Časopis pro pěstování matematiky, roč. 91 (1966), Praha

POLOGRUPA NEPRÁZDNÝCH PODMNOŽIN CYKLICKÉ POLOGRUPY

BOHDAN ZELINKA, Liberec

(Došlo dne 29. prosince 1964)

V tómto článku je popsána pologrupa. jejímiž prvky jsou neprázdné podmnožiny cyklické pologrupy a násobení je definováno pomocí násobení v této cyklické pologrupě.

Neprázdné podmnožiny dané pologrupy tvoří opět pologrupu. Touto pologrupou se zabýval P. DUBREIL [1] a S. LÁJOS [2] a zmiňuje se o nich i E. S. LJAPIN [3]. V tomto článku je studována takováto pologrupa v případě, že výchozí pologrupa je cyklická.

Budiž A cyklická pologrupa vytvořená prvkem a, budiž $\mathfrak{A}$ systém všech neprázdných podmnožin (nikoli pouze podpologrup) pologrupy A. Je-li $B \in \mathfrak{A}$, $C \in \mathfrak{A}$, pak BC je množina prvků pologrupy A, které lze vyjádřit jako součin bc, kde $b \in B$, $c \in C$. Takto definované násobení podmnožin je zřejmě asociativní a v našem případě i komutativní, protože výchozí pologrupa A je cyklická, tudíž komutativní.

P. Dubreil uvažuje systém všech podmnožin pologrupy A, přičemž $\emptyset B = B\emptyset = \emptyset$ pro každé $B \subset A$. Prázdná množina je potom nulovým prvkem pologrupy $\mathfrak{A}$, a to zevně připojeným, to jest není součinem žádných dvou prvků z $\mathfrak{A}$ různých od $\emptyset$ (součin dvou neprázdných podmnožin je zřejmě neprázdná množina). Tedy prázdnou množinu není třeba uvažovat, pokud ji nepotřebujeme (jako P. Dubreil) pro některé speciální úvahy.

Dokážeme některá tvrzení o pologrupě $\mathfrak{A}$.

Věta 1. *Je-li A nekonečná nebo konečná s předperiodou, pak nerozložitelnými prvky v $\mathfrak{A}$ jsou právě všechny podmnožiny A obsahující a a tyto prvky tvoří systém generátorů pologrupy $\mathfrak{A}$. Je-li A konečná bez předperiody, pak $\mathfrak{A}$ neobsahuje nerozložitelné prvky.*

Důkaz. Je-li A nekonečná nebo konečná s předperiodou, pak a je jejím nerozložitelným prvkem. Tudíž množina BC, kde $B \in \mathfrak{A}$, $C \in \mathfrak{A}$, nemůže obsahovat a, neboť a nelze vyjádřit jako součin dvou prvků b, c. Tedy prvek a mohou obsahovat pouze nerozložitelné prvky pologrupy $\mathfrak{A}$. Na druhé straně je-li $B = \{a^{k_1}, a^{k_2}, \ldots\}$, kde všechny exponenty u a jsou alespoň rovny dvěma a k_1 je nejmenší z těchto exponentů, lze vyjádřit B ve tvaru $\{a\}^{k_1 - 1} . \{a, a^{k_2 - k_1 + 1}, a^{k_3 - k_1 + 1}, \ldots\}$, tedy jako součin množin obsahujících prvek a. Je-li A konečná bez předperiody, je grupou, tudíž obsahuje jednotkový prvek e. Zřejmě množina $\{e\}$ je jednotkovým prvkem v $\mathfrak{A}$, tudíž $\mathfrak{A}$ nemůže obsahovat nerozložitelné prvky.

Věta 2. *Jedinými idempotenty pologrupy $\mathfrak{A}$ jsou právě všechny podmnožiny A, které jsou grupami.*

Důkaz. Je-li G idempotent, pak $G^2 = G$, což je speciální případ vztahu $G^2 \subset G$, který charakterisuje podpologrupu. Každý idempotent z $\mathfrak{A}$ musí být tedy podpologrupou A. Nechť a^k je mocnina a z G s nejmenším exponentem. Poněvadž $G^2 = G$, lze a^k vyjádřit jako součin dvou prvků z G, tedy mocnin a s exponentem větším nebo rovným k. To však lze jen tehdy, je-li A konečná a a^k nepatří do její předperiody. Tedy ani ostatní prvky z G, které mají větší exponent u a než k, nemohou patřit do předperiody. Avšak podpologrupa konečné pologrupy, která neobsahuje prvky z její předperiody, je grupou, tedy G je grupa. Na druhé straně pro každou grupu G platí $G^2 = G$, tedy věta je dokázána.

Důsledek. *Je-li A nekonečná, pak $\mathfrak{A}$ neobsahuje idempotenty a tudíž ani periodické podpologrupy.*

Věta 3. *Je-li A konečná pologrupa bez předperiody řádu n, pak $\mathfrak{A}$ obsahuje nulový prvek A a jednotkový prvek $\{a^n\}$. Je-li A konečná pologrupa typu* (h, d) (viz definici v [3]), *kde $h \neq 1$, pak $\mathfrak{A}$ obsahuje nulový prvek $G = \{a^h, \ldots, a^{h+d-1}\}$ a neobsahuje jednotkový prvek. Je-li A nekonečná, pak $\mathfrak{A}$ neobsahuje ani jednotkový, ani nulový prvek.*

Důkaz. V prvním případě A je grupou a tedy $AB = A$ pro každé $B \subset A$. Prvek a^n je jednotkovým prvkem A, tudíž (jak bylo podotknuto už v důkaze věty 1) je $\{a^n\}$ jednotkovým prvkem $\mathfrak{A}$. V druhém případě $aG = \{a^{h+1}, \ldots, a^{h+d-1}, a^h\} = G$, tudíž $a^kG = G$ pro každé k, tedy $BG = G$ pro každé B skládající se z mocnin a. Poněvadž v tomto případě $\mathfrak{A}$ obsahuje nerozložitelné prvky, nemůže obsahovat jednotkový prvek. Ve třetím případě $\mathfrak{A}$ neobsahuje idempotenty, neobsahuje tedy ani nulový, ani jednotkový prvek.

Uvažujme nyní A konečnou typu (h, d). Budiž e dělitel čísla d, budiž a^p idempotent pologrupy A. Množinu prvků a^k, kde $k \equiv p (\bmod e)$, $k \geqq h$, označíme G_e. Množiny G_e jsou, jak známo, právě všechny množiny v $\mathfrak{A}$, které jsou grupami. Označme dále pro všechny dělitele e čísla d symbolem $\mathfrak{A}_e$ množinu prvků z $\mathfrak{A}$, jejichž některou mocninou je G_e. Každý prvek z $\mathfrak{A}$ náleží zřejmě právě do jedné z množin $\mathfrak{A}_e$, neboť generuje konečnou cyklickou pologrupu, která má právě jeden idempotent a tento idempotent je grupou, tedy patří mezi G_e.

Věta 4. *Budiž $B = \{a^{k_1}, \ldots, a^{k_m}\}$. Platí $B \in \mathfrak{A}_e$ právě tehdy, je-li splněno: $k_i \equiv k_j$* $(\bmod e)$ *pro všechna i, j $(1 \leqq i \leqq m,\ 1 \leqq j \leqq m)$ a je-li e' dělitel d větší než e, pak $k_{i'} \not\equiv k_{j'}$* $(\bmod e')$ *alespoň pro jednu dvojici i', j'.*

Důkaz. Nechť platí podmínka věty. Protože se při násobení prvků z A exponenty sčítají, budou prvky n-té mocniny B vyjádřeny jako mocniny a, jejichž exponenty jsou všechny možné součty n prvků z $\{k_1, \ldots, k_m\}$. Tyto součty musí však být také kongruentní modulo e. Idempotentem cyklické pologrupy generované prvkem B bude tedy takové $G_{e''}$, kde je toto splněno, to jest kde $e'' \geqq e$. Je-li nyní $e' > e$ a existují i', j' tak, že $k_{i'} \not\equiv k_{j'}(\text{mod } e')$, pak v B^n existují prvky s exponenty $k_1(n-1) + k_{i'}$, $k_1(n-1) + k_{j'}$, které rovněž nejsou kongruentní modulo e'. Tedy i v $G_{e''}$ existují takovéto prvky a musí být $e'' \neq e'$. Protože však jsme o e' předpokládali pouze $e' > e$, musí být $e'' = e$. Tedy $B \in \mathfrak{A}_e$. Jestliže podmínka věty neplatí, pak buď existují v B prvky, jejichž exponenty u a nejsou kongruentní modulo e a tedy (analogicky dokázanému výše) v každé mocnině B jsou takovéto prvky a tudíž G_e není mocninou B, nebo existuje $e' > e$ dělící d takové, že $k_i \equiv k_j(\text{mod } e')$ pro všechna i, j a pak $B \in \mathfrak{A}_{e''}$, kde $e'' \geqq e' > e$.

Věta 5. *Nechť $B = \{a^{k_1}, \ldots, a^{k_m}\} \in \mathfrak{A}_e$ a nechť $0 \leqq e' < e$, $k_i \equiv e'(\text{mod } e)$ pro každé i $(1 \leqq i \leqq m)$. Nechť $e'' = (e, e')$, to jest největší společný dělitel e a e'. Pak podpologrupa pologrupy $\mathfrak{A}$ generovaná prvkem B má periodu délky e/e''.*

Důkaz. Je-li q délka periody cyklické pologrupy generované prvkem B, pak q je nejmenší přirozené číslo takové, že $B^q G_e = G_e$. Všechny exponenty u a prvků z B^q jsou kongruentní s $e'q$ modulo e. Všechny exponenty u a prvků z G_e jsou kongruentní s p modulo e. Tedy exponenty u a prvků z $B^q G_e$ jsou kongruentní s $p + e'q$, ovšem současně i s p, poněvadž $B^q G_e = G_e$. Je tedy $p + e'q \equiv p(\text{mod } e)$, tedy $e'q \equiv 0$ $(\text{mod } e)$. Je tedy $e'q$ společný násobek e a e'. Protože však q je nejmenší číslo splňující tuto podmínku, je $e'q$ nejmenší společný násobek e a e', tedy $e'q \,.\, e'' = ee'$, z toho $q = e/e''$.

Věta 6. *Je-li $B \in \mathfrak{A}_e$, $C \in \mathfrak{A}_f$, pak $BC \in \mathfrak{A}_{(e,f)}$.*

Důkaz. Nechť $B = \{a^{k_1}, \ldots, a^{k_p}\}$, $C = \{a^{l_1}, \ldots, a^{l_q}\}$. Nechť $BC \in \mathfrak{A}_g$. Tedy všechny exponenty u a prvků z BC jsou kongruentní modulo g, tedy speciálně čísla $k_1 + l_1, k_2 + l_1, \ldots, k_p + l_1$ jsou kongruentní modulo g. Pak ovšem jsou kongruentní modulo g i čísla $k_1, k_2, \ldots, k_p$. Jelikož všechna tato čísla jsou kongruentní modulo e, jsou také kongruentní modulo $[e, g]$, kde hranaté závorky označují nejmenší společný násobek. Protože však e i g jsou děliteli d, je i $[e, g]$ dělitelem d a musí být tedy $[e, g] \leqq e$, tudíž $[e, g] = e$ a g je dělitelem e. Analogicky pomocí čísel $k_1 + l_1, k_1 + l_2, \ldots, k_1 + l_q$ dokážeme, že g je dělitelem f. Číslo g je tedy dělitelem (e, f), avšak poněvadž (e, f) je dělitelem d, musí být $(e, f) \leqq g$, tudíž $g = (e, f)$.

Speciálně $G_e G_f = G_{(e,f)}$.

Věta 7. *Je-li D podmnožina množiny dělitelů čísla d, pak $\mathfrak{J} = \bigcup_{e \in D} \mathfrak{A}_e$ je ideálem v $\mathfrak{A}$ právě tehdy, jestliže D obsahuje s každým svým prvkem všechny jeho dělitele.*

Důkaz. Je-li $B \in \mathfrak{A}_e \subset \mathfrak{J}$, $C \in \mathfrak{A}_f \subset \mathfrak{A}$, pak $BC \in \mathfrak{A}_{(e,f)}$. Avšak je-li podmínka věty splněna, je $\mathfrak{A}_{(e,f)} \subset \mathfrak{J}$, poněvadž je-li $e \in D$, musí být i $(e, f) \in D$. Jestliže nyní $e \in D$, $e' \notin D$ a e' je dělitelem e, nechť $B' \in \mathfrak{A}_e \subset \mathfrak{J}$, $C' \in \mathfrak{A}_{e'} \subset \mathfrak{A} \dot{-} \mathfrak{J}$. Je $B'C' \in \mathfrak{A}_{(e,e')} = \mathfrak{A}_{e'} \subset \mathfrak{A} \dot{-} \mathfrak{J}$ a $\mathfrak{J}$ není ideálem v $\mathfrak{A}$.

Vyslovme ještě větu o ideálech $\mathfrak{A}$, je-li A nekonečná.

Věta 8. *Budiž A nekonečná. Označme M_i množinu všech a^j pro $j \geqq i$, označme $\mathfrak{M}_k$ systém všech M_i pro $i \geqq k$. Každé $\mathfrak{M}_k$ je ideálem v $\mathfrak{A}$ a je-li $\mathfrak{J}$ ideál v $\mathfrak{A}$, jehož některý prvek obsahuje prvek a^l* (l je přirozené číslo), *pak $\mathfrak{M}_{l+1} \subset \mathfrak{J}$.*

Důkaz. Budiž $M_j \in \mathfrak{M}_i$, to jest $j \geqq i$, a budiž $B \in \mathfrak{A}$. Nechť a^k je prvek z B s nejmenším exponentem u a. Pak BM_j obsahuje všechny prvky $a^{j'+k}$, kde $j' \geqq j$, tedy $BM_j \supset M_{j+k}$. Avšak prvek a^{j+k} má nejmenší exponent u a z prvků BM_j, protože je to součin prvků s nejmenšími exponenty v množinách B, M_j; tedy $BM_j = M_{j+k} \in \mathfrak{M}_i$ a $\mathfrak{M}_i$ je ideálem v $\mathfrak{A}$. Budiž nyní $\mathfrak{J}$ ideál v $\mathfrak{A}$ a budiž $a^l \in C \in \mathfrak{J}$. Budiž a^m prvek s nejmenším exponentem u a v C. Pak zřejmě $CM_i = M_{i+m}$ pro všechna přirozená i, tedy $C\mathfrak{M}_1 = \mathfrak{M}_{m+1}$. Avšak $\mathfrak{M}_{l+1} \subset \mathfrak{M}_{m+1} = C\mathfrak{M}_1 \subset C\mathfrak{A} \subset \mathfrak{J}$.

Konečně dokážeme ještě větu o mohutnostech podmnožin A.

Věta 9. *Nechť A je nekonečná nebo konečná bez předperiody. Je-li $B \in \mathfrak{A}$, $C \in \mathfrak{A}$, pak mohutnost BC je větší nebo rovna větší z mohutností množin B a C. Je-li A konečná s předperiodou, toto tvrzení obecně neplatí.*

Důkaz. Nechť platí předpoklad. Nechť bez újmy na obecnosti B má mohutnost větší nebo rovnou mohutnosti C. Nechť $B = \{a^{k_1}, a^{k_2}, \ldots\}$, $a^l \in C$. Pak množina BC obsahuje všechny prvky $a^{k_1+l}, a^{k_2+l}, \ldots$ které jsou navzájem různé, poněvadž $a^{k_1}, a^{k_2}, \ldots$ jsou navzájem různé. Množina prvků $a^{k_1+l}, a^{k_2+l}, \ldots$ má zřejmě tutéž mohutnost jako B a je podmnožinou BC. Nechť nyní A je konečná pologrupa s předperiodou typu (h, d) a budiž $k \leqq \frac{1}{2}h$. Pak

$$\{a^{h-k}, a^{h+d-k}\}^2 = \{a^{2h-2k}, a^{2h+d-2k}, a^{2h+2d-2k}\} = \{a^{2h-2k}\},$$

protože $2h - 2k \geqq h$ a d je délka periody. Tedy součinem dvou dvouprvkových množin je tu množina jednoprvková.

Literatura

[1] *Dubreil P.:* Contribution à la théorie des demi-groupes. III. Bull. Soc. Math., France, *81* (1953), 289–306.

[2] *Лайош, Ш.:* О полугруппе подмножеств полугруппы. Publ. Math. Debrecen *9* (1962), 223–226.

[3] *Ляпин, Е. С.:* Полугруппы. Москва 1960.

Adresa autora: Liberec, Jarošova 5 (Vysoká škola strojní a textilní).

Резюме

ПОЛУГРУППА НЕПУСТЫХ ПОДМНОЖЕСТВ ЦИКЛИЧЕСКОЙ ПОЛУГРУППЫ

БОГДАН ЗЕЛИНКА (Bohdan Zelinka), Либерец

Исследуется полугруппа $\mathfrak{A}$ образованная всеми непустыми подмножествами (не только подполугруппами) циклической полугруппы A, причем произведение BC двух подмножеств B и C определено как множество произведений bc, где $b \in B$, $c \in C$. Найдены условия для того, чтобы элемент из $\mathfrak{A}$ был неразложим и чтобы он был идемпотентен. Исследованы единичный и нулевой элементы полугруппы $\mathfrak{A}$. В случае конечной полугруппы A образовано разложение $\mathfrak{A}$ по идемпотентам, найдена длина периода цилической подполугруппы полугруппы $\mathfrak{A}$. Исследуются идеалы полугруппы $\mathfrak{A}$ и доказывается одна теорема о мощности произведения двух подмножеств A.

Summary

THE SEMIGROUP OF NON-VOID SUBSETS OF A CYCLIC SEMIGROUP

BOHDAN ZELINKA, Liberec

One explores the semigroup $\mathfrak{A}$ formed by all non-void subsets (not only subsemigroups) of a cyclic semigroup A, while the product BC of two subsets B and C is defined as the set of products bc, where $b \in B$, $c \in C$. The conditions for an element of $\mathfrak{A}$ to be indecomposable and to be idempotent are found. The unit and zero elements of the semigroup $\mathfrak{A}$ are explored. In the case of a finite semigroup A the decomposition of $\mathfrak{A}$ according to idempotents is constructed, the length of the period of a cyclic subsemigroup of the semigroup $\mathfrak{A}$ is found. Ideals of the semigroup $\mathfrak{A}$ are explored and one theorem on the cardinality of the product of two subsets of A is proved.