B-POLOGRUPY

JURAJ BOSÁK, Bratislava

V práci sa študujú také pologrupy, v ktorých zjednotením ľubovoľných dvoch čiastočných pologrúp je opäť pologrupa. Zvlášť sa vyšetrujú niektoré špeciálne prípady: prípad cyklickej pologrupy a prípad grupy.

1. Úvod*

Pod pologrupou rozumieme množinu (prázdnu alebo neprázdnu), na ktorej je definovaná binárna asociatívna operácia. Pre zjednodušenie označovania nebudeme rozlišovať medzi touto množinou a príslušnou pologrupou. Pod čiastočnou pologrupou pologrupy S rozumieme takú podmnožinu množiny S, ktorá vzhľadom na operáciu v S tvorí tiež pologrupu. Pologrupa sa nazýva komutatívna, ak príslušná operácia je komutatívna, v opačnom prípade sa nazýva nekomutatívna. V ľubovoľnej pologrupe S zavádzame obvyklým spôsobom prirodzenú mocninu a^n prvku $a \in S$, pričom platia pravidlá $a^m . a^n = a^{m+n}$, $(a^m)^n = a^{mn}$, a v komutatívnej pologrupe $(ab)^n = a^n b^n$ ($a \in S$, $b \in S$, m, n sú prirodzené čísla). Prvok $x \in S$, pre ktorý $x^2 = x$, nazývame idempotentom. Množinu tých prvkov $x \in S$, ktoré sa v postupnosti $\{a^n\}_{n=1}^{\infty}$ ($a \in S$) vyskytujú práve raz, nazývame predperiódou prvku a. Kardinálne číslo predperiódy nazývame dĺžkou predperiódy a označujeme $q(a)$. Množinu tých prvkov $x \in S$, ktoré sa v postupnosti $\{a^n\}_{n=1}^{\infty}$ ($a \in S$) vyskytujú aspoň dva razy (a teda nekonečne mnohokrát), nazývame periódou prvku a. Kardinálne číslo periódy nazývame dĺžkou periódy a označujeme $r(a)$; ak je rôzna od nuly, nazývame ho rádom prvku a a hovoríme, že prvok a má konečný rád; v opačnom prípade hovoríme, že prvok a má nekonečný rád.

Nech $a \in S$, $m \neq n$. Potom $a^m = a^n$ platí práve vtedy, keď platí súčasne: $m > q(a)$, $n > q(a)$, $m \equiv n \pmod{r(a)}$. Ak $r(a) \neq 0$, v postupnosti $\{a^n\}_{n=1}^{\infty}$ existuje práve jeden idempotent. Vtedy hovoríme, že prvok a patrí k tomuto idempotentu. Množinu všetkých prvkov pologrupy S, ktoré patria k idempotentu $e \in S$, označujeme K_e a nazývame K-triedou, príslušnou k idempotentu e. Vlastnosti K-tried sa skú-

* Okrem niektorých názvov, ktoré sú tu použité po prvý raz (pozri definíciu 1 až 4), používam mnohé termíny, bežne sa vyskytujúce v literatúre (porovnaj napr. [1], [3]); vzhľadom na isté menšie významové rozdiely a v záujme prehľadnosti práce uvádzam stručne aj definície niektorých známych pojmov.

mali napr. v prácach [3, 5, 6]. Periodickou pologrupou nazývame takú pologrupu, v ktorej každý prvok má konečný rád. V tomto prípade je pologrupa zjednotením navzájom disjunktných K-tried.

Je zrejmé, že prienikom ľubovoľného systému čiastočných pologrúp danej pologrupy je opäť pologrupa. Prirodzene, analogické tvrdenie pre zjednotenie pologrúp neplatí všeobecne, ale len v niektorých špeciálnych prípadoch, ktorými sa budeme v ďalšom zaoberať.

Vyjdime od ľubovoľnej pologrupy S a od jej podmnožiny M (t. j. $M \subseteq S$). Označme $\overline{M}$ prienik všetkých pologrúp T takých, že $M \subseteq T \subseteq S$. Zrejme $\overline{M}$ je — v istom zmysle — najmenšou pologrupou, obsahujúcou množinu M. Takýmto spôsobom každej podmnožine M množiny S je priradená iná podmnožina $\overline{M}$ množiny S, ktorá pri uvedenej operácii tvorí pologrupu.* Pritom zrejme pre ľubovoľné $A \subseteq S$, $B \subseteq S$ platí:

$$(1) \quad A \subseteq \bar{A},$$

$$(2) \quad A \subseteq \bar{B} \Rightarrow \bar{A} \subseteq \bar{B},$$

$$(3) \quad \bar{\emptyset} = \emptyset,$$

$$(4) \quad \bar{S} = S,$$

$$(5) \quad \bar{\bar{A}} = \bar{A},$$

$$(6) \quad A \subseteq B \Rightarrow \bar{A} \subseteq \bar{B},$$

$$(7) \quad \overline{A \cap B} \subseteq \bar{A} \cap \bar{B},$$

$$(8) \quad \overline{A \cup B} \supseteq \bar{A} \cup \bar{B}.$$

Zrejme podmienka, že A je čiastočnou pologrupou pologrupy S, môže sa pri našom označení vyjadriť takto: $\bar{A} = A (A \subseteq S)$. Ďalej pre ľubovoľné $a \in S$ je $\overline{\{a\}}$ zhodné s množinou všetkých členov postupnosti $\{a^n\}_{n=1}^{\infty}$; túto množinu budeme označovať $\{a^n \mid n \geq 1\}$. Pologrupu, ktorú možno písať v takomto tvare (ako mocniny istého jej prvku), nazveme cyklickou.

My sa budeme zaoberať otázkou, kedy uvedená unárna operácia (t. j. priradenie $M \to \overline{M}$) je distributívna, takže tvorí operáciu uzáveru, t. j. kedy platí

$$(9) \quad \overline{A \cup B} = \bar{A} \cup \bar{B}.$$

V tomto prípade, ako je známe, táto operácia v S definuje topológiu. Ľahko dokážeme, že podmienka (9) je ekvivalentná podmienke

$$(10) \quad \bar{A} = A, \quad \bar{B} = B \Rightarrow \overline{A \cup B} = A \cup B,$$

t. j. požiadavke, aby zjednotenie ľubovoľných dvoch čiastočných pologrúp pologrupy S bola pologrupa, a teda čiastočná pologrupa pologrupy S. Tieto úvahy nás vedú k tejto definícii:

* Prirodzene, priradenie $M \to \overline{M}$ možno zaviesť pre ľubovoľné grupoidy; pre naše účely ho však budeme využívať len v asociatívnych grupoidoch, t. j. pologrupách.

Definícia 1. *B-pologrupou budeme nazývať takú pologrupu, v ktorej zjednotenie ľubovoľných čiastočných pologrúp je pologrupa.*

Príklad 1. Jednoduchým príkladom B-pologrupy je množina čísel $\{-1, 0, 1\}$ s operáciou násobenia. Ďalšie príklady uvedieme neskôr.

2. Vlastnosti B-pologrúp

Priamo z definície 1 vyplývajú tieto dôsledky:

Dôsledok 1. *Každá čiastočná pologrupa B-pologrupy je B-pologrupa.*

Dôsledok 2. *Pologrupa S je B-pologrupou práve vtedy, keď zjednotením ľubovoľného (konečného alebo nekonečného) počtu čiastočných pologrúp pologrupy S je opäť čiastočná pologrupa pologrupy S.*

Veta 1. *Nevyhnutná a postačujúca podmienka na to, aby pologrupa S bola B-pologrupou, je, aby pre ľubovoľné dva prvky x, y pologrupy S platila podmienka*
(A) *existuje prirodzené číslo n tak, že buď $xy = x^n$, alebo $xy = y^n$.*

Dôkaz. 1. Postačujúca podmienka: Nech $\bar{A} = A \subseteq S$, $\bar{B} = B \subseteq S$, $x \in A \cup B$, $y \in A \cup B$. Nech n je prirodzené číslo. Ak $x \in A$, aj $x^n \in A$, ak $x \in B$, aj $x^n \in B$; teda v každom prípade $x^n \in A \cup B$. Podobne $y^n \in A \cup B$. Z podmienky (A) vyplýva, že $xy \in A \cup B$, čo bolo treba dokázať.

2. Nevyhnutná podmienka: Nech S je B-pologrupa, nech $x \in S$, $y \in S$. Keďže x aj y patria do pologrupy $\overline{\{x, y\}}$, aj $xy \in \overline{\{x, y\}} = \overline{\{x\}} \cup \overline{\{y\}} = \{x^n \mid n \geqq 1\} \cup \{y^n \mid n \geqq 1\}$, z čoho vyplýva (A).

Dôsledok 3. *Množina idempotentov ľubovoľnej B-pologrupy tvorí opäť B-pologrupu.*

Dôsledok 4. *Pologrupa S, ktorej každý prvok je idempotent, je B-pologrupou práve vtedy, keď pre ľubovoľné $x \in S$, $y \in S$ platí buď $xy = x$, alebo $xy = y$.*

Poznámka 1. Špeciálne dôsledok 4 platí pre polozväzy, t. j. komutatívne pologrupy, ktorých každý prvok je idempotent. Ak tu zavedieme obvyklým spôsobom čiastočné usporiadanie ($a \leqq b \Leftrightarrow ab = a$), platí: polozväz je B-pologrupou práve vtedy, keď je reťazcom (úplne usporiadanou množinou).

Príklad 2. Ľubovoľná množina s operáciou $x \odot y = x$ tvorí B-pologrupu (nekomutatívnu, ak má aspoň dva rôzne prvky). Tento príklad ukazuje, že existujú nekomutatívne B-pologrupy ľubovoľnej mohutnosti, väčšej ako 1.

Príklad 3. Ľubovoľná usporiadaná množina s operáciou $x \odot y = \operatorname{Max}\{x, y\}$ tvorí komutatívnu B-pologrupu. Keďže existujú usporiadané množiny ľubovoľnej mohutnosti (dokonca s najmenším prvkom), existujú komutatívne B-pologrupy ľubovoľnej mohutnosti (dokonca s jednotkovým prvkom).

Poznámka 2. Veta 1 často umožňuje rozhodnúť o tom, či je daná pologrupa B-pologrupou. V niektorých prípadoch je však ťažšie použiteľná; pomerne ťažko sa pomocou nej rieši napr. úloha nájsť všetky maximálne B-pologrupy, obsiahnuté v danej pologrupe S (ktorá sama nie je B-pologrupou), t. j. také čiastočné B-pologrupy pologrupy S, ktoré nie sú okrem seba samých obsiahnuté už v žiadnej inej B-pologrupe. Pri riešení podobných otázok môžu byť užitočné tieto vety:

Veta 2. *Nech pologrupa S je B-pologrupou. Potom S je periodickou pologrupou a pre každý prvok $a \in S$ platí:*
(B) $q(a) < 5$,
(C) *$r(a)$ je celá nezáporná mocnina prvočísla.*

Dôkaz. Nech S je B-pologrupa, $a \in S$. Prvok $a^5 = a^2a^3$ podľa vety 1 sa musí rovnať niektorému z čísel a^{2n} alebo a^{3n} (kde n je vhodne zvolené prirodzené číslo) takže patrí do periódy prvku a. Preto S je periodickou pologrupou a platí $q(a) < 5$ takže platí (B). Nech prvok $b \in S$ nesplňuje podmienku (C). Keďže – podľa prvej časti dôkazu – $q(b) < 5$, je $r(b) \neq 0$, takže $r(b)$ možno písať v tvare st, kde s, t sú nesúdeliteľné prirodzené čísla, väčšie ako 1. Prvok $b^{s+t} = b^s b^t$ sa dá podľa vety 1 písať v tvare b^{sn} alebo b^{tn}, takže aspoň jedna z kongruencií

$$sn \equiv s + t \pmod{st},$$

$$tn \equiv s + t \pmod{st}$$

má za riešenie nejaké prirodzené číslo n. To je však nemožné, lebo s, t sú nesúdeliteľné prirodzené čísla, väčšie ako 1.

Poznámka 3. Vzniká otázka, či rád ľubovoľného prvku danej B-pologrupy musí byť mocninou toho istého prvočísla. Toto tvrdenie všeobecne neplatí, ako ukazuje príklad B-pologrupy, danej multiplikatívnou tabuľkou

	a	b	c	d	e
a	b	a	a	a	a
b	a	b	b	b	b
c	a	b	d	e	c
d	a	b	e	c	d
e	a	b	c	d	e

ktorá má prvok a rádu 2 a prvok c rádu 3. V 4. odseku zostrojíme dokonca príklad B-pologrupy, ktorá má prvky ľubovoľného rádu, prípustného podľa podmienky (C). Platí však nasledujúca veta.

Veta 3. *Všetky prvky B-pologrupy, patriace k tomu istému idempotentu, majú rády rovné celej nezápornej mocnine toho istého prvočísla.*

K dôkazu použijeme dve známe lemmy:

Lemma 1. *Periodická pologrupa je grupou vtedy a len vtedy, keď má jediný idempotent a keď každý jej prvok má prázdnu periódu.*

Dôkaz. Pozri [1], str. 15.

Lemma 2. *Žiadna grupa nie je zjednotením svojich dvoch vlastných podgrúp.*

Dôkaz. Pozri [7], str. 492.

Dôkaz vety 3. Ak všetky prvky B-pologrupy S, patriace k idempotentu $e \in S$, majú rád 1, veta zrejme platí. Preto predpokladajme, že prvok $a \in S$, patriaci k idempotentu e, má rád > 1. Nech b je ľubovoľný prvok pologrupy S, patriaci tiež k idempotentu e. Nech A je perióda prvku a, B perióda prvku b. A, B sú cyklické grupy, ktorých rád (= počet prvkov) je rovný rádom (= dĺžkam periódy) zodpovedajúcich prvkov a, b. Keďže S je B-pologrupa, $\overline{A \cup B} = \bar{A} \cup \bar{B}$. Pologrupa $A \cup B$ je periodická, má jediný idempotent e; každý prvok pologrupy $A \cup B$ má prázdnu periódu. Preto podľa lemmy 1 tvorí $A \cup B$ grupu. Z lemmy 2 vyplýva, že A, B nemôžu byť súčasne vlastnými podgrupami grupy $A \cup B$. Preto buď $A \subseteq B$, alebo $B \subseteq A$. Podľa vety 2 rády prvkov a, b, a teda aj rády grúp A, B sú mocninami istých prvočísel. Keďže však, ako je známe, pre konečné grupy rád podgrupy je deliteľom rádu grupy, musí existovať prvočíslo p tak, že rády obidvoch prvkov a, b sú mocninami prvočísla p. Vzhľadom na to, že $r(a) > 1$, je toto prvočíslo jednoznačne určené (nezávisí od voľby prvku b). Teda všetky prvky pologrupy S, patriace k idempotentu e, majú rád rovný mocnine toho istého prvočísla p, čo dokazuje vetu.

Veta 4. *Nevyhnutnou podmienkou na to, aby pologrupa S bola* B-*pologrupou, je, aby všetky jej* K-*triedy boli* B-*pologrupy.*

Dôkaz. Vzhľadom na dôsledok 1 stačí dokázať, že ľubovoľná K-trieda K_e B-pologrupy S je pologrupa. Nech $x \in K_e$, $y \in K_e$. Potom zrejme pre ľubovoľné prirodzené číslo n je $x^n \in K_e$, $y^n \in K_e$, takže podľa vety 1 aj $xy \in K_e$, čo sme mali dokázať.

Poznámka 4. Podmienka uvedená vo vete 4 nestačí na to, aby S bola B-pologrupou, a to ani vtedy, keď jej idempotenty spĺňajú podmienky z dôsledkov 3,4 (buď $xy = x$, alebo $xy = y$). Príklad: Pologrupa daná tabuľkou

	a	b	c	d	e
a	b	b	d	e	e
b	b	b	e	e	e
c	d	e	e	e	e
d	e	e	e	e	e
e	e	e	e	e	e

nie je B-pologrupou, hoci obidve jej K-triedy $K_b = \{a, b\}$, $K_e = \{c, d, e\}$ sú B-pologrupy.

3. Niektoré špeciálne prípady

V tomto odseku nájdeme – odhliadnúc od izomorfizmu – všetky B-pologrupy vo dvoch špeciálnych prípadoch: ak daná pologrupa je cyklická (veta 5) a ak daná pologrupa je grupou (veta 6). Najprv však dokážeme túto lemmu:

Lemma 3. *Nech všetky prvky pologrupy S spĺňajú podmienky* (B), (C) *z vety 2. Podmienkou postačujúcou na to, aby pre prvky $x \in S$, $y \in S$ platila podmienka* (A) *z vety 1, je, aby pre tieto prvky platilo:*

(D) *existuje prvok $a \in S$ a prirodzené čísla m, n tak, že $a^m = x$, $a^n = y$.*

Dôkaz. Nech pre prvky x, $y \in S$ je splnená podmienka (D). Označme* $a^{d(m,n)} = b$, $\frac{m}{d(m,n)} = m'$, $\frac{m}{d(m,n)} = n'$. Potom $b^{m'} = x$, $b^{n'} = y$, $d(m', n') = 1$, $xy = b^{m'+n'}$. Ak m', resp. n' je rovné 1, je b rovné x alebo y, takže podmienka (A) je splnená. Ak $m' = n'$, (A) opäť platí. Preto sa stačí zaoberať prípadom $m' \geq 2$, $n' \geq 2$, $m' \neq n'$. Vtedy bude $m' + n' \geq 5 > q(b)$, takže vzhľadom na podmienku (B) prvok $xy = b^{m'+n'}$ patrí do periódy prvku b. Ďalej podľa (C) existuje prvočíslo p a celé nezáporné číslo c tak, že $r(b) = p^c$. Vzhľadom na to, že $d(m', n') = 1$, aspoň jedno z čísel $d(r(b), m')$, $d(r(b), n')$ sa rovná 1. Preto aspoň jedna z kongruencií

$$m'z \equiv n' \pmod{r(b)},$$
$$n'z \equiv m' \pmod{r(b)}$$

má riešenie z (dokonca nekonečne mnoho). Nech je to napr. prvá z nich. Zvoľme riešenie z tak, aby $z > \frac{q(b)}{m'} - 1$ (zrejme je to možné voliť). Potom bude $m'(z+1) > q(b)$. Z prvej kongruencie vyplýva aj $m' + n' \equiv m'(z+1) \pmod{r(b)}$. Vzhľadom na uvedené vzťahy je $xy = b^{m'+n'} = b^{m'(z+1)} = x^{z+1}$, čo sme mali dokázať. Ak je riešiteľná len druhá z uvedených kongruencií, podobne vyjde $xy = y^{z+1}$. Tým je lemma 3 dokázaná.

Poznámka 5. Z podmienky (D) vyplýva, že prvky a, x, y patria k tomu istému idempotentu (do tej istej K-triedy). Podmienka (D) však nie je nevyhnutná na to, aby platilo (A), ani vtedy, keď pre všetky prvky platí (B), (C) a keď prvky x, y patria k tomu istému idempotentu, ako ukazuje príklad B-pologrupy, danej tabuľkou

	a	b	c
a	a	b	a
b	b	a	b
c	a	b	a

$bc = b^1$, ale neexistuje prvok pologrupy, ktorého mocninou by bolo b aj c.

* Znak $d(u, v)$ značí najväčšieho spoločného deliteľa čísel u, v.

Veta 5. *Cyklická pologrupa, vytvorená mocninami* $a, a^2, a^3, \ldots$ *svojho prvku* a *je* B-*pologrupou práve vtedy, keď prvok* a *spĺňuje podmienky* (B), (C) *z vety 2, t. j. keď* $q(a) < 5$, $r(a) = p^c$, *kde* p *je prvočíslo,* c *celé nezáporné číslo.*

Dôkaz. Ak cyklická pologrupa je B-pologrupou, podľa vety 2 uvedené podmienky sú splnené. Obrátene, ak tieto podmienky platia, je pre každé prirodzené n $q(a^n) \leqq q(a) < 5$, $r(a^n) \mid r(a) = p^c$, takže pre všetky prvky pologrupy platí (B), (C). Keďže pre ľubovoľné dva prvky platí zrejme aj (D), podľa lemmy 3 platí (A), takže podľa vety 1 je daná pologrupa B-pologrupou.

Poznámka 6. Pripomeňme, že pre ľubovoľné celé čísla $Q \geqq 0$, $R \geqq 1$ existuje (odhliadnúc od izomorfizmu) práve jedna cyklická pologrupa $\{a^n \mid n \geqq 1\}$ taká, že $q(a) = Q$, $r(a) = R$. Preto veta 5 dáva všetky neizomorfné cyklické B-pologrupy.

Definícia 2. B-*pologrupu, ktorá je súčasne grupou, budeme nazývať* B-*grupa.*

Poznámka 7. Z dôsledku 1, z vety 2 a lemmy 1 vyplýva, že *každá čiastočná pologrupa* B-*grupy je grupa. Preto môžeme* B-*grupu definovať aj ako takú grupu, v ktorej zjednotenie ľubovoľných dvoch (resp. ľubovoľného počtu) podgrúp je grupa.* Vidieť, že *podmienka* (A) *v prípade grúp sa môže nahradiť podmienkou*

(A′) *existuje prirodzené číslo* m *tak, že buď*

$$y = x^m, \qquad \text{alebo} \qquad x = y^m.$$

Z toho ľahko odvodíme, že *každá* B-*grupa je komutatívna.* Z lemmy 2 vyplýva, že *grupa je* B-*grupou práve vtedy, keď jej podgrupy tvoria reťazec v zmysle množinovej inklúzie.* Z vety 3 vyplýva, že *každá* B-*grupa je primárnou grupou* (t. j. všetky jej prvky majú rád rovný mocnine toho istého prvočísla). Keďže existujú nekomutatívne primárne grupy (napr. 8prvková grupa kvaterniónov ± 1, $\pm i$, $\pm j$, $\pm k$), obrátené tvrdenie neplatí.

Poznámka 8. H. Prüfer zaviedol r. 1921 tzv. grupy typu p^∞ (p je pevné prvočíslo), ktoré majú súhrnný názov quasicyklické grupy. Ako dokázal L. Rédei (porov. [4], str. 24), grupu typu p^∞ možno charakterizovať vlastnosťou, že obsahuje ako podgrupy cyklické grupy rádu p^n pre ľubovoľné prirodzené číslo n, pričom žiadna jej vlastná podgrupa už nemá túto vlastnosť. Túto charakterizáciu je pre naše účely výhodné upraviť takto: grupa G je grupou typu p^∞ vtedy a len vtedy, keď sa dá písať v tvare zjednotenia

$$G = \bigcup_{c=0}^{\infty} G_c, \qquad (*)$$

kde G_c sú cyklické grupy rádu p^c.

Veta 6. *Konečná grupa je* B-*grupou vtedy a len vtedy, keď je cyklickou grupou, ktorej rád je celou nezápornou mocninou prvočísla. Nekonečná grupa je* B-*grupou vtedy a len vtedy, keď je quasicyklickou grupou.*

Dôkaz. Ako je známe (pozri napr. [4], str. 24), podgrupy ľubovoľnej cyklickej grupy, ktorej rád je mocninou prvočísla, a taktiež podgrupy ľubovoľnej quasicyklickej grupy, tvoria reťazec v zmysle množinovej inklúzie, takže podľa poznámky 7 sú tieto grupy B-grupami. Obrátene, nech je daná B-grupa G. Ak je G konečná, z podmienky (A′) z poznámky 7 možno indukciou ľahko dokázať existenciu prvku $a \in G$ tak, že $G = \{a^n \mid n \geqq 1\}$. Je teda G cyklickou grupou a súčasne cyklickou pologrupou. Podľa vety 5 rád prvku a, a teda aj rád grupy G je mocninou prvočísla, čo sme mali dokázať.

Predpokladajme teraz, že G je nekonečná grupa. Podľa poznámky 8 stačí dokázať, že sa dá písať v tvare (*). Podľa vety 3 existuje prvočíslo p také, že rády všetkých prvkov grupy G sú mocninami p. Označme G_c množinu všetkých prvkov z G, ktorých rád je menší alebo rovný p^c. Zrejme platí rovnica (*). Indukciou vzhľadom na c dokážeme, že G_c je cyklickou grupou rádu p^c. Pre $c = 0$ toto tvrdenie zrejme platí. Nech platí pre $c = k$. Keďže G_k má len konečný počet prvkov, je $G - G_k \neq 0$. Nech $a \in G - G_k$; potom platí $r(a) = p^m$, kde $m > k$; položme $b = a^{p^{m-k-1}}$, potom bude $r(b) = p^{k+1}$. Dokážeme, že $G_{k+1} = \overline{\{b\}}$. Zrejme $\overline{\{b\}} \subseteq G_{k+1}$. Aby sme dokázali opačnú inklúziu, zvoľme $d \in G_{k+1}$. Keďže podgrupy grupy G podľa poznámky 7 tvoria reťazec, $G_k \subseteq \overline{\{b\}}$. Preto ak $r(d) \leqq p^k$, je $d \in G_k$, a teda $d \in \overline{\{b\}}$. Ak $r(d) = p^{k+1}$, $\overline{\{d\}}$ je, podobne ako $\overline{\{b\}}$, cyklickou grupou rádu p^{k+1}. Keďže obidve tieto grupy majú rovnaký počet prvkov, z podmienky (A′) z poznámky 7 vyplýva $\overline{\{b\}} = \overline{\{d\}}$. Preto $d \in \overline{\{b\}}$, a teda $G_{k+1} \subseteq \overline{\{b\}}$. Preto platí $G_{k+1} = \overline{\{b\}}$. G_{k+1} je teda cyklická grupa rádu p^{k+1}, čím je druhý krok indukcie a súčasne celý dôkaz ukončený.

Poznámka 9. Z vety 6 môžeme odvodiť niektoré zaujímavé dôsledky. Ako je známe ([4], str. 23 a 24), všetky cyklické grupy rovnakého rádu sú navzájom izomorfné; aj všetky grupy typu p^∞ pri tom istom p sú navzájom izomorfné. Ako príklad grupy typu p^∞ môže slúžiť multiplikatívna grupa C_p všetkých komplexných koreňov z jednotky stupňa p^n, kde n prebieha množinou všetkých prirodzených čísel. Všetkými vlastnými podgrupami grupy C_p sú cyklické podgrupy rádu p^c, pričom každému celému nezápornému c odpovedá práve jedna podgrupa grupy C_p rádu p^c. Z toho vyplýva, že grupa je B-grupou práve vtedy, keď je izomorfná s niektorou podgrupou niektorej z grúp C_p. *Každú* B-*grupu môžeme teda „izomorfne reprezentovať" v multiplikatívnej pologrupe komplexných čísel.*

Keďže každá quasicyklická grupa má vždy spočetný počet prvkov, vzhľadom na vetu 6 B-*grupa má buď konečný počet prvkov (rovný mocnine prvočísla), alebo spočetný počet prvkov.* Teda tým, že sme na B-pologrupu, ktorá mohla mať (ako vidno z príkladov 2, 3) ľubovoľný konečný, spočetný, alebo nespočetný počet prvkov, kládli ďalšie požiadavky algebraického rázu (platnosť všetkých axiómov grupy), podstatne sme obmedzili túto ľubovoľnosť.

4. Význačné príklady B-pologrúp

V tomto odseku zostrojíme pologrupu, o ktorej sa hovorilo v poznámke 3 (veta 7), ďalej nájdeme všetky maximálne multiplikatívne B-pologrupy komplexných čísel (veta 8) a vyšetríme, pri akom module multiplikatívna pologrupa úplného systému zvyškových tried tvorí B-pologrupu. Z nových pojmov zavedieme usporiadaný súčet pologrúp (definícia 3) a maximálnu B-pologrupu (definícia 4).

Definícia 3. *Nech sú dané pologrupy S_w, kde w prebieha istú množinu indexov W. Usporiadajme množinu W ľubovoľným, ale určitým spôsobom (znak usporiadania: $<$). Utvorme množinu S všetkých dvojíc tvaru (w, x), kde $w \in W$, $x \in S_w$. Zaveďme na množine S binárnu operáciu takto: Ak $w < w'$, $(w, x) \odot (w', x') = (w', x') \odot (w, x) = (w, x)$; ak $w = w'$, $(w, x) \odot (w', x') = (w, xx')$. Potom množina S s touto operáciou tvorí pologrupu, ktorú nazývame usporiadaným súčtom pologrúp S_w, príslušným k usporiadaniu $<$, a ktorú označujeme $\overset{(<)}{\sum_{w \in W}} S_w$.*

Poznámka 10. Ľahko sa dokáže: pri pevnom $w \in W$ množina všetkých dvojíc tvaru (w, x), $x \in S_w$ tvorí pologrupu, izomorfnú pologrupe S_w. Z toho vyplýva, že usporiadaný súčet pologrúp S_w sa dá písať v tvare zjednotenia disjunktných pologrúp (tzv. zložiek súčtu), izomorfných jednotlivým pologrupám S_w. Preto sa rovnajú napr. aj dĺžky predperiódy a periódy odpovedajúcich si prvkov.

Usporiadaný súčet pologrúp možno s výhodou použiť na vytváranie nových pologrúp. Týmto spôsobom môžeme zostrojiť aj príklad z poznámky 3, v ktorom pologrupa $\{a, b, c, d, e\}$ je usporiadaným súčtom grúp $\{a, b\}$, $\{c, d, e\}$.

Lemma 4. *Usporiadaný súčet pologrúp S_w je B-pologrupou vtedy a len vtedy, keď všetky S_w sú B-pologrupy.*

Dôkaz. Ak $S = \overset{(<)}{\sum_{w \in W}} S_w$ je B-pologrupa, potom všetky jej zložky R_w, a teda aj k nim izomorfné pologrupy S_w sú B-pologrupy. Obrátene, nech všetky S_w, a teda aj odpovedajúce zložky R_w sú B-pologrupy. Potom z vety 1 bezprostredne vyplýva, že aj S je B-pologrupou.

Veta 7. *Existuje B-pologrupa S tejto vlastnosti: k ľubovoľným celým nezáporným číslam p, c, Q takým, že p je prvočíslo, $Q < 5$, existuje prvok $a \in S$ taký, že $q(a) = Q$, $r(a) = p^c$.*

Dôkaz. Usporiadaný súčet všetkých neizomorfných cyklických B-pologrúp (pozri vetu 5 a poznámku 6) pri ľubovoľnom usporiadaní má podľa lemmy 4 a poznámky 10 požadovanú vlastnosť.

Definícia 4. *Pod maximálnou B-pologrupou danej pologrupy S rozumieme takú čiastočnú B-pologrupu pologrupy S, ktorá nie je obsiahnutá v žiadnej inej čiastočnej B-pologrupe pologrupy S.*

Lemma 5. *Každá čiastočná B-pologrupa pologrupy S je obsiahnutá v niektorej maximálnej B-pologrupe pologrupy S.*

Dôkaz. Nech S' je čiastočná B-pologrupa pologrupy S. Systém všetkých čiastočných B-pologrúp pologrupy S, obsahujúcich S', tvorí (vzhľadom na množinovú inklúziu) čiastočne usporiadanú množinu, v ktorej každý reťazec má horné ohraničenie (a to zjednotenie všetkých pologrúp tohto reťazca; toto zjednotenie je pologrupou; je dokonca B-pologrupou, ako vyplýva z vety 1). Preto podľa známej Zornovej lemmy o čiastočne usporiadaných množinách (pozri napr. [4], str. 31) existuje maximálny prvok čiastočne usporiadanej množiny, ktorým je v našom prípade maximálna B-pologrupa, obsahujúca S'.

Veta 8. *Každá maximálna B-pologrupa multiplikatívnej pologrupy komplexných čísel má tvar $S_p = \{0\} \cup C_p$, kde C_p je množina všetkých čísel tvaru $e^{2\pi i \frac{c}{p^d}}$, kde p je pevné prvočíslo, c, d prebiehajú množinou všetkých celých nezáporných čísel.*

Dôkaz. Označme jednu z týchto maximálnych B-pologrúp znakom S. Z vety 2 vyplýva, že pre každé $a \in S$ je buď $a = 0$, alebo $|a| = 1$, pričom v druhom prípade a je riešením nejakej binomickej rovnice $x^n = 1$, kde n je mocninou prvočísla. Z vety 3 vyplýva, že toto prvočíslo musí byť spoločné pre všetky prvky S, rôzne od nuly. Označme toto prvočíslo p. Potom $S \subseteq \{0\} \cup C_p$, kde C_p má ten istý význam ako v znení vety 8 alebo v poznámke 9. Ľahko sa presvedčíme, že už $S_p = \{0\} \cup C_p$ je maximálnou B-pologrupou. Nech $x, y \in S_p$. Ak $xy = 0$, podmienka (A) z vety 1 zrejme platí. Ak $xy \neq 0$, potom $|x| = |y| = 1$ a existujú celé nezáporné čísla c, c', d, d' tak, že

$$x = \exp\left(2\pi i \frac{c}{p^d}\right), \qquad y = \exp\left(2\pi i \frac{c'}{p^{d'}}\right).$$

Označme

$$a = \exp\left(\frac{2\pi i}{p^{d+d'}}\right).$$

Zrejme $a \in S_p$, $a^{cp^{d'}} = x$, $a^{c'p^d} = y$, takže platí podmienka (D) a podľa lemmy 3 aj podmienka (A), takže podľa vety 1 S_p je B-pologrupa, a teda maximálna B-pologrupa.

Poznámka 11. Keďže S_p sú maximálne B-pologrupy, *každá B-pologrupa, ktorá je čiastočnou pologrupou multiplikatívnej pologrupy komplexných čísel, je* podľa lemmy 5 a vety 8 *čiastočnou pologrupou niektorej z pologrúp S_2, S_3, S_5, S_7, S_{11}, ..., S_p, ... a opačne, všetky takéto pologrupy sú podľa dôsledku* 1 *B-pologrupami.* Čiastočné pologrupy pologrúp S_p možno určiť už bez ťažkostí.

Veta 9. *Multiplikatívna pologrupa Z_n úplného systému zvyškových tried $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$* modulo *$n$ je B-pologrupou vtedy a len vtedy, keď $n \leqq 4$ alebo keď n je prvočíslo tvaru $2^{2^s} + 1$, kde s je prirodzené číslo.*

Dôkaz. Keďže prípady $n \leqq 4$ môžeme bezprostredne preveriť, predpokladajme, že $n > 4$. Nech Z_n je B-pologrupou. Nech $n = p_1^{c_1} p_2^{c_2} \dots p_t^{c_t}$ je kanonický rozklad čísla n. Keby bolo $t > 1$, pre triedy $\bar{u}, \bar{v}$, reprezentované číslami $u = p_1^{c_1}$, $v = p_2^{c_2} p_3^{c_3} \dots p_t^{c_t}$ by platilo $\bar{u}\bar{v} = \bar{0}$. Zrejme však pre žiadne prirodzené k neplatí $\bar{u}^k = \bar{0}$ ani $\bar{v}^k = \bar{0}$, čo je spor, lebo nie je splnená podmienka (A) z vety 1. Preto $t = 1$. Keby bolo $c_1 > 1$, $p_1 = 2$, triedy $\bar{2}, \bar{3}$ by nesplňovali (A). Keby $c_1 > 1$, $p_1 > 2$, triedy $\bar{2}$, $\overline{p_1}$ by nesplňovali (A). Preto $c_1 = 1$, takže n je prvočíslo. Vtedy však triedy $\bar{1}\ \bar{2}, \dots, \overline{n-1}$ tvoria grupu a keďže Z_n je B-pologrupa, B-grupu. Podľa vety 6 musí byť rád tejto grupy (t. j. číslo $n - 1$) rovný mocnine nejakého prvočísla, ktoré označme p'. Keďže n je prvočíslo, väčšie ako 4, musí byť n nepárne. Preto p' musí byť párne prvočíslo, t. j. $p' = 2$. Teda n je tvaru $2^m + 1$, kde m je celé číslo (väčšie ako 1, keďže $n > 4$). Ako je známe (pozri [2], str. 144), číslo uvedeného tvaru môže byť prvočíslom len vtedy, ak $m = 2^s$, kde s je vhodne zvolené prirodzené číslo. Tým je prvá časť vety dokázaná.

Obrátene, nech n je prvočíslo tvaru $2^{2^s} + 1$. Triedy $\bar{1}, \bar{2}, \dots, \overline{n-1}$ tvoria grupu. Ako je známe (pozri napr. [2], str. 90), prvky tejto grupy možno vytvoriť pomocou istého jej prvku (tzv. primitívneho koreňa). Je to teda cyklická grupa a keďže jej rád je mocninou dvojky, je to (podľa vety 6) B-grupa. Keďže pre $\bar{x}\bar{y} = \bar{0}$ je podmienka (A) vždy splnená (n je prvočíslo!), z predošlého vyplýva, že pre ľubovoľné $\bar{x} \in Z_n$, $\bar{y} \in Z_n$ platí (A), takže podľa vety 1 je Z_n B-pologrupa.

Poznámka 12. Prvočísla tvaru $2^{2^s} + 1$ sa nazývajú Fermatove prvočísla. Uvedený výraz, ako je známe (napr. [2], str. 144), dáva prvočísla pre $s = 1, 2, 3, 4$. Či existujú iné prvočísla uvedeného tvaru, nie je známe; je však dokázané, že pre niektoré s (napr. $s = 5$) je $2^{2^s} + 1$ zložené číslo. Podľa toho pologrupy Z_n sú B-pologrupami pre $n = 1, 2, 3, 4, 5, 17, 257$ a 65 537. Otázka existencie B-pologrúp Z_n pri iných moduloch je teda ekvivalentná otázke existencie ďalších Fermatových prvočísel (pre $s > 4$).

LITERATÚRA

[1] Schwarz Š., *Teória pologrúp*, Sborník prác Prírodovedeckej fakulty Slovenskej univerzity v Bratislave, Bratislava 1943, 1—64.

[2] Rychlík K., *Úvod do elementární číselné theorie*, Přírodovědecké nakladatelství, Praha 1950 (2. vyd.).

[3] Schwarz Š., К теории периодических полугрупп, Чехословацкий математический журнал 3 (78), (1953) 7—21.

[4] Fuchs L., *Abelian groups*, Publishing House of the Hungarian Academy of Sciences, Budapest 1958.

[5] Kolibiarová B., *O komutatívnych periodických pologrupách*, Matematicko-fyzikálny časopis VIII (1958), 127—135.

[6] Kolibiarová B., *O čiastočne komutatívnych periodických pologrupách*, Matematicko-fyzikálny časopis IX (1959), 160—172.

[7] Haber S., Rosenfeld A., *Groups as unions of proper subgroups*, American mathematical Monthly 66 (1959), 491—494.

Došlo 19. 4. 1960.

Kabinet matematiky
Slovenskej akadémie vied
v Bratislave

В-ПОЛУГРУППЫ

Юрай Босак

Резюме

В-полугруппой называется такая полугруппа, в которой теоретико-множественное объединение произвольных двух ее частичных полугрупп является полугруппой. В-группой называется группа, которая одновременно является В-полугруппой. Под длиной предпериода (соотв. длиной периода) элемента x данной полугруппы мы понимаем мощность множества всех таких различных элементов последовательности $\{x^n\}_{n=1}^{\infty}$, которые в этой последовательности содержатся точно один раз (соотв. более чем один раз). Под К-классом периодической полугруппы S (принадлежищим к идемпотенту $e \in S$) понимается множество всех элементов $x \in S$, некоторой степенью которых является e. Работа состоит из четырех разделов.

В первом разделе вводится соответствие $M \to \overline{M}$, при котором каждому подмножеству M полугруппы S сопоставляется пересечение $\overline{M}$ всех полугрупп, которые содержат множество M в качестве подмножества. При этом выполняются правила (1)—(8). В работе рассматриваются полугруппы, для которых выполнено также, правило (9) и поэтому данная операция является операцией замыкания. Именно такие полугруппы и являются В-полугруппами.

Во втором разделе доказаны теоремы:

Необходимым и достаточным условием для того, чтобы полугруппа являлась В-полугруппой, является выполнение для произвольных x, y условия (А): xy является либо степенью x либо степенью y (теорема 1).

Необходимые условия для того, чтобы полугруппа S была В-полугруппой, таковы:

1. S является периодической полугруппой;
2. для произвольного $x \in S$ имеет место (В): длина предпериода элемента x меньше чем 5;
3. для произвольного элемента $x \in S$ выполнено (С): длина периода (= порядок) элемента x является (целой неотрицательной) степенью простого числа (теорема 2);
4. это простое число одинаково для всех элементов из одного и того же К-класса (теорема 3);
5. все К-классы являются полугруппами (теорема 4).

В третьем разделе найдены все циклические В-полугруппы: это такие циклические полугруппы, образующий элемент которых удовлетворяет условиям (В), (С) (теорема 5). Здесь найдены и все В-группы: это циклические группы, порядок которых является целой неотрицательной степенью простого числа, и все квазициклические группы (теорема 6).

В четвертом разделе построена В-полугруппа, которая содержит элементы с произвольной длиной предпериода и периода, ограниченные условиями (В), (С) (теорема 7). Далее найдены все максимальные мультипликативные В-полугруппы комплексных чисел: они состоят из нуля и всех комплексных корней из единицы степени p^n, где p — фиксированное простое число; n пробегает множество всех натуральных чисел (теорема 8).

Далее исследуется, для каких натуральных чисел n мультипликативная полугруппа классов вычетов по модулю n образует В-полугруппу: это всякое $n \leqq 4$ и всякое n равное простому числу Ферма (теорема 9).

B-SEMIGROUPS

Juraj Bosák

Summary

A semigroup, in which set-theoretical union of any two subsemigroups is semigroup, is called B-semigroup. A group, which is also B-semigroup, is called B-group. By the length of preperiod (respectively by length of period) of element x of given semigroup we mean the cardinal number of the set of all such (different) elements of the sequence $\{x^n\}_{n=1}^{\infty}$, which occur in this sequence just one time (respectively more than one time). By K-class of torsion semigroup S (belonging to idempotent $e \in S$) we mean a set of all elements $x \in S$, some power of which is equal e. This paper is divided into four parts.

In the first part there is defined correspondence $M \to \overline{M}$, in which to any subset M of semigroup S correspond the set-theoretical intersection $\overline{M}$ of all semigroups which contains the set M as a subset. Moreover the rules (1)—(8) hold. In this paper we are occupied with semigroups for which also the rule (9) holds so that the mentioned operation is the operation of closure. Such a semigroups are just B-semigroups.

In the second part there are proved theorems: Necessary and sufficient for a semigroup S to be B-semigroup is that for any $x \in S$, $y \in S$ holds the condition (A): xy is either power of x or power of y (theorem 1). Necessary conditions for a semigroup S to be B-semigroup are: 1. S is torsion semigroup; 2. for any element $x \in S$ holds (B): the length of preperiod of element x is smaller than 5; 3. for any element $x \in S$ holds (C): the length of period (= order) of element x is a prime power (by non-negative integer) (theorem 2); 4. this prime is common for all elements of the same K-class (theorem 3); 5. all K-classes are semigroups (theorem 4).

In the third part there are found all cyclic B-semigroups: these are such cyclic semigroups, a generator of which satisfies conditions (B), (C) (theorem 5). There are found also all B-groups: these are cyclic groups, order of which is prime power (by non-negative integer) and all quasicyclic groups (theorem 6).

In the fourth part there is constructed B-semigroup, which has elements with any length of preperiod and period, determinate by (B), (C) (theorem 7). Further there are found all maximal multiplicative B-semigroups of complex numbers: they consist of a zero and of all p^n-th complex roots of unity, where p is fixed prime, n is running over the set of all natural integers (theorem 8). Further it is researched, for which natural numbers n the multiplicative semigroup of complet system of residue classes modulo n is B-semigroup: it is each $n \leqq 4$ and each n which is Fermat prime (theorem 9).