Werk

Label: Article

Jahr: 1949

PURL: https://resolver.sub.uni-goettingen.de/purl?31311028X_0074|log62

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

O ZOVŠEOBECNENIACH POJMU GRUPY.

ŠTEFAN SCHWARZ, Bratislava.

V posledných desiatich rokoch sme vo vývine matematiky svedkami veľmi intenzívnych snáh, ktorých cieľom je zovšeobecniť pojem grupy.

Pojem grupy, ktorý sa ukázal byť jedným zo základných matematických pojmov, vznikol abstrakciou z celkom konkrétnych aritmetických, geometrických, ba i fyzikálnych pojmov. Z podobného hľadiska núkajú sa nám často i rozmanité zovšeobecnenia pojmu grupy. Okrem tohto, povedzme kvazi — praktického, hľadiska je už čisto noeticky dôležité a matematicky účelné študovať, ako sa zmenia vety z klasickej teórie grúp, ak niektorý z axiómov vynecháme alebo zmeníme. Takto dostávame výsledky, ktoré sú niekedy podobné známym vetám z teórie grúp; často vety, ktoré sú triviálne, ak prejdeme ku grupám; inokedy výsledky nemajúce analogie v teórii grúp.

Systematické štúdium zovšeobecnených grúp začína sa okolo roku 1937. Už predtým (od r. 1928) sa objavovaly tu a tam rozmanité príspevky — boly však do istej miery náhodné. Počet väčších — menších prác, uverejnených na túto tému, možno odhadnúť na 120—130. Za hlavných zakladateľov možno zhruba označiť SUŠKEVIČA, ORE-A a DUBREILLA.

V tejto prednáške nemôžem prirodzene referovať o *obsahu* publikovaných prác. Podám skôr len *formuláciu* niekoľkých hlavných problémov tohto pracovného úseku. Nie je dnes ešte čas prorokovať, či tieto teórie budú mať ten význam vo vývine matematiky, ako mala a má teória grúp.

V literatúre prejednávané spôsoby zovšeobecnenia grúp sú veľmi rôznorodé. Neexistuje ešte jednotného a teda dosť prehľadného hľadiska. Nebude preto len vecou osobnej nešikovnosti, ak sa mi nepodarí absolvovať vytknutý program k úplnej spokojnosti. I obmedzené miesto pôsobí prirodzene, že výber problematiky je subjektívne podfarbený.

Ako je známo, nazývame grupou neprázdnu množinu elementov, medzi ktorými je definované násobenie splňujúce tieto axiómy:

A 1. Ku každej dvojici elementov a, b existuje taký jediný element c, že $a \,.\, b = c$.

A 2. Platí zákon asociatívny: $a(b \,.\, c) = (a \,.\, b)c$.

A 3. (Axióm existencie podielu.) Ku každej dvojici a, b existujú také elementy x, y, že rovnice $ax = b$, $ya = b$ majú jediné riešenie.[1])

Zovšeobecnenie pojmu grupy možno previesť jednoducho tak, že niektorý z axiómov A 1—A 3 vynecháme alebo nahradíme slabším.

Hlavné v literatúre prejednávané systémy sú tieto:

a) *Grupoid*: platí iba axióm A 1 a nič viac.

b) *Kvazigrupa*: platí A 1 a A 3.

c) *Pologrupa* (semigrupa): platí 1 A a A 2.

[1]) Túto formuláciu axiómov volím s ohľadom na ďalšie.

Ďalšia možnosť zovšeobecnenia je v tom, že v A 1 vynecháme slová „jediný element" a nahradíme ich slovami „množina elementov". Ak nepridáme žiadne ďalšie podmienky, dostaneme najvšeobecnejší možný pojem, tzv. *multigrupoid*. Jeho špeciálnym prípadom je tzv. *multigrupa*. O tom detailnejšie v odstavci IV.

Je prirodzené, že sú tým naznačené iba najpodstatnejšie možnosti zovšeobecnenia. Často sa ukazuje zaujímavým alebo užitočným študovať napr. pologrupy alebo kvazigrupy s ďalšími dodatkovými podmienkami.

Prebereme jednotlivé pojmy tak, ako sme ich citovali za sebou.

I. Grupoidy.

Grupoidom nazývame množinu, v ktorej je definované násobenie spĺňajúce axióm A 1 a nič viac. (Ore-Hausmann [1]).

To je pojem veľmi obecný, od ktorého nie je možno na prvý pohľad mnoho očakávať. Nie je tomu ale tak.

Môžeme predpokladať, že sú jasné tieto pojmy: grupoid konečný, nekonečný, komutatívny, nekomutatívny, podgrupoid (čiastočný grupoid), Cayleyho tabuľka. Práve tak môžeme predpokladať, že je známy pojem komplexu a počítanie komplexami, ako i pojem izomorfizmu a homomorfizmu.

Upozornime hneď na niektoré *drobnosti*, ktorými sa grupoid *líši* od grupy:

a) V grupe (rôznej od jednotkovej) existuje vždy vlastná podgrupa, totiž jednotková. Grupoid nemusí mať však vôbec žiadny vlastný podgrupoid, tým menej jednotkový element.

b) Dva vlastné podgrupoidy daného grupoidu môžu mať prázdny prienik. (Ak je prienik neprázdny, je sám podgrupoidom).

c) Nech a je elementom grupoidu $\mathbf{G}$. V grupoide je rozdiel medzi $a \,.\, (a \,.\, a)$ a $(a \,.\, a) \,.\, a$. Nemá teda smyslu hovoriť o elemente a^3. Má najvýš smysel hovoriť o podgrupoide $\{a\}$, ktorý pozostáva zo všetkých možných súčinov vzniklých z jediného elementu a. Takýto grupoid sa volá *cyklický* grupoid vytvorený elementom a.

1.

Podívajme sa na grupoid $\mathbf{G}$ na chvíľku iba ako na množinu. Myslime si, že $\mathbf{G}$ rozdelíme nejakým spôsobom na súčet disjunktných množín (tried). Každý takýto rozklad R nám dáva možnosť definovať v $\mathbf{G}$ ekvivalenciu a to tým, že dva elementy nazveme ekvivalentnými, ak patria do tej istej triedy. Je zvykom písať $a \equiv b \pmod{R}$, ak a, b patria do tej istej triedy. Takýto rozklad nerešpektujúci vzájomný vzťah elementov množiny $\mathbf{G}$ nemôže ovšem viesť k žiadnemu pre nás zaujímavému výsledku.

DUBREILL [4][2]) zaviedol dôležitý pojem. Rozklad R grupoidu $\mathbf{G}$ budeme volať *regulárnym* rozkladom, ak platí toto: keď elementy $a, b, c, \ldots$ sú v spoločnej triede T, potom i elementy $ax, bx, cx, \ldots$ sú opäť v akejsi spoločnej triede T' a práve tak elementy $xa, xb, xc, \ldots$ v nejakej (obecne inej) triede T'' a to pre každé $x \in \mathbf{G}$. (Pre rôzne x dostávame prirodzene rôzne triedy). V Symboloch: rozklad R voláme regulárnym, ak vzťah $a \equiv b \pmod R$ implikuje $ax \equiv bx, xa \equiv xb \pmod R$. Populárne povedané, pri takomto rozklade násobenie triedu nerozbije, ale iba ako celok vnorí do inej triedy. Tu sa už uplatňujú individuálne vlastnosti grupoidu.

Je zaujímavé, že skoro všetky dosiaľ v algebre používané rozklady majú túto vlastnosť. U grupy je napr. rozklad do tried podľa normálneho deliteľa regulárnym rozkladom a ľahko sa dokáže, že takto dostaneme každý regulárny rozklad grupy.

Nechajme zatiaľ stranou veľmi dôležitú otázku, akým spôsobom možno na rôznych typoch grupoidov *realizovať* regulárne rozklady.

Majme grupoid $\mathbf{G}$ a na ňom regulárny rozklad. Z regularity plynie: ak násobím ktorýkoľvek element triedy T_a a ktorýkoľvek element triedy T_b, dostanem vždy element akejsi triedy T_c. Teda triedy tvoria grupoid, ak medzi nimi definujeme násobenie vzťahom: $T_a \odot T_b = T_c$, keď v smysle násobenia komplexov je $T_a \,.\, T_b \subseteq T_c$. Regulárny rozklad umožňuje teda definovať obvyklým spôsobom *faktorový grupoid* $\mathbf{G} \mid R$, totiž ako grupoid tried. Takmer ihneď sa dokáže:

Veta o izomorfizme pre grupoidy: a) Faktorový grupoid $\mathbf{G} \mid R$ je homomorfný ku grupoidu $\mathbf{G}$. b) Ak grupoid $\mathbf{G}'$ je homomorfným obrazom grupoidu $\mathbf{G}$, existuje taký regulárny rozklad grupoidu $\mathbf{G}$, že $\mathbf{G} \mid R$ je izomorfné s grupoidom $\mathbf{G}'$.[3])

2.

Dívajme sa opäť na chvíľu na grupoid $\mathbf{G}$ iba ako na množinu. Majme dva rozklady R_1, R_2. Budeme hovoriť, že je $R_1 \leqq R_2$, keď $a \equiv b \pmod{R_1}$ implikuje $a \equiv b \pmod{R_2}$.

Pre rozklady možno definovať dve operácie a to *prenik* a *súčin*. Prenikom $D = R_1 \cap R_2$ nazývame taký rozklad D, pri ktorom sú dva elementy ekvivalentné vtedy a len vtedy, keď sú ekvivalentné vzhľadom k obidvom rozkladom R_1 a R_2. Prenik D vždy existuje, pretože napríklad rozklad E, pri ktorom je každý element sám triedou, spĺňuje vždy $E \leqq R_1$, $E \leqq R_2$. Súčin dvoch rozkladov $R_1 \,.\, R_2$ definujeme takto. Uvažujme všetky rozklady C, pre ktoré platí $R_1 \leqq C$, $R_2 \leqq C$. Množina elementov C je neprázdna, keďže obsahuje v sebe napr. tzv. absolútny

[2]) Tento pojem pochádza v podstate od ORE-A. (Viď tiež DUBREIL P.-DUBREILL-JACOTIN [1], [2], BORŮVKA [4] a iní.)

[3]) Stačí dať do tej istej triedy vždy tie elementy, ktoré sú originálom patriacim k tomu istému elementu $a' \in G'$.

rozklad, pri ktorom sú všetky elementy spolu ekvivalentné. Prenik všetkých rozkladov C horeuvedenej vlastnosti voláme súčinom $R_1 . R_2$.

Je zrejmé, že množina všetkých rozkladov tvorí *sväz*. (Pritom sme sväzové operácie práve vymenovali.)

Čo je pre nás dôležité, je, že i množina všetkých regulárnych rozkladov tvorí sväz. Teda i množina všetkých regulárnymi rozkladmi definovaných faktorových grupoidov tvorí sväz (pričom sväzové operácie nemusíme podrobne vypisovať).

Pre tento sväz možno odvodiť vety o izomorfizme, obzvlášť teda rozšíriť na grupoidy i ďalšie dve vety o izomorfizme známe z teórie grúp. Tieto vety majú príliš obecné znenie, preto upúšťam od ich formulácie (viď napr. Borůvka [4]). Ďalej sem možno previesť rad viet spočívajúcich výhradne na vetách o izomorfizme, teda vety z okruhu viet Jordan-Hölderových. Tieto vety sú potom už zrejme podradené obecnej teórii sväzov, keďže, okrem predpokladu regularity rozkladu, nikde neužívame toho, že elementy samotné ako indivíduá tvoria grupoid.

Toľko o obecnej teórii grupoidov. (Ďalšia literatúra: Borůvka [1]—[5], Bruck, [4], p. 247—254, Ore [1], Richardson [1], [2]).

II. Kvazigrupy.

Teória grupoidov sa stane bohatšou, ak pribereme axióm A 3. Grupoid, v ktorom sú splnené axiómy A 1 a A 3, volá sa *kvazigrupou*.

Objavujú sa isté *podobnosti* s grupami:

a) Z jednoznačnosti riešenia rovníc $ax = b, ya = b$ vyplýva platnosť „pravidla o krátení". V Cayley-ho tabuľke sa to prejaví tým, že v každom riadku a každom stĺpci sú zastúpené všetky elementy.

b) Každý podgrupoid konečnej kvazigrupy je kvazigrupa.[4])

1.

Keby sme pre kvazigrupu $\mathbf{Q}$ pripustili platnosť asociatívneho zákona, dostali by sme grupu. Ak nechceme mať (z nášho hľadiska) triviálne výsledky, nesmú byť všetky trojice asociatívne.

Prvá prirodzená otázka je táto. Nazvime element $\alpha \in \mathbf{Q}$ asociatívnym, ak pre všetky dvojice $x, y \in \mathbf{Q}$ je $x(\alpha y) = (xx)y$. Čo vieme povedať o množine $\boldsymbol{A}$ asociatívnych elementov? Odpoveď (Garrison [1]): Množina $\boldsymbol{A}$ je neprázdna vtedy a len vtedy, ak $\mathbf{Q}$ obsahuje obojstranný jednotkový element e. Množina $\boldsymbol{A}$ je potom grupou a e je jej jednotkovým elementom[5]).

[4]) Neplatí to samozrejme pro nekonečné kvazigrupy, lebo podobná veta neplatí ani pre nekonečné grupy.

[5]) Keď obecný grupoid má obojstranný jednotkový element, má taký len jediný. Pravých (alebo ľavých) jednotiek môže mať grupoid (špeciálne tiež kvazigrupa alebo pologrupa) i nekonečne mnoho.

Podobne: množina A_p tých elementov α, ktoré splňujú $(xy)\alpha = x(y\alpha)$ pre každé $x, y \in \mathbf{Q}$, tvorí grupu. Táto grupa je neprázdna vtedy a len vtedy, ak existuje v $\mathbf{Q}$ pravá jednotka e_p. Toto e_p je potom jednotkovým elementom grupy A_p[6]).

2.

Začnime sledovať ako ďaleko siahajú *analogie* s teóriou grúp.

Nech $\mathbf{Q}, \mathbf{Q}'$ sú dve kvazigrupy. Nech $\mathbf{Q}' \subset \mathbf{Q}$. Z axiómu A 3 je jasné, že vždy možno písať (s vhodne volenými $\alpha, \beta, \gamma, \ldots$)

$$\mathbf{Q} = \mathbf{Q}'\alpha + \mathbf{Q}'\beta + \mathbf{Q}'\gamma + \ldots \qquad (1)$$

Takýto rozklad budeme volať rozkladom v *triedy mod* $\mathbf{Q}'$, ak

a) množiny $\mathbf{Q}'\alpha, \mathbf{Q}'\beta, \ldots$ sú disjunktné,

b) každý element $\in \mathbf{Q}'\varkappa$ vytvoruje $\mathbf{Q}'\varkappa$, t. j. $\mathbf{Q}'\varkappa = \mathbf{Q}'(q'\varkappa)$, pre každé $q' \in \mathbf{Q}'$.

Vo všeobecnosti nemusí byť splnené ani a) ani b). Pýtajme sa, aké musí byť $\mathbf{Q}$, aby bol možný rozklad v triedy mod $\mathbf{Q}'$ pre každú čiastočnú kvazigrupu $\mathbf{Q}'$ kvazigrupy $\mathbf{Q}$. Odpoveď (Ore-Hausmann [1]): Nutná a dostačujúca podmienka pre to, aby to bolo možné, je: každé tri elementy $a, b, c \in \mathbf{Q}$ splňujú vzťah $a \,.\, (bc) = \alpha \,.\, c$, kde je $\alpha \in \{a, b\}$.[7])[8])

Táto *zoslabená forma asociatívneho zákona* je typickou ukázkou, ako možno v kvazigrupách obnoviť platnosť známych viet z teórie grúp. Rôzne formy zoslabeného asociatívneho zákona majú ovšem rôzny dosah a takto možno študovať i akúsi „hierarchiu dosahu" rôznych náhražok asociatívneho zákona (Ore-Hausmann [1], Suškevič [5]).

V téorii grúp hrá rozhodujúcu úlohu pojem *normálneho deliteľa*. Pokúsime sa tento pojem previesť do teórie kvazigrúp. Poznamenajme ihneď, že toto je *najdôležitejší problém* o kvazigrupách, ktorému je venovaných mnoho prác. (Albert [1], [2], Baer [3], [4], Bates [1], [2], Bates-Kiokmeister [1], Bruck [1], Garrison [1], [2], Kiokmeister [1], Smiley [1], Zelinsky [1]).

Ponúka sa nám definícia: $\mathbf{N}$ je normálne, ak platí $a\mathbf{N} = \mathbf{N}a$ pre každé $a \in \mathbf{Q}$. Táto definícia je nevhodná, lebo i keď existuje rozklad v triedy

$$\mathbf{Q} = \mathbf{N}a + \mathbf{N}b + \mathbf{N}c + \ldots$$

(a na to je treba istých slabých foriem asoc. zákona), nemusia tieto triedy tvoriť ani grupoid, tým menej kvazigrupu. Teda by sa stratily najzákladnejšie vlastnosti tohto pojmu. Okrem toho chceme vybudovať

[6]) Bruck [4] uvažuje i v obecnom grupoide množiny podobných typov, ktoré nazýva asociátormi.

[7]) To znamená: patrí do grupoidu vytvoreného elementami a, b.

[8]) Keď pre konečné $\mathbf{Q}, \mathbf{Q}'$ možno písať rozklad tvaru (1) splňujúci podmienku a), platí zrejme i Lagrangeova veta: rad $\mathbf{Q}'$ delí rad $\mathbf{Q}$. (Toto neplatí ale už napr. pre pologrupy.)

teóriu normality čo možno obecných kvazigrúp, v ktorých nebudeme predpokladať platnosť žiadnej formy asociatívneho zákona.

Ponúka sa nám — ako východisko — pojem homomorfizmu. U grúp — ako vieme — každá normálna podgrupa indukuje istý homomorfizmus (totiž na faktorovú grupu); a naopak, každý homomorfizmus možno dostať takýmto spôsobom.

Podívajme sa najprv trošku ako vypadá homomorfný obraz kvazigrupy $\mathbf{Q}$. Je ním grupoid $\mathbf{Q}'$, v ktorom majú rovnice $a'x = b'$, $ya' = b'$ riešenie. Keďže tieto rovnice nemusia mať *jediné* riešenie, nemusí byť $\mathbf{Q}'$ obecne kvazigrupa.[9])

Majme teraz ale kvazigrupu $\mathbf{Q}$, ktorá je homomorfne zobrazená na nejakú kvazigrupu $\mathbf{Q}'$. Nech je $a' \in \mathbf{Q}'$. Nech $\mathbf{A}$ je súhrnom originálov patriacich k a'. Per analogiam s teóriou grúp sme vedení k tejto definícii: ak množina $\mathbf{A}$ je sama kvazigrupou, nazvime ju normálnym deliteľom kvazigrupy $\mathbf{Q}$. Teda $\mathbf{N}$ je normálnym deliteľom v $\mathbf{Q}$, ak existuje taký homomorfizmus $\mathbf{Q} \to \mathbf{Q}'$, že $\mathbf{N}$ má za svoj obraz jediný element kvazigrupy $\mathbf{Q}'$. (Podľa takéhoto $\mathbf{N}$ možno tvoriť triedy a tieto tvoria grupoid, ktorý je kvazigrupou.)

Je tu však veľká nevýhoda proti teórii grúp. Homomorfizmy a norm. delitelia si *neodpovedajú* vzájomne *jedno-jednoznačne*. Každým homomorfizmom nemusí byť definovaný nejaký normálny deliteľ a na druhej strane môže jeden homomorfizmus definovať i viac normálnych deliteľov.

Tieto ťažkosti odpadnú v jednom veľmi dôležitom prípade, totiž u kvazigrúp *majúcich jednotkový element*. To je tak dôležitý prípad kvazigrúp, že dostal v anglosaskej literatúre zvláštny názov: *loop*.

Nech $\mathbf{Q}$ je kvazigrupa s jednotkou, ktorá je homomorfne zobrazená na nejakú kvazigrupu $\mathbf{Q}'$.[10]) Množinu $\mathbf{N}$ všetkých elementov $\in \mathbf{Q}$, ktorých obrazom je e' (jednotkový element $\mathbf{Q}'$), nazvime *jadrom* daného *homomorfizmu*. Potom platí táto veta:

a) Faktorový grupoid $\mathbf{Q} \mid \mathbf{N}$ je kvazigrupa izomorfná s kvazigrupou $\mathbf{Q}'$. (Pritom faktorový grupoid tvoríme obvyklým spôsobom pomocou tried.)

b) Každý homomorfizmus kvazigrupy $\mathbf{Q}$ s jednotkou na nejakú kvazigrupu $\mathbf{Q}'$ dostaneme týmto spôsobom.

Definujeme teda: $\mathbf{N}$ je normálnym deliteľom kvazigrupy s jednotkou $\mathbf{Q}$, keď je jadrom akéhosi homomorfizmu $\mathbf{Q} \to \mathbf{Q}'$. Homomorfizmy a normálni delitelia si *odpovedalú jedno—jednoznačne*.[11]) [12])

[9]) Je to ale napr. iste kvazigrupa, ak $\mathbf{Q}'$ je konečné.

[10]) Kvazigrupa $\mathbf{Q}'$ má potom samozrejme tiež jednotku. Možno sostrojiť i kvazigrupu s jednotkou, ktorej homomorfným obrazom nie je kvazigrupa (BATES-KIOKMEISTER [1]).

[11]) Normálny deliteľ kvazigrupy s jednotkou sa dá definovať i inak. Napr. touto rovnocennou definíciou. Je to množina $\mathbf{N}$, ktorá splňuje pre každé $x, y \in \mathbf{Q}$ vzťahy $x(y\mathbf{N}) = (xy)\mathbf{N} = (\mathbf{N}x)y$.

[12]) Z týchto vývodov je vidieť, že existencia jednotky narobí v kvazigrupe podstatné zmeny. Je tomu práve naopak ako u pologrúp, kde existencia jednotkového elementu nie je pre väčšinu úvah podstatná (naopak, je skôr „škodlivá").

Teória kvazigrúp s jednotkou je neobyčajne *podobná teórii grúp*. Platí totiž veta. Množina normálnych deliteľov kvazigrupy s jednotkou tvorí modulárny sväz (s obvyklými sväzovými operáciami). Z toho plynie, že pre normálnych deliteľov platia vety o izomorfizme a vety Jordan-Hölderove i v Zassenhausovom zovšeobecnení, ktoré sa dokážu použitím Ore-ho postupu platného pre ľubovoľné čiastočne usporiadané množiny.

Teóriu normality možno vybudovať i pre kvazigrupy bez jednotkového elementu. Výsledky však nie sú už tak prehľadné (GARRISON [1], [2]; KIOKMEISTER [1]).

4.

Prv ako skončíme o kvazigrupách, spomeňme ešte aspoň, aké *ďalšie problémy* sú už čiastočne rozriešené.

Je to napr. teória abelových kvazigrúp, teória konečných kvazigrúp, rôzne typy špeciálnych kvazigrúp (viď hlavne BRUCK [4]). Ponúka sa teória jednoduchých kvazigrúp, špeciálne kvazigrúp s jednotkou (ALBERT [2], BRUCK [3]). Tak budeme nazývať kvazigrupu, ktorá neobsahuje vlastnú čiastočnú kvazigrupu (okrem e). Z tohto oboru aspoň jeden malý výsledok. Dá sa dokázať na príklade, že pre každé konečné $n \neq 4$ existujú jednoduché kvazigrupy s jednotkou. To je výsledok iste pozoruhodný, ak ho konfrontujeme s problémom jednoduchých grúp. Týchto je — ako vieme — pomerne „málo“.[13])

ALBERT ([1], [2]) zaviedol dôležitý pojem *izotopie*. Tento pojem zovšeobecňuje pojem izomorfie a umožňuje z jednotného hľadiska dokázať celý rad rôznorodých viet nielen o kvazigrupách, ale i o neasociatívnych systémoch vôbec. Nedostatok miesta mi bráni zaoberať sa ním bližšie.

III. Pologrupy.

Pologrupou nazývame grupoid, v ktorom je splnený axióm A 2.

Všimnime si najprv, v čom sa pologrupa *podobá* grupe.

a) Keďže $a(bc) = (ab)c$, má smysel hovoriť o mocninách $a^2, a^3, a^4, \ldots$

b) Každý podgrupoid pologrupy je sám pologrupou. Napr. všetky mocniny elementu a tvoria tzv. *cyklickú* pologrupu $\{a\}$.

c) Každá konečná pologrupa radu n je izomorfná s pologrupou „substitúcií“ typu $\begin{pmatrix} 1, 2, \ldots, n \\ i_1, i_2, \ldots, i_n \end{pmatrix}$. Tieto sa líšia od známych permutácií tým, že v „menovateli“ vystupujúce čísla $i_1, i_2, \ldots, i_n$ sú síce z množiny $1, 2, \ldots, n$, niektoré však môžu chýbať, iné vystupovať viackrát.[14])

[13]) Ostatne dá sa dokázať celkom elementárne, že všetky kvazigrupy s jednotkou radu $\leqq 4$ sú grupy.

[14]) Pritom je násobenie definované ako u permutácií a dôkaz plynie z Cayley-ho tabuľky ako u grúp. To sa dá rozšíriť i na pologrupy so *spočítateľne* mnoho elementami (SUŠKEVIČ [1], [3], [4], [6], [12]).

Podívajme sa teraz, v čom sa *odlišuje* pologrupa od grupy.

a) Pologrupa môže mať viac alebo i nekonečne mnoho tzv. *idempotentných* elementov (t. j. elementov, pre ktoré platí $e^2 = e$). Napr. ľavé (pravé) jednotky sú také. Ale idempotent nemusí byť jednotkou.

b) Pologrupa $\boldsymbol{P}$ môže, ale nemusí mať tzv. *nulový element*, t. j. element z, pre ktorý platí $az = za = z$ pre každé $a \in \boldsymbol{P}$. Ak existuje, je len jediný.

c) Dve čiastočné pologrupy môžu mať prázdny prenik. (Ak je neprázdny, je to ovšem pologrupa).

d) V pologrupe nemusí platiť „pravidlo o krátení" (t. j. $ax = bx$ neimplikuje obecne $a = b$).

e) Všimnime si konečne cyklickej pologrupy

$$\{a, a^2, a^3, \ldots\}.$$

V tejto pologrupe sú buď všetky elementy navzájom rôzne, alebo existujú dve celé čísla $0 < m < n$, že je $a^m = a^n$. Voľme za n najmenšie takéto možné číslo. Elementy sa potom opakujú v tomto poradí

$$a, a^2, \ldots, a^{m-1} \mid a^m, \ldots, a^{n-1} \mid a^m, \ldots, a^{n-1} \mid \ldots \qquad (2)$$

Hovoríme, že a je konečného radu a číslo $m - 1$ voláme dĺžkou *predperiódy*. Existencia predperiódy je niečo, čo u grúp nie je možné.

1.

Položme si túto otázku: Môže mať pologrupa $\boldsymbol{P}$ čiastočnú pologrupu, ktorá je sama grupou?[15])

Odpoveď je ľahká. — K tomu je nutné a stačí, aby v $\boldsymbol{P}$ existovaly idempotentné elementy. Každý idempotent e je sám — i keď triviálnym spôsobom — grupou. Budú nás zrejme zaujímať *maximálne grupy*.[16]) Ľahko nahliadneme: ku každému idempotentu e existuje jediná maximálna grupa $\boldsymbol{G}_e$, ktorá má e za jednotkový element.

Idempotenty — a teda grupy — existujú napr. vždy, keď pologrupa má nejaký element konečného radu. Je totiž skoro bezprostredne vidieť, že v postupnosti (2) tvoria elementy $a^m, a^{m+1}, \ldots, a^{n-1}$ cyklickú grupu, ktorej jednotkovým elementom je idempotent a^{n-1}.

Vynorujú sa dve otázky: (Clifford [4], Schwarz [1], Poole [1]).

a) Kedy sú maximálne grupy disjunktné? To nastane napr., keď každý element pologrupy $\boldsymbol{P}$ je konečného radu.[17])

b) Kedy súhrn maximálnych grúp vyčerpá celé $\boldsymbol{P}$? Na to je opäť

[15]) Slabšou formou tohto problému je napr., či — a kedy — možno nájsť čiastočné systémy, v ktorých platí „pravidlo o krátení".

[16]) T. j. také, ktoré nie sú vlastnou časťou nejakej inej grupy z $\boldsymbol{P}$. Ak v $\boldsymbol{P}$ existuje nulový element z, je tento sám o sebe maximálnou grupou.

[17]) Špeciálne tedy napr. v konečnej pologrupe.

jednoduchá odpoveď, ak každé element ϵP je konečného radu. Potom to nastane vtedy a len vtedy, keď žiadny element nemá predperiody.

Pologrupy, ktoré sú *súčtom disjunktných grúp*, hrajú v teórii pologrúp, ako uvidíme, fundamentálnu úlohu.

2.

V teórii pologrúp pristupuje nový faktor, ktorý v grupách ani v kvazigrupách nemá analogie — totiž pojem *ideálu*.

Množinu I nazývame ľavým ideálom z P, ak platí $PI \subseteq I$. Podobne sa definuje pravý a obojstranný ideál.

Každý ideál je čiastočnou pologrupou z P. (P a z — ak existuje — sú obojstranné ideály.) Prenik dvoch ideálov (ak je neprázdny) a spojová množina dvoch ideálov je opäť ideál.

Z teorie hyperkomplexných čísel je známe, akú dôležitú úlohu hrajú ideály pre vyšetrenie ich štruktúry. Je preto prirodzené, že sa pokúsime — a to s úspechom — preniesť odtiaľ niektoré pojmy do teórie pologrúp.

Prvým takým pojmom je pojem *minimálneho ideálu*. Hovoríme, že I je minimálny ľavý ideál, ak neexistuje taký ľavý ideál I', že je $I' \subset I$. Podobne sa definuje minimálny pravý a min. obojstranný ideál.[18]) Ľahko sa dokáže: a) Každé minimálne ľavé (pravé) ideály sú disjunktné. b) Ak existuje obojstranný min. ideál, existuje taký len jediný.[19])

O štruktúre min. ľavých (pravých) ideálov možno povedať toto. Minimálny ľavý ideál I je pologrupa, v ktorej má rovnica $xa = b$ vždy riešenie. Vtedy a len vtedy, keď má I aspoň jeden idempotent, je toto riešenie *jednoznačné*. Potom je I súčtom disjunktných grúp. (CLIFFORD [1], [6], SCHWARZ [1]).[20]) [21])

Pýtajme sa, aký je súvis medzi minimálnymi ľavými ideálmi a minimálnym obojstranným ideálom n.

V pologrupách, ktoré majú nulový element, je takto kladená otázka nezaujímavá. Predpokladajme preto na chvíľku, že P nemá nulový element.

a) Predpokladajme najprv, že P má aspoň jeden min. ľavý ideál I. Potom sa ukáže: *každý* min. ľavý ideál sa dá písať v tvare $I_a = I \cdot a$ (s vhodne zvoleným a) a n je súčtom všetkých minimálnych ľavých ideálov: $n = \sum_a I_a$.

---

[18]) V každej pologrupe *nemusí existovať* min. ideál. Napr. pologrupa rac. celých čísel s obvyklou definíciou násobenia nemá zrejme min. ideál. V postupnosti ideálov $\{1, 2, 3, \ldots\} > \{2, 4, 6, \ldots\} > \{4, 8, 12, \ldots\} >$ neexistuje žiadny minimálny. Kedykoľvek hovoríme o min. ideále, predpokladáme samozrejme, že taký existuje.

[19]) Keď P má nulový element z, je ním zrejme $\{z\}$.

[20]) Podobne to platí ovšem pre min. pravé ideály.

[21]) Pologrupa, v ktorej má každá rovnica $xa = b$ jediné riešenie, nazýva sa *l'avostrannou* grupou. Taká je vždy súčtom disjunktných grúp (CLIFFORD [1], Sušk evič [3]).

b) Predpokladajme naviac, že P má aspoň jeden min. ľavý ideál l a aspoň jeden minimálny pravý ideál r. Potom možno písať

$$n = \sum_a l_a, \quad n = \sum_b r_b$$

$$n = n^2 = \sum_a r_a \,.\, \sum_b l_b = \sum (r_a \,.\, l_b) = \sum (r_a \cap l_b) = \sum g_{ab}.$$

Dá sa ukázať 1. $g_{ab} \neq \emptyset$ je grupa, 2. v napísanom rozklade sú všetky sčítance disjunktné. Teda i n je súčtom disjunktných grúp. (Clifford [6]).

c) Podobná veta sa dá dokázať i za iných podmienok. Ak napr. každý element je konečného radu, stačí žiadať iba existenciu aspoň jednoho min. ľavého ideálu. Potom, nielen že n je súčtom disjunktných grúp, ale dokonca sú všetky grupy g_{ab} izomorfné (Schwarz [1]).

Ak existuje jediný min. pravý a jediný min. ľavý ideál (ako je tomu napr. u komutatívnych pologrúp) je n grupou.

Pologrupy, ktoré majú takú štruktúru, ako min. obojstranný ideál n z odstavca b), nazvime *Suškevičovho typu*. Dôležité je, že o takýchto pologrupách možno získať *úplný prehľad*. Ako, to si teraz krátko vyložíme. (Rees [1], [2]).

Majme ľubovoľnú grupu G a pridajme k nej nulový element 0. Sostrojme si všetky také $L \,.\, K$, matice, ktorých elementami sú prvky z $G + 0$ a ktoré majú iba na jedinom mieste element rôzny od nuly. Matica, ktorá má element $a \in G$ na mieste i, k nech je $(a)_{ik}$. Túto množinu matíc urobím pologrupou tým, že definujem medzi nimi násobenie $\odot$ takto. Vezmem si ešte pevnú $K \,.\, L$ maticu $M = (p_{ik})$, ktorej elementami sú opäť prvky z G všetky $\neq 0$. Potom nech je

$$(a)_{ik} \odot (b)_{ln} = (a)_{ik} \,.\, M \,.\, (b)_{ln} = (a p_{kl} b)_{in},$$

kde napravo je obyčajné násobenie matíc.

Dá sa dokázať, že takto vzniklá pologrupa je Suškevičovho typu. Naopak (a to je *dôležitejšie*!) každá pologrupa P Suškevičovho typu je izomorfná s akousi pologrupou matíc vytvorených takýmto spôsobom. (Pritom za grupu G stačí vziať grupu ePe, kde e je ľubovoľný idempotent.)

Podľa analogie s teóriou hyperkomplexných čísel nazývame pologrupu *jednoduchou*, ak neobsahuje vlastný obojstranný ideál s výnimkou možného nulového elementu. Z práve dokázaného plynie: Ovládame dokonale *štruktúru jednoduchých pologrúp bez nulového elementu*, ktoré majú aspoň jeden minimálny ľavý a pravý ideál.

Podobne možno ovládnuť pomocou matíc a horeuvedenej konštrukcie i širšiu triedu pologrúp, majúcich poprípade i nulový element, tzv. *kompletne jednoduché pologrupy*. (Naša pologrupa Suškevičovho typu je špeciálnym prípadom kompletne jednoduchých pologrúp.) (Clifford [4], [5], [6]; Rees [1], [2]; Stoll [1]).

3.

Naznačíme ešte *niekoľko ďalších* problémov z teórie pologrúp.

Pre celú algebru dôležitou otázkou je problém *vnorenia pologrupy* do grupy.

Je daná pologrupa $\boldsymbol{P}$. Pýtame sa: existuje grupa $\boldsymbol{G}$, ktorá by obsahovala pologrupu $\boldsymbol{P}'$ izomorfnú s našou pologrupou $\boldsymbol{P}$? Krátko: existuje grupa $\boldsymbol{G}$, do ktorej možno vnoriť našu pologrupu $\boldsymbol{P}$?

Aby to bolo možno, musí ovšem v $\boldsymbol{P}$ platiť „pravidlo o krátení zprava i zľava", t. j. každý zo vzťahov $ax = bx$, $ya = yb$ implikuje $a = b$.

Malcev ([1], [2], [3]) ukázal už v roku 1936, že táto podmienka nie je postačujúca. V roku 1940 udal nutné a postačujúce podmienky, kedy to je možné. Tieto majú takýto tvar: isté reťazce rovníc implikujú platnosť ďalších rovníc. A takých implikácií je nekonečne mnoho. To je veľmi komplikované. Je preto zaujímavé nájsť aspoň, čo možno obecné, postačujúce podmienky. Tým sa podrobne zaoberal P. Dubreill [3], [4] (viď ďalej M. L. Dubreill-Jacotin [1], Vandiver [1]). Napr. sa ľahko ukáže, že pologrupa $\boldsymbol{P}$, pre ktorú platia nasledujúce dve podmienky, sa dá vnoriť do grupy. 1. Platí „pravidlo o krátení". 2. Ku každým dvom elementom a, b existujú dva také iné elementy x, y, že $ax = by$ (t. j. každé dva elementy majú spoločný násobok).[22])

Postup dôkazu je celkom elementárny a analogický známej metóde zavedenia rac. čísel pomocou dvojíc celých čísel. Ľahko sa dokáže, že takto sostrojená grupa je najmenšou grupou majúcou žiadanú vlastnosť.

Problém vnorenia nie je možno ani po Malcevových výsledkoch považovať prirodzene ešte za rozriešený.

4.

Iným dôležitým problémom je otázka *normálnych deliteľov*, *homomorfizmov* a *faktorovej pologrupy* danej pologrupy.

Týmito otázkami sa zaoberal opäť veľmi podrobne Dubreill ([2], [4]). Budem ale radšej referovať o metóde Liapina [4], ktorá sa mi zdá byť priamejšia.

Nemá smyslu opäť definovať normálneho deliteľa $\boldsymbol{N}$ pomocou vzťahu $a\boldsymbol{N} = \boldsymbol{N}a$. Podáme Liapinovu definíciu, ktorá umožňuje homomorfné zobrazenie pologrupy na pologrupu.

Nech $\boldsymbol{P}$ má jednotkový element. Čiastočnú pologrupu $\boldsymbol{N}$ budeme nazývať normálnou v $\boldsymbol{P}$, ak platí toto: $a\boldsymbol{N}b \subseteq \boldsymbol{N}$ platí vtedy a len vtedy, keď platí $ab \in \boldsymbol{N}$ (a to pre každé $a, b \in \boldsymbol{P}$).[23])

[22]) Špeciálnym prípadom takýchto pologrúp sú komutatívne pologrupy, ktoré sa teda vždy dajú vnoriť do grupy. [Uvedená veta pochádza v podstate od Ore-a].

[23]) T. j. ab a $a\boldsymbol{N}b$ buď súčasne patria alebo nepatria do $\boldsymbol{N}$.

Ak $\boldsymbol{P}$ je grupou, je každá množina tejto vlastnosti normálnou podgrupou a naopak.

Platí:

a) Nech $\boldsymbol{P}$ je homomorfne zobrazené na nejakú pologrupu $\boldsymbol{P}'$.

Potom jadro homomorfizmu[24]) je normálnym deliteľom pologrupy $\boldsymbol{P}$.

b) Naopak: Nech $\boldsymbol{N}$ je ľubovoľný normálny deliteľ pologrupy $\boldsymbol{P}$. Potom existuje homomorfizmus Σ pologrupy $\boldsymbol{P}$ na akúsi pologrupu $\boldsymbol{P}'$ a to taký, že $\boldsymbol{N}$ je presne jadrom homomorfizmu Σ.

Toto druhé tvrdenie dokážeme tak, že si sostrojíme priamo faktorovú pologrupu $\boldsymbol{P} \mid \boldsymbol{N}$. Túto nevytvoria ale triedy tvaru $\boldsymbol{N} \,.\, a$! Zavedieme si ekvivalenciu takto. Budeme písať $x \equiv y \pmod{\boldsymbol{N}}$, ak existujú také elementy $x_1, x_2, y_1, y_2 \in \boldsymbol{P}$, $n_1, n_2 \in \boldsymbol{N}$, že $x = x_1 x_2$, $y = y_1 y_2$, $x_1 n_1 x_2 = y_1 n_2 y_2$. Ľahko sa dokáže, že táto ekvivalencia definuje regulárny rozklad v triedy, pričom je $\boldsymbol{N}$ samo triedou. Vo faktorovej pologrupe $\boldsymbol{P} \mid \boldsymbol{N}$ je $\boldsymbol{N}$ jednotkovým elementom.

5.

Posledný problém, ktorý tu spomenieme, je *aritmetika pologrúp*.

V pologrupe možno definovať deliteľnosť, jednotky, nerozložiteľný element, atď., podobne ako v elementárnej teórii čísel. Nemôže byť ovšem vo všeobecnosti reči o *jednoznačnosti* rozkladu elementu v súčin nerozložiteľných elementov. Problémom je, aké vlastnosti musí spĺňovať pologrupa, aby takýto rozklad bol jednoznačný. Inak tiež: aké musí mať vlastnosti pologrupa, aby sa dala vnoriť do pologrupy, v ktorej je táto podmienka splnená. To je v podstate tá istá otázka ako v algebraickej teórii čísel, kde zavedením ideálnych elementov vynútime jednoznačnosť rozkladu. Tam postupujeme tak, že pologrupu hlavných ideálov oboru integrity celých čísel vnoríme do pologrupy všetkých ideálov. I v Dedekindovej teórii tvoria ideály iba pologrupu a nie okruh (dajú sa násobiť, ale nie sčítať). Z toho sa dá súdiť, že docielenie jednoznačnosti je problém multiplikatívny a ideály dávajú kľúč k rozriešeniu tejto otázky.

Skutočne sa podarilo vhodným rozšírením pojmu ideál[25]) dosiahnúť veľmi dobrej analogie s teóriou celých čísel a ideálov algebraických číselných telies. (Arnold [1], Clifford [2], [3], Lorenzen [1]). Napr. sa podarilo udať pomocou ideálov kritéria, za ktorých platí v pologrupe veta o jednoznačnosti rozkladu v súčin nerozložiteľných elementov. Podarilo sa to dokonca čiastočne i pre nekomutatívne pologrupy. (Kawada-Koiti [1]).

---

[24]) T. j. množina elementov, ktorých obrazom je jednotkový element $e' \in \boldsymbol{P}'$.

[25]) Rozšírenie, ktoré v sebe obsahuje dedekindovské ideály ako špeciálny prípad.

IV. Multigrupy.

Prenikavé zovšeobecnie pojmu grupy dostaneme takto.

Nech $\boldsymbol{M}$ je množina, v ktorej je definované násobenie. Nechajme padnúť axióm A 1 a nahraďme ho axiómom:

B 1. Súčin dvoch elementov množiny $\boldsymbol{M}$ je podmnožina z $\boldsymbol{M}$:

$$a \,.\, b = \{c_1, c_2, c_3, \ldots\}.$$

Množina, ktorá splňuje axióm B 1 a nič viac, sa volá *multigrupoidom*.

Multigrupou nazývame multigrupoid, v ktorom sú nadto splnené tiety dva ďalšie axiómy:

B 2. Zákon asociatívny: $a(bc) = (ab)c$.

B 3. (Axióm existencie podielu.) Ku každým dvom elementom a, b existujú dva také elementy x, y, že platí

$$ax \supset b, \quad ya \supset b.$$

Vznik tohto pojmu (Márty [1]) sa datuje z tohto jednoduchého príkladu. Nech

$$\boldsymbol{G} = \boldsymbol{H} + \boldsymbol{H}a + \boldsymbol{H}b + \ldots$$

je rozklad nejakej grupy $\boldsymbol{G}$ modulo $\boldsymbol{H}$ v pravé triedy. Systém tried tvorí multigrupu, ak súčinom tried

$$\boldsymbol{H}a \,.\, \boldsymbol{H}b = \{\boldsymbol{H}c_1, \boldsymbol{H}c_2, \boldsymbol{H}c_3, \ldots\},$$

rozumieme tú množinu tried $\boldsymbol{H}c_i$, ktoré obsahujú elementy súčinu z ľavej strany[26].)

V multigrupách možno zaviesť rad obvyklých pojmov (Ore-Dresher [1]). Tak napr. element e voláme ľavou (pravou) *jednotkou*, ak platí $ea \supset a$ ($ae \supset a$). Jednotkou voláme element, pre ktorý sú splnené súčasne oba tieto vzťahy. *Absolútnou jednotkou* voláme element, ktorý splňuje dokonca $ae = ea = a$ (pre každé $a \in \boldsymbol{M}$).

Prvý nápadný rozdiel voči grupám je, že multigrupa nemusí mať vôbec žiadnu jednotku žiadneho druhu, alebo každý jej element môže byť jednotkou určitého druhu.

1.

Aké vety platia pre multigrupy? Odpoveď na túto otázku osvetlí *dosah* axiómu A 1. Je prekvapujúce, že analogie s teóriou grúp sú pomerne dost ďalekosiahle.

Prvá celkom jednoduchá otázka je táto. Nazvime element α *skalárnym*, keď pre každé $x \in \boldsymbol{M}$ sa súčiny $x \,.\, \alpha$, $\alpha \,.\, x$ rovnajú jedinému elementu z $\boldsymbol{M}$. Čo možno povedať o množine skalárnych elementov?

[26]) Ak $\boldsymbol{H}$ je normálnym deliteľom $\boldsymbol{G}$, máme ovšem grupu.

Ľahko sa dokáže: nutná a postačujúca podmienka pre to, aby existovaly skalárne veličiny, je: existuje absolútna jednotka e. Množina všetkých skalárnych elementov tvorí potom grupu, ktorá má e za jednotkový element.[27]) (Ore-Dresher [1]).

2.

Iná dôležitejšia otázka je táto. Nech $\boldsymbol{N}$ je čiastočnou multigrupou multigrupy $\boldsymbol{M}$. Kedy je možný rozklad tvaru

$$\boldsymbol{M} = \boldsymbol{N}a + \boldsymbol{N}b + \boldsymbol{N}c + \ldots ? \tag{3}$$

K tomuto účelu je výhodné zaviesť tento pojem. Čiastočnú multigrupu $\boldsymbol{N}$ nazývame *zprava reverzibilnou* v $\boldsymbol{M}$, ak vzťah $a_1 \subset a_2 n'$, $n' \in \boldsymbol{N}$ implikuje $a_2 \subset a_1 n''$, $n'' \in \boldsymbol{N}$ (pre každé $a_1, a_2 \in \boldsymbol{M}$).

Potom sa ľahko dokáže: Rozklad v disjunktné triedy tvaru (3) existuje vtedy a len vtedy, keď $\boldsymbol{N}$ je reverzibilné v $\boldsymbol{M}$. Potom naviac každý element triedy $\boldsymbol{N}a$ vytvoruje triedu $\boldsymbol{N}a$. Jedna z tried v (3) je $\boldsymbol{N}$ samotné. V rozklade (3) možno považovať triedy za elementy novej multigrupy $\boldsymbol{M} \mid \boldsymbol{N}$, tzv. ľavej *faktorovej multigrupy*. Pritom je násobenie definované obvyklým spôsobom, totiž (v ľahko pochopiteľnej symbolike)

$$\boldsymbol{N}a \,.\, \boldsymbol{N}b = \{\boldsymbol{N}c_1, \boldsymbol{N}c_2, \ldots\}.$$

Je to naozaj multigrupa a nie iba multigrupoid.

3.

Je celkom prirodzeným pokúsiť sa o definíciu *normálneho deliteľa*. Analogia s teóriou grúp je tak silná, že sa tentoraz hodí definícia: $\boldsymbol{N}$ voláme normálnym deliteľom multigrupy $\boldsymbol{M}$, ak pre každé $a \in \boldsymbol{M}$ platí $a\boldsymbol{N} = \boldsymbol{N}a$.

Ak $\boldsymbol{N}$ je normálne a reverzibilné, je ľavá a pravá faktorová multigrupa totožná.

Majme multigrupu, ktorá má nejakú jednotku (napr. ľavú alebo pravú jednotku). Uvažujme množinu všetkých normálnych a súčasne reverzibilných čiastočných multigrúp. Tieto tvoria *sväz*, pričom sväzovými operáciami rozumieme tvorenie preniku a spojovej množiny. Tento sväz je dokonca *modulárny*. Teda možno dokázať vety o izomorfizme a napr. Jordan-Hölderovu vetu, ktorá má toto znenie. Reťazec multigrúp

$$\boldsymbol{A} \supset \boldsymbol{A}_1 \supset \ldots \supset \boldsymbol{A}_n = \boldsymbol{B},$$

voláme kompozičným, ak každé $\boldsymbol{A}_i$ je normálne a reverzibilné v predošlom. Potom platí: každé dva maximálne kompozičné reťazce medzi $\boldsymbol{A}$

[27]) Túto vetu možno postaviť napr. po bok vete o asociatívnych elementoch v kvazigrupe, alebo vetám o grupách v pologrupe.