorí pologrupu, nazývame *čiastočnou pologrupou* pologrupy S.

Neprázdnu podmnožinu L pologrupy S nazývame *ľavým ideálom* pologrupy S, ak je splnený vzťah $SL \subseteq L$, t. j. pre každé $s \in S$, $l \in L$ platí $sl \in L$. *Pravým ideálom* nazývame neprázdnu podmnožinu R, ktorá spĺňuje podmienku $RS \subseteq R$. *Obojstranným ideálom* nazývame podmnožinu M, ktorá je súčasne ľavým aj pravým ideálom pologrupy S, t. j. spĺňuje podmienky $SM \subseteq M$, $MS \subseteq M$.

Každý ľavý (pravý, obojstranný) ideál pologrupy S je jej čiastočnou pologrupou.

Prenik (ak je neprázdny) a súčet dvoch ľavých (pravých, obojstranných) ideálov je ľavý (pravý, obojstranný) ideál.

Ľavý (pravý, obojstranný) ideál pologrupy S nazývame *minimálnym ideálom* pologrupy S, ak už neobsahuje v sebe ako vlastnú podmnožinu žiadny iný ľavý (pravý, obojstranný) ideál pologrupy S.

Pologrupa nemusí obsahovať minimálne ideály.

Prenik dvoch rôznych minimálnych ľavých (pravých) ideálov je prázdna množina.

Pologrupa S môže mať najviac jeden minimálny obojstranný ideál N. Tento je potom podmnožinou každého obojstranného ideálu z S a dá sa teda definovať ako prenik všetkých obojstranných ideálov z S (tzv. *Suškevičovo jadro*).

Pologrupa S môže (ale nemusí) obsahovať element z tej vlastnosti, že pre každé $a \in S$ je $za = az = z$. Takýto element nazývame *nulou* pologrupy.

Pologrupa môže obsahovať najviac jednu nulu.

Nula (ak existuje) je pri uvedenej definícii minimality zrejme jediným existujúcim minimálnym ľavým (pravým, obojstranným) ideálom. V tomto prípade je preto výhodné minimálny ideál definovať ako ideál, ktorý okrem nuly (nulového ideálu) neobsahuje už žiadny iný podideál rovnakého druhu. Potom platí:

Prenik dvoch rôznych minimálnych ľavých (pravých) ideálov je nulový ideál.

Pologrupa môže mať viac (aj nekonečne mnoho) minimálnych obojstranných ideálov.

My sa tu budeme zaoberať iba pologrupami bez nuly, takže nebude záležať na tom, ktorú definíciu minimality použijeme.

Pologrupa môže (ale nemusí) obsahovať *idempotentný element* (krátko *idempotent*), t. j. taký element e, pre ktorý platí $e^2 = e$.

Každá konečná pologrupa obsahuje aspoň jeden idempotent.

Pologrupa S môže mať najviac jeden *jednotkový element (jednotku)*, t. j. taký element $e \in S$, ktorý pre každé $a \in S$ splňuje vzťah $ea = ae = a$.

Pologrupa S môže mať aj viac (aj nekonečne mnoho) *ľavých jednotiek*, t. j. elementov $e_l \in S$, ktoré pre každé $a \in S$ splňujú vzťah $e_l a = a$. Podobne môže existovať viac (aj nekonečne mnoho) *pravých jednotiek*, t. j. elementov $e_r \in S$, ktoré pre každé $a \in S$ splňujú vzťah $ae_r = a$.

Každý idempotent minimálneho ľavého (pravého) ideálu je jeho pravou (ľavou) jednotkou.

Poznámka o označovaní: Symbol $S_1 \subset S$ značí (na rozdiel od $S_1 \subseteq S$), že S_1 je *vlastnou* podmnožinou množiny S. Súčet dvoch množín S_1, S_2 budeme značiť $\{S_1, S_2\}$ alebo $S_1 + S_2$. Rovnaký význam má symbol $\sum_i S_i$. Ostatné označenia majú obvyklý význam.

1. ŠTRUKTÚRA KONEČNÝCH JEDNODUCHÝCH POLOGRÚP BEZ NULY

Keďže sa v ďalšom budeme zaoberať špeciálnejšími otázkami, ktoré sa týkajú jednoduchých pologrúp bez nuly, musíme si najprv trochu podrobnejšie vyložiť štruktúru takýchto pologrúp. To bude obsahom tohto odseku. Niektoré výsledky tohto odseku sú známe (pozri napr. Suschkewitsch [1], Schwarz [2]). Podáme ich však vo forme pre naše účely obzvlášť výhodnej.

Definícia 1,1. *Pologrupu S nazývame jednoduchou, ak neobsahuje žiadny obojstranný ideál rôzny od S a nulového ideálu (ak S má nulu).*

Špeciálne prípady jednoduchých pologrúp sú tzv. zľava a sprava jednoduché pologrupy.

Definícia 1,2. *Pologrupu S nazývame zľava (sprava) jednoduchou, ak neobsahuje žiadny ľavý (pravý) ideál rôzny od S a nulového ideálu (ak S má nulu).*

Veta 1,1. *Pologrupa S bez nuly je zľava (sprava) jednoduchá vtedy a len vtedy, ak v nej rovnica $xa = b$ $(ax = b)$ má riešenie pre každé $a, b \in S$.*

Dôkaz. Pozri napr. Ivan [1], veta 1 a 1a.

Z axiomatiky teórie grúp a z vety 1,1 vyplýva, že *zľava a zároveň sprava jednoduchá pologrupa bez nuly je grupou.*

Veta 1,2. *Nech S je pologrupa bez nuly, L jej minimálny ľavý a R minimálny pravý ideál. Potom L je zľava a R sprava jednoduchá pologrupa bez nuly.*

Dôkaz. Pozri napr. Schwarz [3], veta 3,5.

Veta 1,3. *Jednoduchá pologrupa S bez nuly, ktorá obsahuje aspoň jeden minimálny ľavý (pravý) ideál, je súčtom minimálnych ľavých (pravých) ideálov.*

Dôkaz. Pozri napr. Schwarz [2], veta 2,1.

Poznámka. Odteraz sa budeme zaoberať už iba konečnými pologrupami bez nuly.

Veta 1,4. *Nech S je konečná pologrupa bez nuly, nech L_i je jej ľubovoľný minimálny ľavý a R_k minimálny pravý ideál. Potom:*

1. *$L_i \cap R_k = G_{ik}$ je grupa,*
2. *G_{ik} je minimálnym pravým ideálom v L_i a minimálnym ľavým ideálom v R_k,*
3. *grupa G_{ik} sa dá vyjadriť aj takto:*

$$G_{ik} = e_{ik} L_i = R_k e_{ik},$$

kde e_{ik} je jednotka grupy G_{ik}.

Dôkaz. 1. Dokážeme najprv, že $G_{ik} = L_i \cap R_k$ je neprázdna množina. Uvažujme súčin $R_k L_i$. Ten je iste neprázdny. Pritom je:

$$R_k L_i \subseteq L_i, \quad R_k L_i \subseteq R_k,$$

to však znamená, že:

$$R_k L_i \subseteq L_i \cap R_k,$$

teda množina $G_{ik} = L_i \cap R_k$ je neprázdna.

Ukážeme teraz, že neprázdna množina $G_{ik} \subseteq S$ je čiastočnou pologrupou pologrupy S. K tomu stačí dokázať, že súčin ľubovoľných dvoch elementov z G_{ik} je opäť element z G_{ik}.

Nech a, b sú ľubovoľné elementy z G_{ik}, t. j.

$$a \in L_i, \ a \in R_k; \ b \in L_i, \ b \in R_k.$$

Pretože L_i, R_k sú pologrupy, platí:

$$ab \in L_i, \ ab \in R_k,$$

teda:

$$ab \in L_i \cap R_k = G_{ik}.$$

Keďže G_{ik} je konečná pologrupa, obsahuje aspoň jeden idempotent. Označme ho e_{ik}. Idempotent e_{ik} patrí do minimálneho ľavého ideálu L_i, teda je pravou jednotkou pre každý element z L_i, teda aj pre každý element z G_{ik}. Ale idempotent e_{ik} patrí zároveň do minimálneho pravého ideálu R_k, teda je zároveň ľavou jednotkou pre každý element z R_k, teda aj pre každý element z G_{ik}. To znamená, že idempotent e_{ik} je jednotkou pologrupy G_{ik}. Iný idempotent už G_{ik} nemôže obsahovať, pretože ten by bol z tých istých dôvodov jednotkou v G_{ik} a pologrupa, ako bolo v úvode konštatované, môže obsahovať najviac jednu jednotku.

Podľa vety 1,2 ideál L_i je zľava a ideál R_k sprava jednoduchá pologrupa bez nuly. To na základe vety 1,1 znamená, že rovnica $xa = b$ má riešenie $x \in L_i$ pre každé $a, b \in L_i$ a rovnica $ay = b$ má riešenie $y \in R_k$ pre každé $a, b \in R_k$. Špeciálne rovnica

$$xa = e_{ik} \tag{1}$$

má riešenie $x \in L_i$ a rovnica

$$ay = e_{ik} \tag{2}$$

má riešenie $y \in R_k$ pre každé $a \in G_{ik}$. Násobme rovnicu (1) elementom y sprava:

$$xay = e_{ik}y,$$

z čoho dostaneme

$$xe_{ik} = e_{ik}y,$$
$$x = y.$$

To znamená, že rovnica (1) má riešenie $x \in G_{ik}$ pre každé $a \in G_{ik}$. Ináč povedané: ku každému elementu $a \in G_{ik}$ existuje (ľavý) inverzný element. Z axiomatiky teórie grúp vyplýva, že množina G_{ik} je grupou, č. b. t. d.

2. Pretože $G_{ik} = L_i \cap R_k$, je $G_{ik} \subseteq L_i$, $G_{ik} \subseteq R_k$. Na základe toho je:

$$G_{ik}L_i \subseteq L_iL_i \subseteq L_i, \quad G_{ik}L_i \subseteq R_kL_i \subseteq R_k,$$

t. j.

$$G_{ik}L_i \subseteq L_i \cap R_k = G_{ik},$$

teda G_{ik} je pravým ideálom pologrupy L_i. Je to zrejme minimálny ideál v L_i, pretože grupa, ako je známe, nemôže obsahovať vlastný ideál.

Práve tak sa dokáže, že G_{ik} je minimálnym ľavým ideálom v R_k.

3. Pretože je $R_kL_i \subseteq G_{ik}$, pre každé $a \in G_{ik}$ platí:

$$aL_i \subseteq G_{ik}, \quad R_ka \subseteq G_{ik}.$$

Množina $aL_i \subseteq L_i$ je zrejme pravým ideálom v L_i a množina $R_ka \subseteq R_k$ ľavým ideálom v R_k. Pretože však G_{ik} je minimálnym pravým ideálom v L_i a minimálnym ľavým ideálom v R_k, platí:

$$G_{ik} = aL_i = R_ka$$

pre každé $a \in G_{ik}$, teda aj pre e_{ik}, t. j. $G_{ik} = e_{ik}L_i = R_ke_{ik}$, č. b. t. d.

Teraz už ľahko dokážeme ďalšiu vetu o štruktúre konečných jednoduchých pologrúp bez nuly.

Veta 1,5. *Konečná jednoduchá pologrupa bez nuly má takúto štruktúru:*

$$S = \sum_{i=1}^{s} L_i = \sum_{k=1}^{t} R_k = \sum_{i=1}^{s}\sum_{k=1}^{t} G_{ik}, \quad L_i = \sum_{k=1}^{t} G_{ik}, \quad R_k = \sum_{i=1}^{s} G_{ik},$$

kde L_i sú jej minimálne ľavé, R_k minimálne pravé ideály, $G_{ik} = L_i \cap R_k$ sú navzájom izomorfné disjunktné grupy a prirodzené čísla s, t majú zrejmý význam.

Dôkaz. Podľa vety 1,3 je $S = \sum_{i=1}^{s} L_i = \sum_{k=1}^{t} R_k$, kde L_i, R_k sú minimálne ľavé, resp. pravé ideály v S. Všetky L_i sú disjunktné, práve tak aj všetky R_k. Teda aj všetky grupy $G_{ik} = L_i \cap R_k$ sú navzájom disjunktné. Z toho ďalej vyplýva, že každý element $a \in S$ padne do niektorého minimálneho ľavého ideálu L_i a do niektorého minimálneho pravého ideálu R_k, teda padne do niektorej grupy G_{ik}. Tým je dokázané, že pologrupa S je súčtom st disjunktných grúp: $S = \sum_{i=1}^{s}\sum_{k=1}^{t} G_{ik}$. Treba ešte dokázať, že všetky tieto grupy sú navzájom izomorfné.

Podľa práve dokázaného je $L_i = \sum_{k=1}^{t} G_{ik}$, $R_k = \sum_{i=1}^{s} G_{ik}$. Podľa vety 1,4 je $G_{ik} = e_{ik}L_i = R_ke_{ik}$. Teda je:

$$G_{ik} = e_{ik}L_i = e_{ik}(G_{i1} + G_{i2} + \ldots + G_{ik} + \ldots + G_{it}) =$$
$$= e_{ik}G_{i1} + e_{ik}G_{i2} + \ldots + G_{ik} + \ldots + e_{ik}G_{it},$$

z čoho vyplýva:

$$e_{ik}G_{i1} \subseteq G_{ik}.$$

Podľa vety 1,4 grupy G_{i1}, G_{ik} sú minimálne pravé ideály v L_i. Množina $e_{ik}G_{i1} \subseteq L_i$ je zrejme pravým ideálom v L_i, pretože $e_{ik}G_{i1}L_i \subseteq e_{ik}G_{i1}$. Pretože však G_{ik} je minimálny pravý ideál v L_i, musí platiť:

$$G_{ik} = e_{ik}G_{i1}. \tag{3}$$

Avšak

$$G_{i1} = R_1e_{i1} = (G_{11} + G_{21} + \ldots + G_{i1} + \ldots + G_{s1})\, e_{i1} =$$
$$= G_{11}e_{i1} + G_{21}e_{i1} + \ldots + G_{i1} + \ldots + G_{s1}e_{i1},$$

z čoho vyplýva:

$$G_{11}\, e_{i1} \subseteq G_{i1}.$$

Podľa vety 1,4 grupy G_{11}, G_{i1} sú minimálne ľavé ideály v R_1. Množina $G_{11}\, e_{i1} \subseteq R_1$ je zrejme tiež ľavým ideálom v R_1. Pretože však G_{i1} je minimálny ľavý ideál v R_1, musí platiť:

$$G_{i1} = G_{11}\, e_{i1}. \tag{4}$$

Z (3) a (4) vyplýva:

$$G_{ik} = e_{ik}\, G_{11}\, e_{i1}. \tag{5}$$

To znamená, že prvky ľubovoľnej grupy G_{ik} môžeme vyjadriť pomocou prvkov grupy G_{11} a jednotiek grúp G_{ik}, G_{i1}.

Prvky grupy G_{11} označme e_{11}, a_{11}, b_{11}, c_{11}, ..., kde e_{11} je jednotka. Ak x_{11}

prebieha všetky elementy z G_{11}, potom podľa (5) $e_{ik} x_{11} e_{i1}$ prebieha všetky elementy grupy G_{ik}. Ak $x_{11} = e_{11}$, potom

$$e_{ik} e_{11} e_{i1} = e_{ik} (e_{11} e_{i1}) = e_{ik} e_{i1} = e_{ik} .$$

To nás nabáda k tomu, aby sme aj ostatné elementy $e_{ik} x_{11} e_{i1} \in G_{ik}$ označili x_{ik}. Teda položme:

$$x_{ik} = e_{ik} x_{11} e_{i1} \tag{6}$$

pre každé $x_{11} \in G_{11}$. Takto dostaneme všetky elementy grupy G_{ik} : e_{ik}, a_{ik}, b_{ik}, c_{ik}, ... Je ich zrejme práve toľko ako elementov grupy G_{11} [na základe vzťahu (5)].

Teraz uvažujme také zobrazenie grupy G_{11} na grupu G_{ik}, ktoré každému elementu $x_{11} \in G_{11}$ priradí element $x_{ik} = e_{ik} x_{11} e_{ik} \in G_{ik}$:

$$x_{11} \to x_{ik} . \tag{7}$$

Toto zobrazenie je v dôsledku vzťahu (5) zrejme vzájomne jednoznačné. Ukážeme, že je to izomorfizmus.

Nech a_{11}, b_{11} sú ľubovoľné elementy grupy G_{11} a nech $a_{11} b_{11} = c_{11}$. V zobrazení (7) im zodpovedajú elementy a_{ik}, b_{ik}, c_{ik}:

$$a_{11} \to a_{ik}, \quad b_{11} \to b_{ik}, \quad c_{11} \to c_{ik} .$$

Treba dokázať, že $a_{ik} b_{ik} = c_{ik}$. Skutočne je:

$$a_{ik} b_{ik} = e_{ik} a_{11} e_{i1} \cdot e_{ik} b_{11} e_{i1} = e_{ik} a_{11} (e_{i1} e_{ik}) b_{11} e_{i1} =$$
$$= e_{ik} a_{11} e_{11} b_{11} e_{i1} = e_{ik} a_{11} (e_{11} b_{11}) e_{i1} = e_{ik} a_{11} b_{11} e_{i1} =$$
$$= e_{ik} (a_{11} b_{11}) e_{i1} = e_{ik} c_{11} e_{i1} = c_{ik} .$$

Tým sme dokázali, že grupa G_{11} je pri zobrazení (7) izomorfná s ľubovoľnou grupou G_{ik}:

$$G_{11} \cong G_{ik} .$$

Pretože však vzťah $\cong$ je reflexívny, symetrický a tranzitívny, tým je dokázané, že všetky grupy G_{ik} sú navzájom izomorfné.

Dôsledok vety 1,5. *Každý minimálny ľavý (pravý) ideál konečnej jednoduchej pologrupy S bez nuly má práve toľko idempotentov, koľko je minimálnych pravých (ľavých) ideálov v S.*

Poznámka 1. V dôkaze vety 1,5 význačnú úlohu mala grupa G_{11}. To však zrejme nie je podstatné. Miesto grupy G_{11} sme mohli hociktorú inú z grúp G_{ik} zvoliť za „prvú". Zmenilo by sa tým iba označenie.

Poznámka 2. Okrem izomorfizmu (7), uvažovaného v dôkaze vety 1,5, môžu zrejme existovať aj iné izomorfizmy. Napr. podobne ako vzťah (5) dá sa dokázať aj vzťah $G_{ik} = e_{1k} G_{11} e_{ik}$, ktorý vedie vo všeobecnosti na iný izomorfizmus.

Definícia 1,3. *Navzájom izomorfné disjunktné grupy G_{ik}, ktorých súčtom je jednoduchá pologrupa S bez nuly, budeme nazývať grupovými komponentmi pologrupy S. Grupovým komponentom budeme nazývať aj abstraktnú grupu $G \cong G_{ik}$.*

Pre grupové komponenty platí:

Veta 1,6. $G_{ik} G_{jl} = G_{jk}$.

Dôkaz. Pretože $G_{ik} = L_i \cap R_k$, $G_{jl} = L_j \cap R_l$, je $G_{ik} \subseteq L_i$, $G_{ik} \subseteq R_k$, $G_{jl} \subseteq L_j$, $G_{jl} \subseteq R_l$.

Na základe toho je: $\quad G_{ik} G_{jl} \subseteq L_i L_j \subseteq L_j$,

pretože L_j je ľavý ideál v S. Zároveň je:

$$G_{ik} G_{jl} \subseteq R_k R_l \subseteq R_k ,$$

pretože R_k je pravý ideál v S. Teda:

$$G_{ik} G_{jl} \subseteq L_j \cap R_k = G_{jk} .$$

Pretože G_{jl} je pravý ideál v L_j, je:

$$G_{ik} G_{jl} L_j \subseteq G_{ik} G_{jl} ,$$

t. j. $G_{ik} G_{jl} \subseteq L_j$ je pravý ideál v L_j. Pretože však G_{jk} je minimálny pravý ideál v L_j, musí platiť:

$$G_{ik} G_{jl} = G_{jk} .$$

Práve tak sa dokáže:

Veta 1,6a. *Nech x_{ik}, x_{jl} sú ľubovoľné elementy z G_{ik}, resp. G_{jl}, potom platí:*

$$x_{ik} G_{jl} = G_{jk} , \quad G_{ik} x_{jl} = G_{jk} .$$

Podľa vety 1,6 vždy platí:

$$G_{ik} G_{jl} = G_{jk} .$$

Vzniká otázka, či aj pre idempotenty (jednotky grúp) vždy platí:

$$e_{ik} e_{jl} = e_{jk} ,$$

t. j., či súčin ľubovoľných dvoch idempotentov je vždy idempotent.

Na základe vety 1,6 môžeme tvrdiť iba to, že:

$$e_{ik} e_{jl} \in G_{jk} .$$

Pre $j = i$ alebo $l = k$ to však vždy platí na základe toho, že každý idempotent minimálneho ľavého (pravého) ideálu je jeho pravou (ľavou) jednotkou. Teda vždy platí:

$$e_{ik} e_{il} = e_{ik} .$$
$$e_{ik} e_{jk} = e_{jk} . \tag{8}$$

Avšak vo všeobecnosti je $e_{ik} e_{jl} \neq e_{jk}$, o čom sa presvedčíme na nasledujúcom príklade.

Príklad. Pologrupa $S = \{a_1, a_2, a_3, a_4, a_5, a_6, a_7, a_8\}$, v ktorej násobenie je definované touto multiplikačnou tabuľkou:

	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
a_1	a_1	a_2	a_1	a_2	a_5	a_6	a_6	a_5
a_2	a_2	a_1	a_2	a_1	a_6	a_5	a_5	a_6
a_3	a_3	a_4	a_3	a_4	a_8	a_7	a_7	a_8
a_4	a_4	a_3	a_4	a_3	a_7	a_8	a_8	a_7
a_5	a_1	a_2	a_2	a_1	a_5	a_6	a_5	a_6
a_6	a_2	a_1	a_1	a_2	a_6	a_5	a_6	a_5
a_7	a_4	a_3	a_3	a_4	a_7	a_8	a_7	a_8
a_8	a_3	a_4	a_4	a_3	a_8	a_7	a_8	a_7

je jednoduchá bez nuly (priamo sa môžeme presvedčiť, že asociatívny zákon je splnený). Jej minimálne ľavé ideály sú:

$$L_1 = \{a_1, a_2, a_3, a_4\}, \; L_2 = \{a_5, a_6, a_7, a_8\}$$

a minimálne pravé ideály:

$$R_1 = \{a_1, a_2, a_5, a_6\}, \; R_2 = \{a_3, a_4, a_7, a_8\}.$$

Vidíme, že $S = L_1 + L_2 = R_1 + R_2$. Podľa vety 1,5 pologrupa S je súčtom štyroch navzájom izomorfných disjunktných grúp. Sú to:

$$G_{11} = L_1 \cap R_1 = \{a_1, a_2\}, \; G_{12} = L_1 \cap R_2 = \{a_3, a_4\},$$
$$G_{21} = L_2 \cap R_1 = \{a_5, a_6\}, \; G_{22} = L_2 \cap R_2 = \{a_7, a_8\}.$$

V našom označení teda je:

$$e_{11} = a_1 \quad e_{12} = a_3 \quad e_{21} = a_5 \quad e_{22} = a_7$$
$$a_{11} = a_2 \quad a_{12} = a_4 \quad a_{21} = a_6 \quad a_{22} = a_8$$

Platí:

$$e_{11}\, e_{12} = a_1\, a_3 = a_1 = e_{11}, \; e_{11}\, e_{21} = a_1\, a_5 = a_5 = e_{21},$$

avšak

$$e_{12}\, e_{21} = a_3\, a_5 = a_8 = a_{22}.$$

Vidíme teda, že súčin dvoch idempotentov nemusí byť vždy idempotent.

Všetky konečné jednoduché pologrupy bez nuly môžeme teraz rozdeliť do dvoch skupín podľa toho, či splňujú alebo nesplňujú podmienku:

$$e_{ik}\, e_{jl} = e_{jk} \tag{9}$$

pre každé i, j, k, l.

Definícia 1,4. *Konečné jednoduché pologrupy bez nuly, ktoré splňujú podmienku (9), budeme nazývať jednoduchými pologrupami typu A; v opačnom prípade budeme hovoriť o pologrupách typu B.*

Z tejto definície a z (8) ihneď vyplýva:

Veta 1,7. *Každá konečná, zľava (sprava) jednoduchá pologrupa bez nuly je typu A.*

Dôsledok vety 1,7. *Každá jednoduchá pologrupa typu B obsahuje aspoň dva minimálne ľavé a aspoň dva minimálne pravé ideály.*

Dohovor. V ďalšom budeme prívlastok „konečná“ vynechávať. Pologrupa S bude však znamenať vždy konečnú pologrupu, ak nebude zvlášť ináč poznamenané.

Veta 1,8. *Nech S je jednoduchá pologrupa bez nuly a nech jej elementy sú označené podľa (6). Potom vzťah*

$$a_{ik}\, b_{jl} = a_{jk}\, b_{jk} \tag{10}$$

platí pre každé $a_{ik}, b_{jl} \in S$ vtedy a len vtedy, ak S je typu A.

Dôkaz. Nech pologrupa S je typu A, t. j. platí $e_{ik}\, e_{jl} = e_{jk}$ pre každé i, j, k, l. Nech a_{ik}, b_{jl} sú ľubovoľné elementy z S, $a_{ik} = e_{ik}\, a_{11}\, e_{i1}$, $b_{jl} = e_{jl}\, b_{11}\, e_{j1}$, potom

$$a_{ik}\, b_{jl} = e_{ik}\, a_{11}\, e_{i1}\, e_{jl}\, b_{11}\, e_{j1} = e_{ik}\, a_{11}\, (e_{i1}\, e_{jl})\, b_{11}\, e_{j1} =$$
$$= e_{ik}\, a_{11}\, e_{j1}\, b_{11}\, e_{j1} = e_{ik}\, a_{11}\, (e_{j1}\, b_{11})\, e_{j1} = e_{ik}\, a_{11}\, b_{11}\, e_{j1} =$$
$$= e_{ik}\, (e_{j1}\, a_{11})\, b_{11}\, e_{j1} = (e_{ik}\, e_{j1})\, (a_{11}\, b_{11})\, e_{j1} = e_{jk}\, c_{11}\, e_{j1} = c_{jk}.$$

Ak $a_{11}\, b_{11} = c_{11}$, potom $a_{jk}\, b_{jk} = c_{jk}$. Teda:

$$a_{ik}\, b_{jl} = c_{jk} = a_{jk}\, b_{jk}.$$

Nech naopak pre ľubovoľné elementy z S platí $a_{ik}\, b_{jl} = a_{jk}\, b_{jk}$. Potom to platí špeciálne aj pre e_{ik}, e_{jl}, t. j. $e_{ik}\, e_{jl} = e_{jk}\, e_{jk} = e_{jk}$. To však znamená, že pologrupa S je typu A.

Poznámka. Ľahko sa môžeme presvedčiť, že elementy ľubovoľného ľavého ideálu L_i jednoduchej pologrupy S bez nuly splňujú (10), t. j. platí $a_{ik}\, b_{jl} = a_{jk}\, b_{jk}$ bez ohľadu na to, či pôvodná pologrupa S je typu A alebo B. Práve tak aj elementy minimálneho pravého ideálu R_1 : $a_{i1}\, b_{j1} = a_{j1}\, b_{j1}$. To je v súhlase s vetou 1,8, pretože každý minimálny ľavý (pravý) ideál je zľava (sprava) jednoduchá pologrupa, teda typu A.

Ak však vezmeme ideál R_k, $k \neq 1$ a S je typu B, potom nemusí byť splnené (10), ak elementy pologrupy R_k berieme s tým istým označením, ktoré dostali v pôvodnej pologrupe S. To zdanlivo odporuje vete 1,8. Rozpor vzniká práve z označenia elementov. Totiž pri „starom“ označení je:

$$a_{ik}\, b_{jk} = e_{ik}\, a_{11}\, e_{i1} \cdot e_{jk}\, b_{11}\, e_{j1}.$$

Máme tu do činenia s idempotentmi e_{i1}, e_{j1}, ktoré nepatria do $R_k (k \neq 1)$, teda nie je zaručené, že platí $e_{i1}\, e_{jk} = e_{j1}$. Z tohto dôvodu nemusí byť $a_{ik}\, b_{jk} = a_{jk}\, b_{jk}$.

Ak sa však na ideál R_k dívame ako na *samostatnú pologrupu* a v nej označíme elementy podľa (6), potom vzťah (10) je prirodzene splnený.

V prípade ideálov R_1 a L_i toto „staré“ označenie nevedie k rozporu s vetou 1,8, pretože vo výrazoch:

$$a_{i1}\, b_{j1} = e_{i1}\, a_{11}\, e_{i1}\, e_{j1}\, b_{11}\, e_{j1}, \qquad a_{ik}\, b_{il} = e_{ik}\, a_{11}\, e_{i1}\, e_{il}\, b_{11}\, e_{i1}.$$

všetky idempotenty patria do R_1, resp. do L_i.

Jednoduché pologrupy typu A majú niektoré „dobré" vlastnosti, ktoré pologrupy typu B nemajú. O najdôležitejšej z nich hovorí veta 1,8. V dôsledku týchto vlastností sa pologrupy typu A, ako uvidíme neskôr, dajú omnoho ľahšie rozložiť na direktný súčin ako pologrupy typu B.

Množinu všetkých idempotentov jednoduchej pologrupy S bez nuly označme E. Je zrejmé, že množina E tvorí čiastočnú pologrupu pologrupy S vtedy a len vtedy, ak S je typu A. Dokážeme, že v tom prípade pologrupa E je tiež jednoduchá bez nuly a obsahuje práve toľko minimálnych ideálov ako S. Najprv si však dokážeme jednu pomocnú vetu.

Lemma 1,1. *Nech pologrupa S', ktorá obsahuje aspoň dva elementy, je homomorfným obrazom jednoduchej pologrupy S bez nuly. Potom S' je nevyhnutne jednoduchá pologrupa bez nuly.*

Dôkaz. Nech $S \sim S'$ a nech S je jednoduchá pologrupa bez nuly. Predpokladajme, že pologrupa S' nie je jednoduchá, t. j. obsahuje vlastný obojstranný ideál $M' \subset S'$. Pre ľubovoľné $s' \in S'$, $m' \in M'$ teda platí:

$$s'm' \in M', \quad m's' \in M'.$$

Množinu tých prvkov z S, ktoré sa pri danom homomorfizme zobrazia na prvky ideálu M', označme M. Množina M je zrejme neprázdna a iste je $M \neq S$. Pre ľubovoľné $m \in M$, $s \in S$ potom platí:

$$m \to m' \in M', \quad s \to s' \in S',$$
$$ms \to m's' \in M', \quad sm \to s'm' \in M',$$

z čoho vyplýva, že

$$ms \in M, \quad sm \in M.$$

To však znamená, že neprázdna množina $M \subset S$ je obojstranným ideálom pologrupy S, čo odporuje predpokladu o jej jednoduchosti.

Treba ešte dokázať, že S' je pologrupa bez nuly. Dokážeme to opäť nepriamo. Nech pologrupa S' obsahuje nulu z'. Množinu tých elementov z S, ktoré sa pri danom homomorfizme zobrazia na z', označme Z. Množina Z je opäť zrejme neprázdna a $\neq S$. Pre ľubovoľné $z \in Z$, $s \in S$ platí:

$$z \to z', \quad s \to s',$$
$$sz \to s'z' = z', \quad zs \to z's' = z',$$

t. j.

$$sz \in Z, \quad zs \in Z.$$

To znamená, že neprázdna podmnožina $Z \subset S$ je obojstranným ideálom pologrupy S, čo je spor. Teda S' je jednoduchá pologrupa bez nuly.

Veta 1,9. *Nech S je jednoduchá pologrupa typu A, ktorá nie je grupou. Nech E je množina všetkých jej idempotentov. Potom:*

1. *Množina E je čiastočnou pologrupou pologrupy S.*
2. *Platí $S \sim E$.*
3. *Pologrupa E je jednoduchá bez nuly. Jej minimálne ľavé, resp. pravé ideály sú:*

$$L_i^{(e)} = L_i \cap E, \quad R_k^{(e)} = R_k \cap E,$$

teda je ich práve toľko ako minimálnych ľavých ideálov L_i, resp. pravých R_k v S.

Dôkaz. 1. Že množina E je čiastočnou pologrupou pologrupy S, vyplýva ihneď z predpokladu, že S je typu A, pretože v tom prípade súčin ľubovoľných dvoch idempotentov je idempotent.

2. Zobrazme pologrupu S na pologrupu E takto: všetkým tým elementom z S, ktoré patria do tej istej grupy G_{ik}, priradíme element $e_{ik} \in E$, t. j.

$$x_{ik} \to e_{ik},$$

ak $x_{ik} \in G_{ik}$. Toto zobrazenie je zrejme jednoznačné a v dôsledku vety 1,6 aj homomorfné. Teda je $S \sim E$.

3. Podľa predpokladu S nie je grupou, teda E obsahuje viac ako jeden element. Podľa práve dokázaného a podľa lemmy 1,1 E je teda jednoduchá pologrupa bez nuly.

Označme $L_i \cap E = L_i^{(e)}$. Potom platí:

$$EL_i^{(e)} \subseteq EL_i \subseteq L_i$$

a zároveň

$$EL_i^{(e)} \subseteq EE \subseteq E,$$

teda

$$EL_i^{(e)} \subseteq L_i \cap E = L_i^{(e)}.$$

To znamená, že $L_i^{(e)} = L_i \cap E = \{e_{i1}, e_{i2}, \ldots, e_{it}\}$ je ľavý ideál v E. Ďalej pre ľubovoľné $e_{ik} \in L_i^{(e)}$ platí:

$$L_i^{(e)} e_{ik} = \{e_{i1}, e_{i2}, \ldots, e_{it}\} e_{ik} = \{e_{i1}, e_{i2}, \ldots, e_{it}\} = L_i^{(e)}.$$

To však znamená, že v ideáli $L_i^{(e)}$ má rovnica $xa = b$ riešenie pre každé $a, b \in L_i^{(e)}$. Podľa vety 1,1 ideál $L_i^{(e)}$ je minimálny. Takých ideálov $L_i^{(e)}$ je v E zrejme toľko, koľko je minimálnych ľavých ideálov L_i v S. Ich súčet je rovný celému E, teda sú to všetky minimálne ľavé ideály v E.

Práve tak sa dokáže, že $R_k^{(e)} = R_k \cap E$ sú všetky minimálne pravé ideály v E.

Poznámka 1. Je zrejmé, že *ak dve pologrupy typu A majú rovnaký počet minimálnych ľavých aj pravých ideálov, potom k nim prislúchajúce pologrupy idempotentov sú izomorfné.*

Poznámka 2. Nech S je ľubovoľná jednoduchá pologrupa bez nuly, ktorá nie je grupou. Množinu všetkých jej grupových komponentov G_{ik} označme $\mathfrak{G}$ a definujme v nej násobenie takto:

$$G_{ik} \cdot G_{jl} = G_{jk}. \tag{11}$$

Nech S' je jednoduchá pologrupa typu A s tým istým počtom minimálnych ľavých aj pravých ideálov ako S. Potom jej čiastočná pologrupa E je toho istého rádu ako $\mathfrak{G}$.

Je hneď vidieť, že zobrazenie $e_{ik} \to G_{ik}$ pologrupy E na pologrupu $\mathfrak{G}$ je izomorfizmus: $E \cong \mathfrak{G}$. Z toho a z vety 1,9 vyplýva:

Množina $\mathfrak{G}$ všetkých grupových komponentov každej jednoduchej pologrupy S bez nuly, ktorá nie je grupou, vzhľadom na násobenie (11) tvorí jednoduchú pologrupu bez nuly, ktorá má práve toľko minimálnych ľavých aj pravých ideálov ako pôvodná pologrupa S.

2. DIREKTNÝ SÚČIN POLOGRÚP A NIEKTORÉ JEHO VLASTNOSTI

Definícia 2,1. *Nech $S_1 = \{a_\alpha\}$, $S_2 = \{b_\beta\}$, kde α, β prebiehajú nejaké množiny indexov, sú dve pologrupy. Množinu S všetkých usporiadaných dvojíc (a_α, b_β), kde $a_\alpha \in S_1$, $b_\beta \in S_2$ a v ktorej rovnosť a násobenie je definované takýmto spôsobom:*

$$(a_\alpha, b_\beta) = (a_\gamma, b_\delta), \text{ vtedy a len vtedy, ak } a_\alpha = a_\gamma, \ b_\beta = b_\delta$$
$$(a_\alpha, b_\beta)(a_\gamma, b_\delta) = (a_\alpha a_\gamma, b_\beta b_\delta)$$

budeme nazývať direktným súčinom pologrúp S_1, S_2 a budeme značiť $S = S_1 \times S_2$.

Z tejto definície hneď vyplýva, že *direktný súčin dvoch pologrúp je pologrupa.* Ďalej platí:

Veta 2,1. *Platí $S_1 \times S_2 \cong S_2 \times S_1$.*

Dôkaz. Nech $S_1 = \{a_\alpha\}$, $S_2 = \{b_\beta\}$, potom $S_1 \times S_2 = \{(a_\alpha, b_\beta)\}$, $S_2 \times S_1 = \{(b_\beta, a_\alpha)\}$.

Zobrazenie
$$(a_\alpha, b_\beta) \to (b_\beta, a_\alpha)$$

pologrupy $S_1 \times S_2$ na pologrupu $S_2 \times S_1$ je zrejme vzájomne jednoznačné. Je to izomorfizmus, pretože z

$$(a_\varkappa, b_\lambda) \to (b_\lambda, a_\varkappa), \ (a_\mu, b_\nu) \to (b_\nu, a_\mu)$$

vyplýva:

$$(a_\varkappa, b_\lambda)(a_\mu, b_\nu) = (a_\varkappa a_\mu, b_\lambda b_\nu) \to (b_\lambda b_\nu, a_\varkappa a_\mu) = (b_\lambda, a_\varkappa)(b_\nu, a_\mu).$$

Teda je $S_1 \times S_2 \cong S_2 \times S_1$.

Zrejmá je ďalej platnosť ďalšej vety.

Veta 2,2. *Nech $S_1 \cong S_1'$, $S_2 \cong S_2'$, potom:*

$$S_1 \times S_2 \cong S_1' \times S_2'.$$

Veta 2,3. *Nech obidve pologrupy S_1, S_2 obsahujú aspoň jeden idempotent. Potom ich direktný súčin $S = S_1 \times S_2$ obsahuje aspoň jednu čiastočnú pologrupu $S_1' \cong S_1$ a aspoň jednu čiastočnú pologrupu $S_2' \cong S_2$.*

Dôkaz. Nech $e_1 \in S_1$, $e_2 \in S_2$ sú idempotentné elementy. Označme

$$S_1' = \{(a_\alpha, e_2)\}, \ S_2' = \{(e_1, b_\beta)\}.$$

Množiny $S_1' \subseteq S$, $S_2' \subseteq S$ sú zrejme čiastočné pologrupy pologrupy S. Zobrazenie

$$(a_\alpha, e_2) \to a_\alpha$$

je zrejme vzájomne jednoznačné zobrazenie pologrupy S_1' na pologrupu S_1. Je to izomorfizmus, pretože z

$$(a_\varkappa, e_2) \to a_\varkappa, \ (a_\mu, e_2) \to a_\mu$$

vyplýva:

$$(a_\varkappa, e_2)(a_\mu, e_2) = (a_\varkappa a_\mu, e_2) \to a_\varkappa a_\mu.$$

Teda je $S_1' \cong S_1$. Práve tak sa dokáže, že $S_2' \cong S_2$.

Veta 2,4. *Nech pologrupa S_1 obsahuje aspoň jednu pravú (ľavú) jednotku a pologrupa S_2 aspoň jednu ľavú (pravú) jednotku. Potom každý element $s \in S = S_1 \times S_2$ sa dá vyjadriť ako súčin $s = s_1 s_2$ $(s = s_2 s_1)$, kde s_1 je určitý element čiastočnej pologrupy $S_1' \cong S_1$ a s_2 určitý element čiastočnej pologrupy $S_2' \cong S_2$, t. j. platí:*

$$S = S_1' S_2' \ (S = S_2' S_1').$$

Dôkaz. Nech a_1 je pravá jednotka v S_1 a b_1 ľavá jednotka v S_2. Podľa predošlej vety je:

$$S_1' = \{(a_\alpha, b_1)\} \cong S_1, \ S_2' = \{(a_1, b_\beta)\} \cong S_2.$$

Nech $s = (a_\alpha, b^\beta)$ je ľubovoľný element pologrupy $S = S_1 \times S_2$. Potom $s_1 = (a_\alpha, b_1) \in S_1'$, $s_2 = (a_1, b^\beta) \in S_2'$ a platí:

$$s = s_1 s_2, \tag{12}$$

pretože

$$(a_\alpha, b_1)(a_1, b_\beta) = (a_\alpha a_1, b_1 b_\beta) = (a_\alpha, b_\beta).$$

Z toho vyplýva: $S = S_1' S_2'$.

Poznámka. Rozklad $S = S_1' S_2'$ nemusí byť jednoznačný. Ak totiž S_1 má ν_1 pravých a S_2 ν_2 ľavých jednotiek, potom máme aspoň $\nu = \nu_1 \nu_2$ rôznych rozkladov:

$$S = S_1' S_2' = \ldots = S_1^{(\nu)} S_2^{(\nu)}.$$

Avšak pri pevnom S_1' a S_2' je rozklad (12) jednoznačný v dôsledku toho, že je $S_1' \times S_2' \cong S$.

Veta 2,5. *Nech $S = S_1 \times S_2$, nech obidve pologrupy S_1, S_2 obsahujú viac ako jeden element. Potom pologrupa S je jednoduchá bez nuly vtedy a len vtedy, ak obidve pologrupy S_1, S_2 sú jednoduché bez nuly.*

Dôkaz. Pozri Ivan [1], veta 7 a 8.

Poznámka. Vety 2,1—2,5 platia zrejme aj pre nekonečné pologrupy. Ďalšie vety budú už hovoriť iba o konečných pologrupách.

Veta 2,6. *Nech sú splnené predpoklady vety 2,5. Potom pologrupa S je jednoduchá typu A vtedy a len vtedy, ak obidve pologrupy S_1, S_2 sú typu A.*

Dôkaz. Nech S_1, S_2 sú jednoduché pologrupy typu A. Podľa vety 2,5 ich direktný súčin $S = S_1 \times S_2$ je tiež jednoduchá pologrupa bez nuly. Chceme dokázať, že je tiež typu A, t. j. že súčin jej ľubovoľných dvoch idempotentov je idempotent.

Je zrejmé, že element $(a_\alpha, b_\beta) \in S$ je idempotentný vtedy a len vtedy, ak elementy $a_\alpha \in S_1$, $b_\beta \in S_2$ sú idempotentné. Idempotenty v S_1 označme e_1', e_2', e_3', ... a v S_2: e_1'', e_2'', e_3'', ... Potom súčin ľubovoľných dvoch idempotentov z S je

$$(e_i', e_k'')(e_j', e_l'') = (e_i' e_j', e_k'' e_l'') = (e_m', e_n''),$$

teda opäť idempotent z S. Teda $S = S_1 \times S_2$ je typu A.

Naopak, nech S je jednoduchá pologrupa typu A a nech $S = S_1 \times S_2$. Podľa vety 2,5 pologrupy S_1, S_2 sú jednoduché bez nuly. Dokážeme, že obidve sú typu A. Keby totiž aspoň jedna z nich, napr. S_1, bola typu B, potom by obsahovala aspoň dva idempotenty e_i', e_j' také, že $e_i' e_j' = a_\mu$, a_μ nie je idempotent. Potom by bylo $(e_i', e_k'')(e_j', e_l'') = (a_\mu, e_n')$, t. j. pologrupa S by obsahovala aspoň dva také idempotenty, že ich súčin nie je idempotent, čo je spor s predpokladom, že S je typu A.

Dôsledok vety 2,6. *Ak $S = S_1 \times S_2$ a S je jednoduchá pologrupa typu B, potom aspoň jedna z pologrúp S_1, S_2 je typu B.*

Častejšie sa budeme odvolávať ešte na túto vetu:

Veta 2,7. *Ak pologrupa S_1 obsahuje n_1 a pologrupa S_2 n_2 minimálnych ľavých (pravých) ideálov potom ich direktný súčin $S = S_1 \times S_2$ obsahuje $n = n_1 n_2$ minimálnych ľavých (pravých) ideálov.*

Dôkaz. Pozri Ivan [1], veta 6.

3. ROZKLAD JEDNODUCHÝCH POLOGRÚP TYPU A

Teraz pristúpime k riešeniu nášho problému, ktorý znie: Nájsť nevyhnutné a postačujúce podmienky k tomu, aby sa jednoduchá pologrupa bez nuly, ktorá nie je grupou, dala rozložiť na direktný súčin iných pologrúp. V tejto práci sa obmedzíme iba na pologrupy typu A.

Je zrejmé, že pre každú pologrupu S platí $S \cong \{e\} \times S' \cong S' \times \{e\}$, kde $S' \cong S$ a $\{e\}$ je pologrupa, ktorá pozostáva z jediného elementu. Tento triviálny prípad nebudeme uznávať za rozklad a vylúčime ho z našich úvah touto definíciou.

Definícia 3,1. *Budeme hovoriť, že pologrupa S sa dá rozložiť na direktný súčin, ak existujú aspoň dve pologrupy S_1, S_2, z ktorých každá má viac ako jeden element, také, že platí $S_1 \times S_2 \cong S$. Pologrupám S_1, S_2 budeme hovoriť direktné činitele (faktory) pologrupy S.*

Z tejto definície ihneď vyplýva:

Veta 3,1. *Nevyhnutná podmienka k tomu, aby sa pologrupa S dala rozložiť na direktný súčin, je: rad pologrupy S nie je prvočíslo.*

Nakoniec ukážeme, že v prípade jednoduchých pologrúp typu A, ktoré nie sú grupy, táto podmienka je aj postačujúca.

Na základe vety 2,3 stačí sa pri hľadaní direktných faktorov S_1, S_2 pologrupy S obmedziť na jej čiastočné pologrupy. V prípade, že pologrupa S je

jednoduchá typu A, potom podľa vety 2,6 aj jej direktné faktory S_1, S_2 musia byť jednoduché pologrupy typu A. Tejto podmienke vyhovujú okrem eventuálnych ďalších tie čiastočné pologrupy jednoduchej pologrupy typu A, s ktorými sme sa zaoberali v odseku 1. Sú to: L_i, R_k, G, E, $L_i^{(e)}$, $R_k^{(e)}$.

Poznámka. V ďalšom bude vždy značiť S jednoduchú pologrupu bez nuly, L_i, R_k jej minimálne ľavé, resp. pravé ideály, G jej grupový komponent, E množinu všetkých jej idempotentov a $L_i^{(e)}$, $R_k^{(e)}$ minimálne ľavé, resp. pravé ideály v E (ak E tvorí pologrupu). Ďalej s bude značiť počet minimálnych ľavých, t počet minimálnych pravých ideálov v S a g rád grupového komponentu G.

Podľa vety 1,9 E obsahuje práve toľko minimálnych ľavých aj pravých ideálov ako S. G neobsahuje žiaden vlastný ideál. Podľa vety 2,7 pologrupa $G \times E$ obsahuje práve toľko minimálnych ľavých aj pravých ideálov ako S. Dá sa čakať, že bude $G \times E \cong S$. Skutočne platí:

Veta 3,2. *Nech S je jednoduchá pologrupa typu A, ktorá nie je grupou a nech $g > 1$. Potom S sa dá rozložiť na direktný súčin. Platí:*

$$S \cong G \times E.$$

Dôkaz. Pretože S nie je grupa, pologrupa E obsahuje viac ako jeden element:

$$E = \{e_{11}, e_{12}, \ldots, e_{ik}, \ldots\}.$$

Pre jednoduchosť za grupový komponent vezmime grupu G_{11}:

$$G = G_{11} = \{e_{11}, a_{11}, b_{11}, c_{11}, \ldots\}.$$

Elementmi pologrupy $G \times E$ budú teda dvojice (x_{11}, e_{ik}), kde x_{11} prebieha všetky elementy z G_{11}, e_{ik} všetky elementy z E.

Zobrazme teraz pologrupu $G \times E$ na pologrupu S takto: elementu $(x_{11}, e_{ik}) \in G \times E$ priradíme element $x_{ik} \in S$:

$$(x_{11}, e_{ik}) \to x_{ik}.$$

Pritom pod elementom x_{ik} rozumieme stále element grupy G_{ik}, ktorý je rovný (ako v dôkaze vety 1,5) $e_{ik} x_{11} e_{i1}$. Vidieť, že dané zobrazenie je jednoznačné a že množina obrazov pokrýva celé S.

Nech (a_{11}, e_{ik}), (b_{11}, e_{jl}) sú ľubovoľné elementy z $G \times E$. V našom zobrazení im zodpovedajú elementy a_{ik}, b_{jl}:

$$(a_{11}, e_{ik}) \to a_{ik}, \ (b_{11}, e_{jl}) \to b_{jl}. \tag{13}$$

Ak $a_{11} b_{11} = c_{11}$, potom súčinu $(a_{11}, e_{ik})(b_{11}, e_{jl}) = (a_{11} b_{11}, e_{ik} e_{jl}) = (c_{11}, e_{jk})$ v našom zobrazení zodpovedá element $c_{jk} \in S$, teda je:

$$(a_{11}, e_{ik})(b_{11}, e_{jl}) \to c_{jk}. \tag{14}$$

Je však (vzhľadom na vetu 1,8 a na naše označenie):

$$a_{ik} b_{jl} = a_{jk} b_{jk} = c_{jk}. \tag{15}$$

Z (13), (14) a (15) však vyplýva, že uvažované zobrazenie je homomorfizmus. Je aj vzájomne jednoznačné, t. j. dvom rôznym elementom z $G \times E$ zodpovedajú rôzne elementy z S. Ak totiž $(a_{11}, e_{ik}) \neq (b_{11}, e_{jl})$, potom musí nastať aspoň jeden z týchto prípadov: $a_{11} \neq b_{11}$, $i \neq j$, $k \neq l$. Je zrejmé, že vo všetkých týchto troch prípadoch je $a_{ik} \neq b_{jl}$. Teda dané zobrazenie je dokonca izomorfizmus, t. j. $S \cong G \times E$, č. b. t. d.

Z práve dokázanej vety a z vety 2,2 vyplýva tento dôsledok:

Dôsledok vety 3,2. *Nech S, S' sú jednoduché pologrupy typu A, ktoré majú rovnaký počet minimálnych ľavých aj pravých ideálov, nech grupový komponent pologrupy S je izomorfný s grupovým komponentom pologrupy S'. Potom je $S \cong S'$.*

Inými slovami: *Jednoduchá pologrupa S typu A je grupovým komponentom G a pologrupou E svojich idempotentov až na izomorfizmus jednoznačne určená.*

Poznámka 1. V prípade $g = 1$ je $E = S$ a podľa vety 3,2 by sme dostali triviálny rozklad $S \cong e \times S$. Práve tak v prípade, že S je grupou: $S = S \times e$. V zmysle definície 3,1 teda všetky predpoklady vety 3,2 sú podstatné.

Veta 3,2 hovorí, že postačujúcou podmienkou k tomu, aby sa jednoduchá pologrupa typu A, ktorá nie je grupou, dala rozložiť na direktný súčin, je: $g > 1$. Táto podmienka však nie je, ako uvidíme na nasledujúcom príklade, nevyhnutná.

Príklad. Pologrupa $S = \{a_1, a_2, a_3, a_4\}$, v ktorej násobenie je dané touto multiplikačnou tabuľkou:

	a_1	a_2	a_3	a_4
a_1	a_1	a_1	a_3	a_3
a_2	a_2	a_2	a_4	a_4
a_3	a_1	a_1	a_3	a_3
a_4	a_2	a_2	a_4	a_4

je jednoduchá bez nuly typu A. Jej minimálne ideály sú:

$$L_1 = \{a_1, a_2\},\ L_2 = \{a_3, a_4\};\ R_1 = \{a_1, a_3\},\ R_2 = \{a_2, a_4\}$$

a grupové komponenty:

$$G_{11} = \{a_1\}, G_{12} = \{a_2\}, G_{21} = \{a_3\}, G_{22} = \{a_4\}.$$

Je teda $g = 1$ a rozklad tvaru uvedeného vo vete 3,2 nie je možný. Avšak táto pologrupa sa predsa dá rozložiť, avšak iným spôsobom. Platí napr.

$$S \cong L_1 \times R_1.$$

Dokonca tu platí $S = L_1 R_1$.

Zobrazme pologrupu $L_1 \times R_1$ na pologrupu S takto:

$$\begin{aligned}(a_1, a_1) &\to a_1 a_1 = a_1,\\ (a_2, a_1) &\to a_2 a_1 = a_2,\\ (a_1, a_3) &\to a_1 a_3 = a_3,\\ (a_2, a_3) &\to a_2 a_3 = a_4.\end{aligned}$$

Označme $(a_1, a_1) = c_1$, $(a_2, a_1) = c_2$, $(a_1, a_3) = c_3$, $(a_2, a_3) = c_4$. Pre $L_1 \times R_1$ dostávame túto multiplikačnú tabuľku:

	c_1	c_2	c_3	c_4
c_1	c_1	c_1	c_3	c_3
c_2	c_2	c_2	c_4	c_4
c_3	c_1	c_1	c_3	c_3
c_4	c_2	c_2	c_4	c_4

Teda skutočne je $L_1 \times R_1 \cong S$.

Poznámka 2. Uvažujme jednoduchú pologrupu S bez nuly (nezávisle od toho či je typu A alebo B). Nech prirodzené čísla g, s, t majú obvyklý význam. Potom má pologrupa S zrejme gst rôznych elementov. Uvažujme ďalej množinu $L_i R_k$ (i, k pevné). Táto množina je zrejme obojstranným ideálom v S. Keďže však S je jednoduchá pologrupa, je nevyhnutne $S = L_i R_k$. Nie je však vo všeobecnosti pravda, že platí $S \cong L_i \times R_k$. Ideál L_i má totiž presne gt, ideál R_k presne gs elementov. Teda $L_i \times R_k$ má presne $g^2 st$ rôznych elementov. Keďže pre $g > 1$ je vždy $g^2 st > gst$, platí táto veta:

Rozklad tvaru $S \cong L_i \times R_k$ je možný iba vtedy, ak $g = 1$.

Prv, ako by sme sa podrobnejšie zaoberali rozkladom takých pologrúp, u ktorých je $g = 1$, t. j. takých, ktoré obsahujú iba samé idempotenty, položme si takúto otázku: V rozklade podľa vety 3,2 jeden direktný faktor je grupa; otázka je, či a kedy sa jednoduchá pologrupa typu A dá rozložiť tak, aby ani jeden direktný faktor nebol grupou. Postačujúcu podmienku pre to nájdeme ľahko. O tom hovorí ďalšia veta.

Veta 3,3. *Nech S je jednoduchá pologrupa typu A, nech $s > 1$, $t > 1$. Potom sa S dá rozložiť na direktný súčin dvoch pologrúp, z ktorých ani jedna nie je grupou. Platí:*

$$S \cong L_i \times R_k^{(e)},\ S = L_i R_k^{(e)} \tag{16}$$

alebo

$$S \cong L_i^{(e)} \times R_k,\ S = L_i^{(e)} R_k. \tag{16'}$$

Dôkaz. Nech S splňuje predpoklady vyslovenej vety. Vidieť, že v tom prípade ideály L_i, R_k, $L_i^{(e)}$, $R_k^{(e)}$ iste nie sú grupy a každý z nich obsahuje viac ako jeden element.

Vezmime teraz ľubovoľný ideál L_i v S a ľubovoľný ideál $R_k^{(e)}$ v E. Podľa vety 1,2 L_i je zľava a $R_k^{(e)}$ sprava jednoduchá pologrupa bez nuly, teda obidve sú typu A. Podľa vety 2,6 aj ich direktný súčin $L_i \times R_k^{(e)}$ je jednoduchá pologrupa typu A. Ďalej, v dôsledku viet 1,4; 1,5; 1,9; 2,7 a vety 10 z práce Ivan [1], pologrupa $L_i \times R_k^{(e)}$ obsahuje práve toľko minimálnych ľavých aj pravých ideálov ako pologrupa S a jej grupový komponent je izomorfný s grupovým komponentom pologrupy S. Podľa dôsledku vety 3,2 teda platí

$$S \cong L_i \times R_k^{(e)}.$$

Pologrupa L_i obsahuje zrejme aspoň jednu pravú jednotku, pretože je minimálnym ľavým ideálom v S a teda každý jej idempotent je jej pravou jednotkou. Práve tak pologrupa $R_k^{(e)}$ obsahuje aspoň jednu ľavú jednotku. Teda podľa vety 2,4 je $S = L_i R_k^{(e)}$.

Práve tak sa dokáže, že je $S \cong L_i^{(e)} \times R_k$, $S = L_i^{(e)} R_k$.

Poznámka 1. Vetu 3,2 sme dokázali tak, že sme našli jedno určité izomorfné zobrazenie pologrupy $G \times E$ na pologrupu S, kým vetu 3,3 sme dokázali bez toho, že by sme museli hľadať nejaké izomorfné zobrazenie pologrupy $L_i \times R_k^{(e)}$ na pologrupu S. Dokázali sme iba, že $L_i \times R_k^{(e)}$ sa dá izomorfne zobraziť na S. Takých zobrazení môže však vo všeobecnosti existovať viac. Jedno z nich nájdeme ľahko. Je to:

$$(x_{i\nu}, e_{\mu k}) \to x_{i\nu} e_{\mu k} = x_{\mu\nu}.$$

Toto zobrazenie pologrupy $L_i \times R_k^{(e)}$ na pologrupu S je zrejme vzájomne jednoznačné, pretože je $S = L_i R_k^{(e)}$. Overíme si, že je to aj homomorfizmus.

Nech $(a_{i\mu}, e_{\nu k})$, $(b_{i\varrho}, e_{\sigma k})$ sú ľubovoľné elementy z $L_i \times R_k^{(e)}$. Potom

$$(a_{i\mu}, e_{\nu k}) \to a_{\nu\mu}, \; (b_{i\varrho}, e_{\sigma k}) \to b_{\sigma\varrho}.$$

Ak $a_{11} b_{11} = c_{11}$, potom $a_{\nu\mu} b_{\sigma\varrho} = a_{\sigma\mu} b_{\sigma\mu} = c_{\sigma\mu}$. Treba teda dokázať, že súčin $(a_{i\mu}, e_{\nu k})(b_{i\varrho}, e_{\sigma k})$ sa zobrazí na $c_{\sigma\mu}$. Skutočne je:

$$(a_{i\mu}, e_{\nu k})(b_{i\varrho}, e_{\sigma k}) = (a_{i\mu} b_{i\varrho}, e_{\nu k} e_{\sigma k}) = (a_{i\mu} b_{i\mu}, e_{\sigma k}) = (c_{i\mu}, e_{\sigma k}) \to c_{\sigma\mu}.$$

Teda uvažované zobrazenie je skutočne izomorfné.

Poznámka 2. Všimnime si, že v predpokladoch vety 3,3 sa nič nehovorí o g, t. j. o počte elementov grupového komponentu. Teda veta 3,3 platí aj pre také pologrupy, ktoré obsahujú iba samé idempotenty. V tom prípade je $E = S$, $L_i^{(e)} = L_i$, teda platí $S \cong L_i \times R_k$, $S = L_i R_k$ (pozri príklad za vetou 3,2). V spojení s poznámkou 2 za vetou 3,2 teda dostávame:

Dôsledok vety 3,3. *Nevyhnutná a postačujúca podmienka k tomu, aby sa jednoduchá pologrupa S typu A dala rozložiť na direktný súčin tvaru*

$$S \cong L_i \times R_k,$$

je: $g = 1$, $s > 1$, $t > 1$.

Veta 3,3 má pred vetou 3,2 tú výhodu, že platí nezávisle od toho, či pologrupa obsahuje iba samé idemponenty alebo nie. Jej nevýhodou však je to, že predpokladá existenciu vlastných minimálnych ľavých aj pravých ideálov.

Všimnime si, čo sa stane, ak vo vete 3,3 predpoklad $s > 1$, $t > 1$ nahradíme predpokladom: $s = 1$, $t > 1$. V tom prípade je $L_i = S$, $R_k^{(e)} = e_{1k}$, $L_i^{(e)} = E$, $R_k = G_{1k}$, takže podľa (16) dostaneme triviálny rozklad $S \cong S \times e_{1k}$ a podľa (16'): $S \cong E \times G_{1k}$, $S = EG_{1k}$. Ak však $g = 1$, potom aj tento druhý rozklad bude triviálny. Ak však pridáme predpoklad $g > 1$, potom takú zľava jednoduchú pologrupu bez nuly môžeme podľa (16') rozložiť, ale pritom jeden faktor rozkladu bude opäť grupou. To isté zrejme platí aj pre sprava jednoduché pologrupy. Takto dostávame ďalšiu vetu, ktorá je vlastne špeciálnym prípadom vety 3,2.

Veta 3,4. *Nech S je zľava (sprava) jednoduchá pologrupa bez nuly, ktorá nie je grupou, nech $g > 1$. Potom S sa dá rozložiť na direktný súčin. Platí:*

$$S \cong E \times G_{1k}, \; S = EG_{1k}, \text{ resp. } S \cong G_{i1} \times E, \; S = G_{i1} E.$$

Poznámka: Z vety 3,4 vyplýva, že každá zľava jednoduchá pologrupa bez nuly, ktorá nie je grupou, má túto vlastnosť: Každý jej element sa dá jednoznačne vyjadriť ako súčin jedného idempotentu a jedného elementu ľubovoľného grupového komponentu G_{1k}. V prípade, že $g = 1$, to tiež platí, pretože v tom prípade je $G_{1k} = \{e_{ik}\}$ a e_{ik} pravou jednotkou v $S = E$. Podobne to platí pre sprava jednoduché pologrupy. Vzniká otázka, či také niečo platí aj pre obyčajnú jednoduchú pologrupu typu A. Kladnú odpoveď dáva táto veta:

Veta 3,5. *Nech sú splnené predpoklady vety 3,3 a nech okrem toho je $g > 1$. Potom pologrupa S sa dá rozložiť takto:*

$$S \cong L_j^{(e)} \times G_{ik} \times R_l^{(e)}, \; S = L_j^{(e)} G_{ik} R_l^{(e)},$$

kde G_{ik} je ľubovoľný grupový komponent a $L_j^{(e)}$, $R_l^{(e)}$ ľubovoľný minimálny ľavý, resp. pravý ideál v E.

Dôkaz. Podľa vety 3,3 platí:

$$S \cong L_i \times R_l^{(e)}, \; S = L_i R_l^{(e)} \tag{17}$$

alebo

$$S \cong L_j^{(e)} \times R_k, \; S = L_j^{(e)} R_k. \tag{17'}$$

Podľa vety 1,2 ideál L_i je zľava jednoduchá pologrupa bez nuly. Jej minimálne pravé ideály sú grupy G_{ik}, $k = 1, 2, \ldots t$. Príslušná pologrupa idempotentov je zrejme $L_i^{(e)}$. Teda podľa vety 3,4 platí:

$$L_i \cong L_i^{(e)} \times G_{ik}, \; L_i = L_i^{(e)} G_{ik}.$$

Ukážeme, že v tomto rozklade ideál $L_i^{(e)}$ môžeme nahradiť ľubovoľným iným ideálom $L_j^{(e)}$, $j \neq i$.

Pretože $L_i^{(e)} \cong L_j^{(e)}$, je $L_i \cong L_j^{(e)} \times G_{ik}$. Ďalej podľa vety 1,6a je $e_{j\nu} G_{ik} = G_{i\nu}$. Na základe toho je:

$$L_j^{(e)} G_{ik} = \{e_{j1}, e_{j2}, \ldots, e_{jt}\} G_{ik} = \{G_{i1}, G_{i2}, \ldots, G_{it}\} = L_i.$$

Teda skutočne je $L_i = L_j^{(e)} G_{ik}$, aj keď $j \neq i$. Ak to dosadíme do (17), dostaneme

$$S \cong L_j^{(e)} \times G_{ik} \times R_l^{(e)}, \; S = L_j^{(e)} G_{ik} R_l^{(e)}. \tag{18}$$

Podobne sa dokáže, že $R_k = G_{ik} R_l^{(e)}$ aj pre $l \neq k$. Po dosadení do (17') dostaneme opäť (18).

Poznámka. Ak nám ide iba o vyjadrenie $S = L_j^{(e)} G_{ik} R_l^{(e)}$, potom môžeme vo vete 3,5 predpoklad $g > 1$ vynechať. Ak však $g = 1$, potom dostaneme rozklad $S \cong L_j^{(e)} \times e_{ik} \times R_l^{(e)}$, ktorý je v podstate ten istý ako podľa vety 3,3, pretože v tom prípade je $L_j^{(e)} \times e_{ik} \times R_l^{(e)} \cong L_j^{(e)} \times R_l^{(e)} = L_j \times R_l$.

Na základe predchádzajúcich viet vieme už rozložiť na direktný súčin každú jednoduchú pologrupu typu A, ktorá nie je grupou, okrem takých, ktoré obsahujú iba samé idempotenty a sú zároveň zľava, resp. sprava jednoduché. Dalšia veta nám však umožní rozložiť aj takéto pologrupy.

Veta 3,6. *Nech S je zľava (sprava) jednoduchá pologrupa bez nuly, nech nie je grupou a nech obsahuje iba samé idempotenty (t. j. $g = 1$). Nevyhnutná a postačujúca podmienka k tomu, aby sa taká pologrupa dala rozložiť na direktný súčin, je: rád pologrupy S nie je prvočíslo.*

Dôkaz. Podmienka je zrejme nevyhnutná. Dokážeme, že je aj postačujúca. Nech rád n pologrupy S, ktorá splňuje predpoklady vyslovenej vety, nie je prvočíslo. To znamená, že sa rád n dá rozložiť takto:

$$n = n_1 n_2, \; n_1 > 1, \; n_2 > 1.$$

Nech S je napr. zľava jednoduchá. Za daných predpokladov to znamená, že každý jej element je jej minimálnym pravým ideálom, t. j. pre každé $a_i \in S$ platí $a_i S = a_i$. Súčet ľubovoľného počtu ideálov je opäť ideál. Teda množiny

$$S_1 = \{a_1, a_2, \ldots, a_{n_1}\}, \; S_2 = \{a_{n_1+1}, a_{n_1+2}, \ldots, a_{n_1+n_2}\}$$

sú pravé ideály v S a teda pologrupy. Je zrejmé, že obidve pologrupy S_1, S_2 sú opäť zľava jednoduché a S_1 obsahuje n_1 a S_2 n_2 minimálnych pravých ideálov. Teda podľa vety 2,7 ich direktný súčin $S_1 \times S_2$ je zľava jednoduchá pologrupa a obsahuje $n = n_1 n_2$ minimálnych pravých ideálov, každý jej element je zrejme idempotentný. Z toho na základe dôsledku vety 3,2 vyplýva, že je $S \cong S_1 \times S_2$.

Pre sprava jednoduché pologrupy sa veta dokáže úplne analogicky.

Poznámka. Pologrupy S_1, S_2 v dôkaze vety **3,6** možno zrejme vybrať aj iným spôsobom. Stačí totiž vybrať z S také dve podmnožiny, z ktorých jedna obsahuje n_1 a druhá n_2 elementov. Vidieť, že všetky takto získané S_1, resp. S_2 sú navzájom izomorfné.

Príklad. Pologrupa $S_1 = \{a_1, a_2, a_3, a_4\}$ s touto multiplikačnou tabuľkou

	a_1	a_2	a_3	a_4
a_1	a_1	a_1	a_1	a_1
a_2	a_2	a_2	a_2	a_2
a_3	a_3	a_3	a_3	a_3
a_4	a_4	a_4	a_4	a_4

splňuje predpoklady vety 3,6. V tom prípade je $n = 4 = 2 \,.\, 2$, teda $n_1 = 2$, $n_2 = 2$.

$$S_1 = \{a_1, a_2\}, \; S_2 = \{a_3, a_4\},$$
$$S_1 \times S_2 = \{(a_1, a_3), (a_1, a_4), (a_2, a_3), (a_2, a_4)\}.$$

Pre jednoduchosť označme $(a_1, a_3) = c_1$, $(a_1, a_4) = c_2$, $(a_2, a_3) = c_3$, $(a_2, a_4) = c_4$. Ľahko sa presvedčíme, že multiplikačná tabuľka pologrupy $S_1 \times S_2$ je:

	c_1	c_2	c_3	c_4
c_1	c_1	c_1	c_1	c_1
c_2	c_2	c_2	c_2	c_2
c_3	c_3	c_3	c_3	c_3
c_4	c_4	c_4	c_4	c_4

Teda skutočne je $S_1 \times S_2 \cong S$. Práve tak je $S \cong \{a_1, a_3\} \times \{a_2, a_4\}$ alebo napr. $S \cong \{a_1, a_4\} \times \{a_2, a_3\}$, $S \cong \{a_1, a_2\} \times \{a_1, a_2\}$.

Ľahko by sme si na tomto príklade mohli tiež overiť, že každé vzájomne jednoznačné zobrazenie pologrupy $S_1 \times S_2$ na pologrupu S je izomorfizmus.

Z dokázaných viet teraz vyplýva:

Veta 3,7. *Jednoduchá pologrupa typu A, ktorá nie je grupou, dá sa rozložiť na direktný súčin pologrúp vtedy a len vtedy, ak nie je prvočíselného rádu.*

Dôkaz. Na základe vety 3,1 treba už dokázať iba to, že podmienka je postačujúca.

Nech pologrupa S splňuje predpoklady vety a nech jej rad n nie je prvočíslo. Môžu nastať tieto dva prípady: $g = 1$, $g > 1$. V prvom prípade sa pologrupa dá rozložiť podľa vety 3,3 a 3,6, v druhom prípade podľa vety 3,2 a 3,3, resp. 3,4 a 3,5.

Tým je náš problém, položený na začiatku tohto odseku, pre jednoduché pologrupy typu A rozriešený. Rozkladom pologrúp typu B sa hodlám zaoberať v ďalšej práci.

LITERATÚRA

Schwarz Št., [1] *Teória pologrúp.* Sborník prác Prírodovedeckej fakulty Slovenskej univerzity v Bratislave, 6 (1943), 1—64.

[2] Структура простых полугрупп без нуля, Чехословацкий математический журнал, т. 1 (76), 1951, 51—65.

[3] *Maximálne ideály a štruktúra pologrúp.* Mat.-fyz. čas. SAV, 3 (1953), 17—38.

Suschkewitsch A., [1] *Über die endlichen Gruppen ohne das Gesetz der eindeutigen Umkehrbarkeit.* Math. Annalen, 99 (1928), 30—50.

Ivan J., [1] *O direktnom súčine pologrúp.* Mat.-fyz. čas. SAV, 3 (1953), 57—66.

Došlo dňa 18. II. 1954.

Katedra matematiky
Slovenskej vysokej školy technickej,
Bratislava

О РАЗЛОЖЕНИИ ПРОСТЫХ ПОЛУГРУПП В ПРЯМОЕ ПРОИЗВЕДЕНИЕ

Я. ИВАН

Выводы

Настоящая работа имеет три части. Первая часть имеет вспомогательный характер. Ее содержанием является доказательство нескольких теорем (по большей части известных) о структуре конечных простых полугрупп без нуля. При этом оказалось удобным разделить конечные простые полугруппы, без нуля в две отделения (классы):

1. Простые полугруппы типа A — удовлетворяющие условию: произведение произвольных двух идемпотентов тоже идемпотент.

2. Простые полугруппы типа B — не удовлетворяющие этому условию.

Содержанием второй части, которая имеет тоже вспомогательный характер, является изучение некоторых свойств прямого произведения полугрупп, именно конечных простых полугрупп без нуля. Доказывается например, следующая теорема:

Пусть S_1, S_2 полугруппы, из которых каждая содержит больше одного элемента. Потом их прямое произведение $S = S_1 \times S_2$ простая полугруппа типа A тогда и только тогда, когда обе полугруппы S_1, S_2 простые типа A.

Ядром работы является часть третья, в которой решается этот вопрос: которые условия необходимые и достаточные для того, чтобы простая полугруппа типа A была разложимая в прямое произведение. При этом мы говорим, что полугруппа S разложимая в прямое произведение, если существуют по меньшей мере две такие полугруппы S_1, S_2, из которых каждая содержит больше одного элемента, что $S \cong S_1 \times S_2$. Главный результат этой части — следующая теорема:

Простая полугруппа типа A, которая не является группой, разложимая в прямое произведение тогда и только тогда, когда ей порядок не является простым числом.

Остальные теоремы имеют более специальный характер.