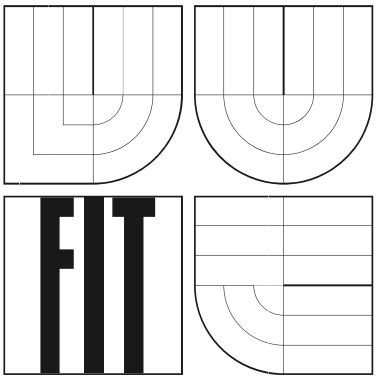
Vysoké učení technické v Brně
Fakulta informačních technologií



Regulární pologrupy

Semestrální práce do předmětu
Algebra, Kombinatorika, Grafy

Tomáš Masopust

Brno, 2006

Obsah

Úvod

Teorie pologrup je součást matematiky, která nachází velké uplatnění jak v teoretické, tak i praktické informatice. Ať již jde o teorii formálních jazyků, kde jazyk je definován jako podmnožina volného monoidu (tj. volné pologrupy s neutrálním prvkem), či o praktické řešení přenosu a uchovávání dat v podobě různých kódů.

Čistě z matematického hlediska je teorie pologrup částí matematické disciplíny nazývané algebra, která studuje abstraktní množiny spolu s jistými operacemi na nich definovanými. Hlavním cílem teorie pologrup je úplný popis a klasifikace všech pologrup. K dosažení tohoto cíle se převážně věnuje studiu problému konstruování nových pologrup ze stávajících, studiu vnitřních struktur pologrup a speciálním druhům pologrup jako jsou například regulární pologrupy či inverzní pologrupy, jimiž se zabýváme v tomto textu.

V první kapitole zavedeme a připomeneme základní pojmy a značení, které budeme používat v dalším textu. Ve druhé kapitole se seznámíme s pojmem regulárního prvku a regulární pologrupy a zaměříme se na základní vlastnosti obecných regulárních pologrup zejména ve vztahu k vlastnostem jejich idempotentních prvků. Ve třetí kapitole se pak blíže podíváme na speciální třídu regulárních pologrup—inverzní pologrupy.

V literatuře je možné nalézt spoustu dalších speciálních tříd regulárních pologrup. Zde se jimi však zabývat nebudeme, neboť nám jde pouze o stručný úvod do teorie regulárních pologrup. Pro více informací odkazujeme čtenáře na výbornou monografii [1].

1 Základní definice

V této kapitole připomeneme některé základní definice a pojmy z teorie pologrup, které budeme potřebovat v dalším textu. Nejprve zavedeme pojem pologrupy.

Definice 1.1 Neprázdná množina S spolu s binární operací $\cdot$ se nazývá *pologrupa*, jestliže operace $\cdot$ je asociativní na S, tj. pro každé $a, b, c \in S$ platí

$$a \cdot (b \cdot c) = (a \cdot b) \cdot c.$$

Pologrupu S s operací $\cdot$ pak zapisujeme jako dvojici $(S, \cdot)$.

V dalším textu se budeme držet zvyklosti psát místo $x \cdot y$ pouze xy a též stručně hovořit o pologrupě S, čímž máme na mysli pologrupu $(S, \cdot)$.

Pokud pro dva prvky $a, b \in S$ platí $ab = ba$, říkáme, že prvky a a b *komutují*. Pologrupa se nazývá *komutativní*, jestliže libovolné dva její prvky komutují.

Příklad 1.2 Příkladem (komutativních) pologrup jsou $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}_n, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$,$(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$, $(\mathbb{Z}_n, \cdot)$, kde $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_n$ postupně značí množiny všech přirozených, celých, racionálních, reálných a komplexních čísel a množinu všech celých čísel modulo n. $\diamond$

Mohutnost množiny S se nazývá *řád* pologrupy S. Předchozí příklad ukazuje, že existují jak nekonečné (spočetné i nespočetné), tak i konečné pologrupy libovolného řádu n pro $n \in \mathbb{N}$.

Nechť S je pologrupa. Jestliže S obsahuje prvek 1 s vlastností

$$1x = x1 = x$$

pro všechna $x \in S$, pak prvek 1 nazýváme *neutrálním prvkem* pologrupy S. Dá se snadno ukázat, že takový prvek, pokud v pologrupě existuje, je pouze jediný. Pologrupa s neutrálním prvkem se nazývá *monoid*.

Nyní zavedeme pojem, který bude hrát klíčovou roli v celém dalším textu.

Definice 1.3 Nechť S je pologrupa a $e \in S$ je prvek takový, že $ee = e$. Pak e nazýváme *idempotentní prvek* či stručně pouze *idempotent* pologrupy S.

Poznamenejme, že pologrupa nemusí mít žádný idempotent, nebo jich může mít i více než jeden.

Definice 1.4 Nechť $(S, \cdot)$, $(T, *)$ jsou pologrupy. Zobrazení $f : S \to T$ se nazývá *homomorfismus*, jestliže pro libovolné prvky $x, y \in S$ platí

$$f(x \cdot y) = f(x) * f(y).$$

Homomorfismus f se nazývá *monomorfismus*, jestliže f je prosté zobrazení. Podobně se f nazývá *epimorfismus*, jestliže f je surjektivní zobrazení. Bijektivní homomorfismus se nazývá *izomorfismus*.

Definice 1.5 Nechť S je pologrupa. Řekneme, že S je grupa, jestliže S je monoid a každý prvek z S má inverzní prvek (ve smyslu grupy), tj. pro libovolné $x \in S$ existuje $y \in S$ takové, že $xy = yx = 1$.

Není těžké ukázat, že libovolný prvek x grupy S má právě jeden inverzní prvek. Budeme jej značit x^{-1}.

Definice 1.6 Pologrupa S se nazývá *pologrupa s krácením*, jestliže pro libovolné její prvky a, b, c platí

$$ca = cb \Rightarrow a = b$$

a rovněž

$$ac = bc \Rightarrow a = b.$$

2 Regulární pologrupy

Jedním ze základních pojmů v teorii pologrup je právě pojem regularity. V této kapitole se proto s tímto pojmem seznámíme a ukážeme některé ze základních vlastností regulárních pologrup. Půjde nám zejména o vlastnosti idempotentních prvků a jejich vliv na strukturu regulární pologrupy.

Definice 2.1 Nechť S je pologrupa. Prvek $a \in S$ se nazývá *regulární*, jestliže existuje prvek $b \in S$ takový, že $a = aba$. Pokud každý prvek pologrupy S je regulární, pak S se nazývá *regulární pologrupa*.

Uvažme libovolnou pologrupu a dva její různé regulární prvky. Je pak též součin těchto prvků regulární prvek? Na tuto otázku dává odpověď následující příklad.

Příklad 2.2 Definujme pologrupu následující tabulkou:

	a	b	c	0
a	a	c	c	0
b	0	b	0	0
c	0	c	0	0
0	0	0	0	0

Prvky a a b jsou idempotenty. Jelikož každý idempotent je regulární prvek ($eee = ee = e$), jsou a a b regulární. Avšak prvek $ab = c$ regulární není. $\diamond$

Lemma 2.3 *Nechť S je pologrupa s krácením a $a \in S$ prvek, který není regulární. Pak ab není regulární pro žádné $b \in S$.*

Důkaz. Důkaz provedeme sporem. Nechť ab je regulární. Pak existuje $y \in S$ takové, že

$$abyab = ab.$$

Jelikož S je pologrupa s krácením, máme též

$$abya = a.$$

Tedy a je regulární. To je však spor s předpokladem. □

Nyní budeme definovat pojem velice podobný pojmu z teorie grup – inverzní prvek. Definice se ovšem poněkud liší, neboť v pologrupě nemáme zaručenu existenci neutrálního prvku.

Definice 2.4 Nechť S je pologrupa. Prvky $a, b \in S$ se nazývají (vzájemně) *inverzní*, jestliže platí $a = aba$ a také $b = bab$.

Všimněme si, že pokud je S grupa, pak každý prvek splňuje předchozí definici.

Dále ukážeme, že libovolný prvek regulární pologrupy má inverzní prvek. Ten však nemusí být dán jednoznačně, jak ukazuje následující příklad.

Příklad 2.5 Nechť S je pologrupa definovaná tabulkou

	a	b
a	a	a
b	b	b

Pak $a = aaa = aba$, $b = bbb = bab$. Tedy každý z obou prvků je inverzní k oběma prvkům. ◇

Věta 2.6 *Nechť S je pologrupa. Pak každý regulární prvek z S má alespoň jeden inverzní prvek.*

Důkaz. Nechť $a \in S$ je regulární prvek a předpokládejme, že $b \in S$ je takový, že $a = aba$. Položme $c = bab$. Nyní máme

$$a = aba = (aba)ba = a(bab)a = aca$$

a také

$$c = bab = b(aba)b = (bab)ab = cab = c(aba)b = ca(bab) = cac.$$

Tím jsme ukázali, že prvky a a c jsou (vzájemně) inverzní. □

Nyní dokážeme tvrzení, které říká, že homomorfní obraz regulární pologrupy S je opět regulární pologrupa. Navíc platí, že idempotenty se zobrazují na idempotenty a na každý idempotent z homomorfního obrazu se zobrazí alespoň jeden idempotent pologrupy S.

Věta 2.7 *Nechť $f : S \to T$ je homomorfismus z regulární pologrupy S do pologrupy T. Pak $imf = \{f(x) : x \in S\}$ je regulární pologrupa. Jestliže g je idempotent v imf, pak existuje idempotent e v S takový, že $f(e) = g$.*

Důkaz. Zřejmě imf je pologrupa. Dokážeme, že je regulární.

Uvažme libovolný prvek z imf. Ten je tvaru $f(x)$ pro nějaké x z S. Avšak, x je regulární, tedy existuje $y \in S$ takové, že $xyx = x$. Pak $f(x)f(y)f(x) = f(xyx) = f(x)$, a tedy $f(x)$ je regulární.

Nechť nyní $g \in imf$ je libovolný idempotent a nechť $a \in S$ je prvek takový, že $f(a) = g$. Pak

$$f(aa) = f(a)f(a) = gg = g.$$

Podle předchozí věty má a^2 inverzní prvek $x \in S$. Tedy platí $a^2xa^2 = a^2$ a $xa^2x = x$. Položme $e = axa$. Pak

$$e^2 = axaaxa = axa^2xa = axa = e$$

a

$$f(e) = f(axa) = f(a)f(x)f(a) = f(a^2)f(x)f(a^2) = f(a^2xa^2) = f(a^2) = g.$$

Tím je důkaz hotov. □

Dále se podíváme na vztah mezi regulárními pologrupami a grupami. Zde se dostáváme k již zmiňované důležitosti vlastností idempotentních prvků. Následující věta říká, že pokud regulární pologrupa S obsahuje právě jeden idempotent, pak S je grupa a onen idempotent hraje roli neutrálního prvku.

Věta 2.8 *Nechť S je regulární pologrupa. Pak následující vlastnosti jsou ekvivalentní:*

(a) *S má právě jeden idempotent;*

(b) *S je pologrupa s krácením;*

(c) *S je grupa.*

Důkaz. Nechť a' značí prvek inverzní k prvku $a \in S$.

$(a) \Rightarrow (b)$: Nechť S má právě jeden idempotent a nechť $ca = cb$, $ad = bd$ pro nějaké libovolné prvky $a, b, c, d \in S$. Jelikož $cc'cc' = cc'$, $c'cc'c = c'c$, tj. cc' i $c'c$ jsou idempotenty, je $cc' = c'c$ pro libovolné $c \in S$. Tedy též $c'c = a'a = dd'$. Nyní

$$ac'c = aa'a = a$$

a též

$$c'ca = cc'a = aa'a = a.$$

Máme tedy, že $c'c = 1$. Odtud plyne

$$ca = cb \Rightarrow c'ca = c'cb \Rightarrow a = b$$

a

$$ad = bd \Rightarrow acc' = add' = bdd' = bcc' \Rightarrow a = b.$$

$(b) \Rightarrow (c)$: Nechť $a \in S$ je libovolný prvek. Pak $aa' = a'a = 1$: Platí totiž

$$c'ca = c'caa'a \Rightarrow c = caa',\ a'cc' = a'aa'cc' \Rightarrow c = aa'c$$

a analogicky

$$acc' = aa'acc' \Rightarrow c = a'ac,\ c'ca' = c'ca'aa' \Rightarrow c = ca'a.$$

Nechť a' a a'' jsou inverzní prvky k $a \in S$. Pak ovšem

$$aa'a = aa''a \Rightarrow aa' = aa'' \Rightarrow a' = a''.$$

Tedy, S má neutrální prvek a každý prvek má právě jeden prvek s ním inverzní ve smyslu inverze v pologrupě. Jelikož však pro libovolný prvek $a \in S$ platí $aa' = a'a = 1$, je $a' = a^{-1}$ též inverzní prvek v grupě.

$(c) \Rightarrow (a)$: Nechť S je grupa. Pak pro libovolné $a \in S$ je $aa^{-1}a = a$. Tedy S je regulární. Předpokládejme, že a je idempotent. Pak

$$a^2a^{-1} = aa^{-1} \Rightarrow a1 = 11 \Rightarrow a = 1.$$

Tedy 1 je jediný idempotent grupy S. □

Mnoho dalších zajímavých tříd regulárních pologrup vznikne, klademe-li na množinu všech idempotentních prvků jistá omezení. V další kapitole se budeme věnovat jedné z nich.

3 Inverzní pologrupy

Z předchozí kapitoly víme, že ke každému prvku a regulární pologrupy S existuje alespoň jeden prvek $b \in S$ takový, že a, b jsou (vzájemně) inverzní. Omezíme-li tento počet inverzních prvků na jeden, dostáváme tzv. *inverzní pologrupu*.

Definice 3.1 Pologrupa S se nazývá *inverzní* (též *invertibilní*), pokud ke každému prvku $a \in S$ existuje právě jeden prvek $a^{-1} \in S$ takový, že a, a^{-1} jsou (vzájemně) inverzní.

Nejprve uvedeme několik základních vlastností vyplývajících přímo z definice:

$$xx^{-1}x = x,\ x^{-1}xx^{-1} = x^{-1},$$

$$(x^{-1})^{-1} = x,$$

$$x^2 = x \Rightarrow x^{-1} = x,$$

$$(xx^{-1})^2 = xx^{-1}.$$

Na tomto místě opět ukážeme důležitost studia idempotentních prvků.

Následující věta říká, že pro regulární pologrupu je podmínka komutativity idempotentních prvků nutnou i postačující pro to, aby pologrupa byla inverzní.

Věta 3.2 *Pologrupa S je inverzní právě tehdy, když je regulární a všechny její idempotenty komutují.*

Důkaz. Nechť S je inverzní pologrupa. Pak S je zřejmě regulární. Nechť $e, f \in S$ jsou dva libovolné idempotenty a nechť $z = (ef)^{-1}$. Uvažme prvek fze. Máme

$$(ef)(fze)(ef) = ef^2ze^2f = efzef = ef,$$

$$(fze)(ef)(fze) = fze^2f^2ze = f(zefz)e = fze.$$

Tedy fze je inverzní prvek k ef. Díky jedinečnosti inverzních prvků platí $z = fze$. Odtud

$$z^2 = fzefze = f(zefz)e = fze = z.$$

Tedy z je idempotent. Pak ovšem $z = z^{-1} = ef$, a tedy ef je idempotent a svůj vlastní inverzní prvek. Podobně se ukáže, že též fe je idempotent a platí

$$(ef)(fe)(ef) = ef^2e^2f = efef = ef,\ (fe)(ef)(fe) = fe^2f^2e = fefe = fe.$$

Tedy i fe je inverzní prvek k ef. Opět z jedinečnosti inverzních prvků máme $ef = fe$.

Nechť naopak S je regulární pologrupa a všechny její idempotenty komutují. Předpokládejme, že x^{-1} a x' jsou dva inverzní prvky k $x \in S$. Máme

$$xx^{-1} = (xx')(xx^{-1}) = (xx^{-1})(xx') = xx'.$$

Dále platí

$$x' = x'xx' = x'xx^{-1}xx' = x^{-1}xx'xx' = x^{-1}xx' = x^{-1}xx^{-1} = x^{-1}.$$

Tím je důkaz hotov. □

Jako jednoduchý důsledek dostáváme

Důsledek 3.3 *V inverzní pologrupě tvoří množina všech idempotentních prvků podpologrupu.*

Důkaz. Nechť E je množina všech idempotentních prvků inverzní pologrupy S a nechť $e, f \in E$. Pak

$$efef = effe = efe = eef = ef$$

Tedy $ef \in E$. □

Pro inverzní prvky součinu platí podobná pravidla jako v případě grup.

Věta 3.4 *Nechť S je inverzní pologrupa. Pak $(ab)^{-1} = b^{-1}a^{-1}$ pro libovolné prvky $a, b \in S$.*

Důkaz. Jelikož $a^{-1}a$ a bb^{-1} jsou idempotenty, platí

$$(ab)(b^{-1}a^{-1})(ab) = a(bb^{-1})(a^{-1}a)b = a(a^{-1}a)(bb^{-1})b = ab,$$

$$(b^{-1}a^{-1})(ab)(b^{-1}a^{-1}) = b^{-1}(a^{-1}a)(bb^{-1})a^{-1} = b^{-1}(bb^{-1})(a^{-1}a)a^{-1} = b^{-1}a^{-1}.$$

Tedy $b^{-1}a^{-1} = (ab)^{-1}$. □

Tento výsledek se dá úplnou indukcí zobecnit na následující tvrzení.

Věta 3.5 *Nechť $a_1, a_2, \ldots, a_n \in S$ jsou prvky inverzní pologrupy. Pak*

$$(a_1 a_2 \ldots a_n)^{-1} = a_n^{-1} \ldots a_2^{-1} a_1^{-1}.$$

Odtud dostáváme $(a^n)^{-1} = (a^{-1})^n$, $n \geq 1$, tedy můžeme stručně psát a^{-n}. Obecně však neplatí rovnost $a^p a^q = a^{p+q}$, $p, q \in \mathbb{Z}$.

Velice podobně jako v předchozí kapitole se dá ukázat následující tvrzení.

Věta 3.6 *Nechť $f : S \to T$ je homomorfismus z inverzní pologrupy S na pologrupu T. Pak T je inverzní pologrupa.*

Na závěr zmíníme ještě jeden velice zajímavý výsledek o inverzních pologrupách, který má motivaci v Cayleyho větě z teorie grup. Jde o charakterizaci všech inverzních pologrup jako podpologrup pologrupy všech částečných prostých zobrazení nějaké množiny do sebe.

Nechť X je neprázdná množina. Označme $\mathcal{I}_X$ množinu všech částečných prostých zobrazení množiny X do sebe. Dá se ukázat, že $\mathcal{I}_X$ spolu s operací skládání zobrazení tvoří inverzní pologrupu. Tuto pologrupu nazýváme *symetrická inverzní pologrupa množiny X*.

Nyní se již dostáváme k hlavnímu výsledku, který zde uvedeme bez důkazu. Čtenáře opět odkazujeme na monografii [1].

Věta 3.7 (Vagner-Preston) *Nechť S je inverzní pologrupa. Pak existuje symetrická inverzní pologrupa $\mathcal{I}_X$ a monomorfismus f z S do $\mathcal{I}_X$. Tedy $f(S)$ je inverzní podpologrupa $\mathcal{I}_X$ izomorfní s S.*

Reference

[1] J. M. Howie. *Fundamentals of Semigroup Theory.* Clarendon Press, Oxford, 1995.

[2] N. Ruškuc. *Semigroups*, lecture notes, 2003.