Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE

Benjamin Vejnar

Abelovsky regulární okruhy

Katedra algebry

Vedoucí bakalářské práce: Mgr. Jan Žemlička, Ph.D.
Studijní program: Matematika, obecná matematika

2007

Děkuji vedoucímu práce Mgr. Janu Žemličkovi, Ph.D. za odborné rady k obsahu této práce a za zapůjčení vhodné literatury.

Prohlašuji, že jsem svou bakalářskou práci napsal samostatně a výhradně s použitím citovaných pramenů. Souhlasím se zapůjčováním práce a s jejím zveřejňováním.

V Praze dne 20. 5. 2007 Benjamin Vejnar

Obsah

Název práce: Abelovsky regulární okruhy
Autor: Benjamin Vejnar
Katedra (ústav): Katedra algebry
Vedoucí bakalářské práce: Mgr. Jan Žemlička, Ph.D.
E-mail vedoucího: *Jan.Zemlicka@mff.cuni.cz*

Abstrakt: V předložené práci studujeme aritmetické a strukturní vlastnosti abelovsky regulárních okruhů, tedy okruhů, jejichž každý levý i pravý konečně generovaný ideál je generován idempotentním prvkem, který leží v centru daného okruhu. Například každý Booleův okruh je abelovsky regulární.

Věnujeme se podmínkám, které uplně charakterizují třídu abelovsky regulárních okruhů, jako například silná regularita. Všímáme si souvislostí mezi Booleovou algebrou všech centrálních idempotentů daného okruhu a hlavními ideály. Dále popisujeme topologii na množině všech prvoideálů a uvědomujeme si, že splývá s topologií ultrafiltrů na Booleově algebře idempotentů.

Klíčová slova: okruhy, idempotentní prvky, silně regulární okruhy

Title: Abelian regular rings
Author: Benjamin Vejnar
Department: Department of Algebra
Supervisor: Mgr. Jan Žemlička, Ph.D.
Supervisor's e-mail address: *Jan.Zemlicka@mff.cuni.cz*

Abstract: In the present work we study arithmetic and structural properties of abelian regular rings. This means rings whose every left and right finitely generated ideal is generated by an idempotent element that lies in the center of the ring. For example every Boolean ring is abelian regular.

We attend to conditions, which completely characterize the class of abelian regular rings as for example strong regularity does. We observe connections between Boolean algebra of all central idempotents of a given ring and principal ideals. Next we describe topology on the set of all prime ideals and we realize that it coincides with the topology of ultrafilters on the Boolean algebra of idempotents.

Keywords: rings, idempotent elements, strongly regular rings

Předmluva

Regulární okruhy zkoumal von Neumann[1] ve třicátých letech minulého století. Pojem silně regulárního okruhu pak zavedli v polovině minulého století Arens[2] a Kaplansky[3], když se zabývali studiem topologických reprezentací algeber (Goodearl [2], str. xv). Abelovsky regulární okruhy mají řadu zobecnění. Jedním z nich jsou například regulární okruhy s omezeným indexem nilpotence.

Abelovsky regulární okruhy lze charakterizovat mnoha, na první pohled zcela rozdílně vypadajícími, podmínkami. Rozhodl jsem se přijmout za definici tu, která se mi zdá být nejpřirozenější a díky které snadno odvodíme důsledky, jež jsou nutné pro dobrou představu o této třídě okruhů. Samozřejmě dokážeme, že vybraná definice je ekvivalentní s tou ze zadání.

V první kapitole si ujasňujeme základní pojmy jako okruh, obor, těleso, prvoideál v okruhu. Uvádíme tvrzení obecného charakteru, na které se pak budeme v dalším textu odvolávat.

V druhé kapitole se věnujeme Booleovým okruhům a uvědomujeme si, že abelovsky regulární okruhy mají velice blízko ke komutativním okruhům v tom smyslu, že obsahují pouze oboustranné ideály. Ukazuje se, že mají distributivní svaz ideálů, protože součin ideálů odpovídá jejich průniku. Speciálně jsou všechny ideály idempotentní. Tyto okruhy lze také vnořit do součinu těles.

Třetí kapitola pojednává o tom, na které ze základních operací je třída abelovsky regulárních okruhů uzavřena.

Ve čtvrté kapitole definujeme pojem silně regulárního okruhu, přestože ihned zjistíme, že tato definice nepřináší nic nového.

Pátá kapitola obsahuje několik ekvivalentních popisů abelovsky regulárních okruhů pomocí regularity, vlastností svazu ideálů nebo neexistence nenulových nilpotentních prvků.

Následující kapitola si všímá vztahu idempotentních prvků a svazu hlavních ideálů, dále korespondence ideálů Booleovy algebry na centrálních idempotentech a ideálů okruhu.

V poslední kapitole popisujeme souvislost topologie na množině prvoideálů a na ultrafiltrech Booleovy algebry idempotentních prvků.

V tomto textu jsem se nezabýval vlastnostmi modulů nad abelovsky regulárními okruhy. Jednak proto, že první přednášku o modulech jsem absolvoval až ve třetím roce studia, kdy už jsem měl bakalářskou práci zadanou, ale také proto, že použití modulů by ve většině případů neumožnilo rychleji dospět ke kýženým výsledkům.

Některá tvrzení bychom mohli zobecnit i pro okruhy, které neobsahují jednotkový prvek. Jinde je ovšem existence jednotkového prvku vhodná (například pro existenci maximálních ideálů). Kvůli jednoduššímu vyjadřování budeme existenci jednotkového prvku předpokládat vždy.

Důkazy tvrzení se snažím podávat co nejstručněji. Je–li například tvrzení ve tvaru ekvivalence, objeví se v důkazu symboly $(\Leftarrow), (\Rightarrow)$, které označují, jakou implikaci právě dokazujeme. Podobně je tomu při důkazu rovnosti dvou množin. Užijeme symboly $(\subseteq), (\supseteq)$ pro znázornění právě dokazované inkluze.

[1] John von Neumann, 1903 – 1957

[2] Richard Friedrich Arens, 1919 – 2000

[3] Irving Kaplansky, 1917 – 2006

Kapitola 1

Předběžnosti

Okruhem máme v celém textu vždy na mysli asociativní okruh s jednotkovým prvkem, tedy šestici $(R, +, -, 0, \cdot, 1)$. Většinou píšeme jen „okruh R“, pokud jsou příslušné operace zřejmé z kontextu. V okruhu připouštíme i možnost $0 = 1$, okruh je pak jednoprvkový a takové nazýváme triviální. Oborem označujeme okruh bez dělitelů nuly, ve kterém platí axiom netriviality $0 \neq 1$. Těleso je pro nás obor, ve kterém jsou všechny nenulové prvky invertibilní. Tělesa také nemusí být komutativní. Předpokládáme platnost axiomu výběru (užíváme ho ve formě Zornova lemmatu), především pro existenci maximálních ideálů v okruhu. Jeho použití nikde explicitně nezmiňujeme. Písmenem $\mathbb{N}$ značíme množinu přirozených čísel $\{1, 2, 3, \dots\}$. Speciálně proto $0 \notin \mathbb{N}$.

Následující definice a tvrzení mají obecnou povahu a nezařazujeme je proto do jednotlivých kapitol, ve kterých je budeme užívat. Tato tvrzení uvádíme bez důkazů.

Definice Oboustranný vlastní ideál P okruhu R se nazývá prvoideál, pokud pro libovolné oboustranné ideály I, J okruhu R platí implikace $IJ \subseteq P \Rightarrow I \subseteq P$ nebo $J \subseteq P$. To je možné ekvivalentně vyjádřit tak, že pro každá $a, b \in R$ platí implikace $aRb \subseteq P \Rightarrow a \in P$ nebo $b \in P$.

Tvrzení 1.1 Buď R okruh a $x \in \bigcap\{P : P \text{ prvoideál}\}$. Pak x je nilpotentní.

Tvrzení 1.2 Je–li R okruh a P jeho prvoideál, pak existuje prvoideál $Q \subseteq P$, který je mezi všemi prvoideály (vzhledem k inkluzi) minimální.

Definice Ideál I okruhu R se nazývá poloprvoideál, pokud je průnikem nějaké množiny prvoideálů okruhu R. Speciálně R je poloprvoideál, protože ho chápeme jako průnik prázdné množiny prvoideálů.

Tvrzení 1.3 Pro oboustranný ideál I okruhu R jsou následující podmínky ekvivalentní

(i) I je poloprvoideál okruhu R.
(ii) Pro každé $x \in R$ splňující $xRx \subseteq I$ platí, že $x \in I$.
(iii) Pro každý oboustranný ideál $J \subseteq R$ splňující $J^2 \subseteq I$ je $J \subseteq I$.
(iv) Pro každý pravý ideál $J \subseteq R$ splňující $J^2 \subseteq I$ je $J \subseteq I$.

Definice Je–li R netriviální okruh, pak Jacobsonovým[4] radikálem okruhu R nazýváme průnik všech maximálních pravých ideálů tohoto okruhu a značíme ho $J(R)$. Pro triviální okruh R definujeme $J(R) = \{0\}$. Jacobsonův radikál lze ekvivalentně popsat jako průnik všech maximálních levých ideálů a jedná se tedy o oboustranný ideál.

[4] Nathan Jacobson, 1910 – 1999

Tvrzení 1.4 Každé konečné těleso je komutativní.
Krátký důkaz je možné nalézt například v [4] na straně 200.

Definice Částečně uspořádaná množina $(M, \leq)$ se nazývá nahoru usměrněná, pokud pro každé $a, b \in M$ existuje $c \in M$ splňující $a \leq c$ a zároveň $b \leq c$.

Definice Ať $(A, \leq)$ je nahoru usměrněná množina, R_α pro $\alpha \in A$ okruhy a $f_{\alpha,\beta} : R_\beta \to R_\alpha$ okruhové homomorfismy splňující pro $\alpha \leq \beta \leq \gamma \in A$ podmínky $f_{\alpha,\beta} \circ f_{\beta,\gamma} = f_{\alpha,\gamma}$ a $f_{\alpha,\alpha} = \mathrm{id}_{R_\alpha}$. Pak limita diagramu tvořeného okruhy R_α a homomorfismy $f_{\alpha,\beta}$ se nazývá inverzní limitou systému $(R_\alpha, f_{\alpha,\beta})$.

Tvrzení 1.5 Inverzní limita systému $(R_\alpha, f_{\alpha,\beta})$ je izomorfní podokruhu součinu $\prod_{\alpha \in A} R_\alpha$ tvaru

$$\big\{(r_\alpha)_{\alpha \in A} : \text{ pro } \alpha, \beta \in A, \alpha \leq \beta \text{ je } f_{\alpha,\beta}(r_\beta) = r_\alpha\big\}.$$

Tvrzení 1.6 Kategorie je úplná, právě když v ní existují součiny a ekvalizátory.

Kapitola 2

Důsledky abelovské regularity

Definice Nechť $(R, +, -, 0, \cdot, 1)$ je okruh. Prvek $x \in R$ se nazývá regulární, pokud existuje $y \in R$ takové, že $xyx = x$.

Okruh R nazýváme (von neumannovsky) regulární, pokud je každý jeho prvek regulární.

Okruh R se nazývá abelovsky regulární, pokud je regulární a každý idempotent z R je centrální (tzn. leží v centru okruhu R).

Stojí za to poznamenat, že platí–li pro prvky x, y okruhu R rovnost $xyx = x$, pak $xyxy = xy$ a $yxyx = yx$. Prvky xy a yx jsou v takovém případě idempotentní.

Každé (obecně nekomutativní) těleso F je abelovsky regulárním okruhem. Jediné idempotentní prvky v tělese jsou totiž 0 a 1, které jistě komutují se všemi ostatními prvky. Je–li $0 \neq x \in F$, stačí položit $y = x^{-1}$, pak bude $xyx = x$. Pro $x = 0$ lze volit y libovolně a dostaneme také $xyx = x$.

Dalším příkladem abelovsky regulárního okruhu je Booleův[5] okruh (tj. okruh, ve kterém je každý prvek idempotentem). Dříve než toto ověříme, vyslovíme následující pomocné tvrzení.

Tvrzení 2.1 Je–li R netriviální Booleův okruh, pak $\mathrm{char}(R) = 2$ a okruh R je komutativní.

Důkaz Prvek $1 + 1$ je idempotent, tedy $1 + 1 = (1 + 1)^2 = 1 + 1 + 1 + 1$. Po odečtení dostáváme $1 + 1 = 0$, což znamená, že $\mathrm{char}(R) = 2$. Pro $x, y \in R$ je $x + y = (x + y)^2 = x^2 + xy + yx + y^2 = x + xy + yx + y$. Tedy $xy = -yx = yx$, a proto je okruh R komutativní. □

Nyní je ověření abelovské regularity Booleova okruhu R přímočaré, neboť z komutativity ihned plyne, že každý idempotent je centrální. Navíc pro $x \in R$ je $x \cdot x \cdot x = x^2 \cdot x = x \cdot x = x$.

V následujících tvrzeních se zabýváme vlastnostmi ideálů abelovsky regulárního okruhu. Ukážeme, že levé a pravé ideály splývají s oboustrannými ideály, konečně generované ideály s hlavními ideály a prvoideály s maximálními ideály. Navíc součin dvou ideálů se rovná jejich průniku.

Lemma 2.2 Každý pravý (levý) ideál I abelovsky regulárního okruhu R je oboustranným ideálem.

Důkaz Buď $x \in I$ a $r \in R$, chceme ukázat, že také $rx \in I$. Existuje $y \in R$, že $xyx = x$. Vynásobením prvkem y zprava dostáváme $xyxy = xy$, proto je xy idempotent, a tedy centrální. Platí, že $rx = rxyx = r(xy)x = xyrx \in xR \subseteq I$. □

[5] George Boole, 1815 – 1864

Tuto důležitou vlastnost budeme velice často mlčky využívat. V dalším textu budeme mluvit již jen o (oboustranných) ideálech.

Tvrzení 2.3 Buď R abelovsky regulární okruh. Pak každý konečně generovaný ideál I je generován idempotentem.

Důkaz (a) Nechť nejprve $I = xR$ je hlavní ideál. Pak existuje $y \in R$, že $xyx = x$. Vynásobením prvkem y zprava máme $xyxy = xy$, tedy xy je idempotent. Platí, že $xR = xyR$. Protože $x = xyx = (xy)x \in xyR$, je $xR \subseteq xyR$. Obrácená inkluze je zřejmá.

(b) Nechť nyní $I = xR + yR$. Pak podle (a) existují idempotenty $e, f \in R$, že $eR = xR$ a $fR = yR$. Prvek $e + f - ef$ je také idempotent, protože

$$(e+f-ef)(e+f-ef) = e^2+ef-e^2f+fe+f^2-fef-efe-ef^2+efef = e+f-ef.$$

Ukážeme, že $eR+fR = (e+f-ef)R$. Protože $(e+f-ef)e = e$ a $(e+f-ef)f = f$, je $e, f \in (e+f-ef)R$. Navíc $e + f - ef \in eR + fR$.

(c) Indukcí podle počtu generátorů ideálu I je důkaz završen. □

Můžeme si všimnout analogie principu inkluze a exkluze. Jsou–li $e_1, \ldots, e_n$ idempotenty v abelovsky regulárním okruhu R, pak generátorem ideálu $e_1R + \cdots + e_nR$ je idempotent

$$\sum_{\emptyset \neq I \subseteq \{1,\ldots,n\}} (-1)^{|I|+1} \prod_{i \in I} e_i.$$

Tvrzení 2.4 Je–li P prvoideál v abelovsky regulárním okruhu R, pak P je maximální ideál a R/P je těleso.

Důkaz Ukážeme nejprve, že R/P je obor. Volme proto $x, y \in R$ a předpokládejme, že platí $(x+P)(y+P) = 0$. Pak také $xy \in P$. Chceme dojít k závěru, že $x \in P$ nebo $y \in P$. K tomu stačí ukázat, že $yrx \in P$ pro každé $r \in R$. Zvolme tedy $r \in R$ libovolně. Víme, že existuje $a \in R$, pro které $rx = rxarx$. Pak platí rovnost $yrx = y(rx) = yrxarx = (arx)(yrx) = ar(xy)rx \in P$. Tedy R/P je opravdu obor.

Pro $x \in R \setminus P$ existuje $y \in R$, že $xyx = x$. Prvky xy a yx neleží v P a $xy + P$, $yx + P$ jsou idempotentní v R/P. Protože R/P je obor, platí že $xy + P = 1 + P = yx + P$.

Pokud by prvoideál P nebyl maximální, existoval by maximální ideál $P \subsetneq M \subsetneq R$ a M/P by byl netriviální vlastní ideál tělesa R/P. □

Tvrzení 2.5 Buď R regulární okruh, I, J ideály okruhu R. Potom $I \cap J = I \cdot J$ a svaz ideálů okruhu R je distributivní.

Důkaz Inkluze $(I \cap J) \supseteq IJ$ platí obecně pro libovolný okruh R. Pro důkaz opačné inkluze vezměme $r \in I \cap J$. Existuje $s \in R$, že $r = rsr = (rs)r \in IJ$. Tedy i $(I \cap J) \subseteq IJ$.

Pro ideály I, J, K platí díky první části důkazu

$$(I + J) \cap K = (I + J)K = IK + JK = (I \cap K) + (J \cap K).$$

□

Lemma 2.6 Je–li I maximální pravý ideál a e centrální idempotent v okruhu R, pak $e \in I$, právě když $1 - e \notin I$.

Důkaz ($\Rightarrow$) Pokud by $1 - e \in I$, pak $1 = (1 - e) + e \in I$, což by byl spor s maximalitou I.

($\Leftarrow$) $I + (1 - e)R \supsetneq I$, tedy podle maximality I je $I + (1 - e)R = R$. Neboli existuje $i \in I$ a $r \in R$, že $1 = i + (1 - e)r$. Přenásobením zleva idempotentem e dostáváme $e = ei = ie \in I$. □

Uvažujme nyní konkrétní příklad abelovsky regulárního okruhu

$$R = \{f : [0, 1] \to \mathbb{R} : f \text{ je po částech konstantní}\}$$

(s operacemi sčítání a násobení funkcí). Pro danou funkci $f \in R$, která se alespoň někde rovná nule, existuje mnoho prvků $g \in R$, že $fgf = f$. Mezi nimi má význačné postavení funkce g, pro kterou $g(x) = 0$, právě když $f(x) = 0$. Takové g má navíc vlastnost, že $gfg = g$. Zobecnění tohoto pozorování je nasnadě.

Tvrzení 2.7 Je–li R abelovsky regulární okruh, pak pro každé $x \in R$ existuje právě jedno $z \in R$, že $xzx = x$ a zároveň $zxz = z$.

Důkaz Existuje $y \in R$, že $xyx = x$. Položme $z = yxy$. Pak $xzx = xyxyx = xyx = x$. Navíc $zxz = (yxy)x(yxy) = y(xy)(xy)(xy) = yxy = z$. Stačí jen dokázat jednoznačnost z. Buď $v \in R$ splňující $xvx = x$ a $vxv = v$. Pak $vx = vxvx = v(xv)x = vx(xv) = (vx)xv = x(vx)v = xv$. Podobně $zx = xz$. Navíc $xv = xzxv = xvxz = xz$. Celkem dostáváme, že $v = vxv = vxz = xzv = zxv = zxz = z$. □

Tvrzení 2.8 Abelovsky regulární okruh R nemá žádné nenulové nilpotentní prvky.

Důkaz Předpokládejme, že $0 \neq x \in R$ má stupeň nilpotence $n \geq 2$. Existuje $y \in R$, že $xyx = x$, tedy i $x^2y = x$. Pak ovšem $0 = 0 \cdot y = x^n y = x^{n-2} \cdot x^2 y = x^{n-1}$, což je spor. □

Tvrzení 2.9 Buď R okruh, $J(R)$ Jacobsonův radikál tohoto okruhu a $e \in R$ idempotent. Pak $e \in J(R)$, právě když $e = 0$.

Důkaz ($\Rightarrow$) Je–li $1 - e$ zprava invertibilní, pak existuje $r \in R$, že $1 = (1 - e)r$. Potom ale $e = e(1 - e)r = 0$, tj. $e = 0$.

Není–li $1 - e$ zprava invertibilní, existuje maximální pravý ideál I, který tento prvek obsahuje. Pak ale $e \notin I$, tedy $e \notin J(R)$.

($\Leftarrow$) Zřejmé. □

Důsledek 2.10 V regulárním okruhu R je $J(R) = \{0\}$.

Důkaz Pro $x \in J(R)$ existuje $y \in R$, že $xyx = x$. Prvek $xy \in J(R)$ je idempotent, a tedy nula. Z toho plyne, že $x = 0$. □

Jsou–li K_α pro α z indexové množiny A tělesa, pak snadno ověříme, že okruh $\prod_{\alpha\in A} K_\alpha$ je abelovsky regulární. Následující věta říká, že každý abelovsky regulární okruh lze subdirektně vnořit do součinu těles.

Věta 2.11 Je–li R abelovsky regulární okruh, pak existují tělesa K_α pro $\alpha \in A$, že R je izomorfní subdirektnímu součinu $\prod_{\alpha\in A} K_\alpha$.

Důkaz Nechť I_α pro $\alpha \in A$ jsou všechny maximální ideály okruhu R. Pak pro každé $\alpha \in A$ je faktorokruh R/I_α tělesem, protože R/I_α má pouze triviální jednostranné ideály. Definujme zobrazení

$$\pi : R \to \prod_{\alpha\in A} R/I_\alpha \quad \text{předpisem} \quad r \mapsto (r + I_\alpha)_{\alpha\in A}.$$

Snadno lze nahlédnout, že π je okruhový homomorfismus s jádrem

$$\operatorname{Ker}\pi = \{r \in R : \forall_{\alpha\in A}\ r \in I_\alpha\} = \bigcap_{\alpha\in A} I_\alpha = J(R) = \{0\}.$$

Homomorfismus π je prostý, a proto $R \simeq \operatorname{Im}\pi$. □

Důsledek 2.12 Každý konečný abelovsky regulární okruh R je izomorfní součinu konečně mnoha konečných těles.

Důkaz Nechť I_α pro $\alpha \in A$ je minimální systém maximálních ideálů splňující $\bigcap_{\alpha\in A} I_\alpha = \{0\}$. Takový systém existuje, protože okruh R je konečný a má proto jen konečně mnoho maximálních ideálů. Nechť zobrazení π je definováno jako v důkazu věty 2.11. Díky minimalitě množiny A existuje pro každé $\alpha \in A$ prvek $r_\alpha \in R\backslash I_\alpha$, že $r_\alpha \in \bigcap_{\beta\neq\alpha} I_\beta$. Všimněme si, že $r_\alpha + I_\alpha \neq I_\alpha$ a pro $\beta \neq \alpha$ je $r_\beta + I_\beta = I_\beta$. Navíc R/I_α je těleso, proto existuje $s_\alpha \in R$, že $(r_\alpha + I_\alpha)(s_\alpha + I_\alpha) = 1 + I_\alpha$. Označíme–li ještě $t_\alpha = r_\alpha s_\alpha$, dostáváme, že $(t_\alpha + I_\beta)_{\beta\in A} = (\delta_{\alpha\beta} + I_\beta)_{\beta\in A}$. Nyní již pro libovolná $c_\alpha \in R$ platí

$$\pi\Big(\sum_{\beta\in A} c_\beta t_\beta\Big) = \Big(\sum_{\beta\in A} c_\beta t_\beta + I_\alpha\Big)_{\alpha\in A} = (c_\alpha t_\alpha + I_\alpha)_{\alpha\in A} = (c_\alpha + I_\alpha)_{\alpha\in A},$$

odkud je okamžitě vidět, že π je surjektivní. Podle věty 2.11 je π prosté, takže jde o hledaný izomorfismus. □

Poznámka Speciálně je proto každý konečný abelovsky regulární okruh komutativní, protože podle Wedderburnovy[6] věty je každé konečné těleso komutativní.

Každý konečný Booleův okruh R je izomorfní součinu konečně mnoha dvouprvkových těles, protože každý maximální ideál v R má podle lemmatu 2.6 právě $\frac{1}{2}|R|$ prvků. Navíc $|R|$ je mocnina dvojky a okruh R je svou mohutností zadán až na izomorfismus jednoznačně (je–li konečný).

[6] Joseph Henry Maclagen Wedderburn, 1882 – 1948

Příklad Okruh $\mathbb{Z}_n$ celých čísel modulo n je abelovsky regulární, právě když n není dělitelné čtvercem žádného prvočísla. Je–li totiž n dělitelné čtvercem prvočísla, obsahuje $\mathbb{Z}_n$ nilpotentní prvky. Pokud je naopak $n = p_1 \cdot \ldots \cdot p_k$ součin po dvou různých prvočísel, pak je podle čínské zbytkové věty $\mathbb{Z}_n$ izomorfní součinu těles $\mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_k}$.

Ze stejných úvah vyplývá, že prvookruhem abelovsky regulárního okruhu je buď okruh celých čísel $\mathbb{Z}$, nebo okruh celých čísel modulo $n \in \mathbb{N}$, kde n není dělitelné druhou mocninou žádného prvočísla.

Každý abelovsky regulární okruh lze vnořit do součinu těles. Existují ale takové, které nejsou izomorfní žádnému součinu těles. Uvažujme libovolné těleso F a podívejme se na komutativní okruh

$$R = \big\{f : \mathbb{N} \to F : f \text{ je od nějakého indexu konstantní}\big\}.$$

Okruh R není izomorfní součinu těles.

Označme pro jednoduchost

$$S = \prod_{\alpha \in A} F_\alpha,$$

kde F_α jsou tělesa pro $\alpha \in A$. Okruh R má spočetně nekonečně mnoho idempotentů. Rozlišme nyní dva případy. Je–li A konečná, pak S obsahuje jen konečně mnoho idempotentů. Pro A nekonečnou obsahuje okruh S nespočetně mnoho idempotentů. V žádném případě tedy nemůže být okruh R izomorfní s S.

K důkazu nám stačily jen velice hrubé znalosti o okruhu R, a sice to, že má spočetně nekonečně mnoho idempotentních prvků.

Nalezený součin těles z věty 2.11, do kterého se okruh R vnořuje může vypadat velice komplikovaně, přestože samotný okruh R máme přímo zadán jako součin těles. Uvažujme například okruh $R = \mathbb{R}^{\mathbb{N}}$ a ať I je ideál všech skoro všude nulových posloupností reálných čísel. Dle Zornova lemmatu existuje maximální ideál M obsahující I. Tvrdíme, že těleso R/M není izomorfní s $\mathbb{R}$.

Ukážeme dokonce, že neexistuje homomorfismus $f : R \to \mathbb{R}$ s jádrem M. Předpokládejme pro spor, že takový existuje. Pak pro $r_n \in \mathbb{R},\ r_n \geq 0$ existují s_n, že $s_n^2 = r_n$. Proto $f((r_n)_{n\in\mathbb{N}}) = f((s_n^2)_{n\in\mathbb{N}}) = f((s_n)_{n\in\mathbb{N}})^2 \geq 0$. Pro $c \in \mathbb{Z}$ platí $f((c)_{n\in\mathbb{N}}) = c$. Speciální volbou $r_n = n$ pro $n \in \mathbb{N}$ dostáváme (díky tomu, že jádro f obsahuje ideál I), že

$$f((n)_{n\in\mathbb{N}}) - c = f((n-c)_{n\in\mathbb{N}}) = f((|n-c|)_{n\in\mathbb{N}}) \geq 0$$

pro libovolné $c \in \mathbb{Z}$. A to je spor.

V případě, že F je konečné těleso a κ kardinální číslo, pak pro okruh $R = F^\kappa$ platí, že všechny jeho faktory podle maximálních ideálů jsou izomorfní s F.

Ať M je maximální ideál okruhu R a označme $a = (a)_{\alpha\in\kappa} \in R$ pro $a \in F$. Definujme homomorfismus $f : F \to R/M$ předpisem $a \mapsto a + M$. Ten je prostý, protože M neobsahuje invertibilní prvky. Protože M je prvoideál v komutativním okruhu R a $\prod_{a\in F}(x-a) = 0 \in M$, existuje $a \in F$, že $x - a \in M$. Tedy f je také surjektivní.

Na závěr této kapitoly vyslovíme tvrzení, ze kterého okamžitě vyplyne, že pokud pro abelovsky regulární okruhy R, S existuje izomorfismus mezi $R[x]$ a $S[x]$, pak jsou i okruhy R, S izomorfní.

Tvrzení 2.13 Je–li R abelovsky regulární okruh, pak regulární prvky okruhu polynomů $R[x]$ jsou právě prvky z R.

Důkaz Zřejmě všechny prvky z R jsou regulární v $R[x]$. Na druhou stranu předpokládejme pro spor existenci polynomů $p, q \in R[x]$, že stupeň p je alespoň jedna a $pqp = p$. Označme $a \in R$ vedoucí koeficient polynomu p. Existuje $b \in R$, že $aba = a$, a položme $e = ab = ba \neq 0$. Definujme ideál $I = (1-e)R$ okruhu R. I je vlastní ideál, neboť $e \notin I$. Označme $\bar{p} = p + I[x]$, $\bar{q} = q + I[x] \in R[x]/I[x] = (R/I)[x]$. Vedoucí koeficient $a + I$ polynomu $\bar{p}$ je invertibilní, protože

$$(a + I)(b + I) = (b + I)(a + I) = e + I = 1 + I.$$

Celkově máme

$$\deg \bar{p} = \deg \bar{p}\bar{q}\bar{p} = \deg \bar{p} + \deg \bar{q} + \deg \bar{p} > \deg \bar{p}.$$

A to je spor. □

Kapitola 3

Zachovávání abelovské regularity

Ukážeme, které ze základních konstrukcí okruhů (součin, podokruh, faktorokruh, průnik) zachovávají abelovskou regularitu. Obecně nemusí být podokruh abelovsky regulárního okruhu abelovsky regulární, jak vidíme na příkladu tělesa $\mathbb{Q}$ a jeho podokruhu $\mathbb{Z}$, ale ukážeme, že centrum již tuto vlastnost mít musí. Snadno také nahlédneme, že okruh polynomů v jedné neurčité a stejně tak okruh $n \times n$ matic ($n \geq 2$) nad abelovsky regulárním okruhem jsou abelovsky regulární jen v triviálním případě, kdy je původní okruh nulový.

Tvrzení 3.1 Libovolný součin abelovsky regulárních okruhů je opět abelovsky regulárním okruhem.

Důkaz Snadné. □

Tvrzení 3.2 Je–li R libovolný okruh a R_α pro $\alpha \in A \neq \emptyset$ abelovsky regulární podokruhy, pak $\bigcap\limits_{\alpha \in A} R_\alpha$ je také abelovsky regulární okruh.

Důkaz Zřejmě všechny idempotenty $\bigcap\limits_{\alpha \in A} R_\alpha$ jsou centrální. Je–li $x \in \bigcap\limits_{\alpha \in A} R_\alpha$, pak podle tvrzení 2.7 existuje pro každé $\alpha \in A$ právě jedno $y_\alpha \in R_\alpha$, že $xy_\alpha x = x$ a $y_\alpha x y_\alpha = y_\alpha$. Zvolme $\alpha, \beta \in A$ a označme $r = y_\alpha,\ s = y_\beta$. Pak platí

$$r = rxr = r(xsxsxsx)r = (rx^2)s^3(x^2r) = xs^3x = s.$$

Proto $r \in \bigcap\limits_{\alpha \in A} R_\alpha$. Jde o regulární okruh. □

Tvrzení 3.3 Centrum $Z(R)$ abelovsky regulárního okruhu R je abelovsky regulární okruh.

Důkaz Buď $x \in Z(R)$. Pak existuje $y \in R$, že $xyx = x$. Položíme–li $z = yxy$, platí rovnost $xzx = x$. Stačí ukázat, že $z \in Z(R)$. Je–li $a \in R$ libovolné, pak

$$az = ayxy = xyay = yaxy = yxya = za.$$

(Druhá a čtvrtá rovnost plyne z toho, že idempotent xy je centrální, třetí z toho, že x je centrální.) □

Tvrzení 3.4 Faktorokruhy (homomorfní obrazy) abelovsky regulárních okruhů jsou opět abelovsky regulární.

Důkaz Buď R abelovsky regulární okruh a I jeho ideál. Pro $x \in R$ existuje $y \in R$, že $xyx = x$. Tím spíše $(x + I)(y + I)(x + I) = x + I$.

Potřebujeme ještě ukázat, že všechny idempotenty faktorokruhu R/I jsou centrální. Ukážeme, že dokonce všechny idempotenty tohoto faktorokruhu jsou

tvaru $e + I$ pro nějaký idempotent $e \in R$, odkud již okamžitě vyplyne, že jsou centrální. Zvolme tedy $r \in R$ takové, že $(r+I)^2 = (r+I)$, tj. $r^2 - r \in I$. Existuje $s \in R$, že $rsr = r$. Tvrdíme, že rs je hledaný idempotent, nebo–li $r - rs \in I$. Ovšem

$$r - rs = rsr - rs = r^2 s - rs = (r^2 - r)s \in I.$$

□

Tvrzení 3.5 Inverzní limita abelovsky regulárních okruhů je abelovsky regulární okruh.

Důkaz Nechť R_α pro $\alpha \in A$ jsou abelovsky regulární okruhy, $(A, \leq)$ nahoru usměrněná množina. Pro $\alpha, \beta \in A, \alpha \leq \beta$ nechť $f_{\alpha,\beta} : R_\beta \to R_\alpha$ jsou okruhové homomorfismy takové, že pro $\alpha \leq \beta \leq \gamma \in A$ je $f_{\alpha,\beta} \circ f_{\beta,\gamma} = f_{\alpha,\gamma}$ a $f_{\alpha,\alpha} = \mathrm{id}_{R_\alpha}$. Pak

$$R = \left\{(r_\alpha)_{\alpha\in A} : \text{ pro } \alpha, \beta \in A, \alpha \leq \beta \text{ je } f_{\alpha,\beta}(r_\beta) = r_\alpha\right\}$$

je inverzní limitou tohoto systému. Ukážeme nejprve, že okruh R je regulární.

Uvažme prvek $(r_\alpha)_{\alpha\in A} \in R$. Pak pro každé $\alpha \in A$ existuje právě jedno $s_\alpha \in R_\alpha$, že $r_\alpha = r_\alpha s_\alpha r_\alpha$ a $s_\alpha = s_\alpha r_\alpha s_\alpha$. Chceme ukázat, že $(s_\alpha)_{\alpha\in A} \in R$. Zvolme proto $\alpha \leq \beta \in A$ libovolně a označme pro jednoduchost $f = f_{\alpha,\beta}$. Protože f je okruhový homomorfismus, dostáváme

$$\begin{aligned} f(r_\beta) &= f(r_\beta)f(s_\beta)f(r_\beta), & f(s_\beta) &= f(s_\beta)f(r_\beta)f(s_\beta) \\ r_\alpha &= r_\alpha f(s_\beta) r_\alpha, & f(s_\beta) &= f(s_\beta) r_\alpha f(s_\beta). \end{aligned}$$

Z posledních dvou rovností díky tvrzení 2.7 vidíme, že nutně $f(s_\beta) = s_\alpha$. Tedy $(s_\alpha)_{\alpha\in A} \in R$.

Je–li $(e_\alpha)_{\alpha\in A} \in R$ idempotent okruhu R, pak zřejmě pro každé $\alpha \in A$ je e_α idempotent okruhu R_α, tedy leží v centru okruhu R_α. Proto i $(e_\alpha)_{\alpha\in A}$ je centrální idempotent okruhu R. □

Existence inverzní limity je také důsledkem obecnějších úvah. Kategorie všech abelovsky regulárních okruhů je totiž úplná, což lze zdůvodnit existencí součinů (limit diskrétních diagramů) a ekvalizátorů. Protože inverzní limita je limita nějakého speciálního diagramu, plyne z úplnosti dané kategorie její existence.

Tvrzení 3.6 Nechť $R \subseteq \prod_{\alpha\in A} K_\alpha$ je regulární podokruh součinu těles. Na každém tělese K_α uvažujme diskrétní topologii a na $\prod_{\alpha\in A} K_\alpha$ součinovou topologii. Pak uzávěr $\overline{R}$ okruhu R je abelovsky regulární okruh.

Důkaz Protože R je podokruh topologického okruhu $S = \prod_{\alpha\in A} K_\alpha$, je $\overline{R}$ opět okruhem. Zřejmě jsou všechny idempotenty v R centrální.

Zbývá dokázat regularitu okruhu $\overline{R}$. Pro $x \in \overline{R}$ existuje právě jedno $y \in S$, že $xyx = x$ a zároveň $yxy = y$. Ukážeme, že každé okolí prvku y protíná R, odkud již vyplyne $y \in \overline{R}$. Zvolme tedy konečnou podmnožinu $K \subseteq A$. Protože $x \in \overline{R}$, existuje $a \in R$, že $a_\alpha = x_\alpha$ pro $\alpha \in K$. Díky abelovské regularitě okruhu R existuje právě jedno $b \in R$, že $aba = a$ a $bab = b$. Nutně $b_\alpha = y_\alpha$ pro $\alpha \in K$. □

Kapitola 4

Silně regulární okruhy

Definice Okruh R se nazývá silně regulární, pokud pro každé $x \in R$ existuje $y \in R$, že $x^2y = x$.

Poznamenejme, že z následujícího tvrzení vyplyne, že každý silně regulární okruh je regulární, a proto předchozí definice není v rozporu s dobrými mravy.

Ukážeme dokonce, že okruh je silně regulární, právě když je abelovsky regulární. Předchozí definice se proto stává nadbytečnou. Uvádíme ji však z toho důvodu, že je stále některými autory používána.

Tvrzení 4.1 Okruh R je abelovsky regulární, právě když je silně regulární.

Důkaz ($\Rightarrow$) Pro $x \in R$ existuje $y \in R$, že $xyx = x$. Protože prvek xy je idempotent, je centrální, a tedy $x = xyx = x(xy) = x^2y$. Tudíž R je silně regulární.

($\Leftarrow$) Zvolme nyní $x \in R$ nilpotentní. Existuje $y \in R$, že $x^2y = x$. Pokud by $n \geq 2$ byl stupeň nilpotence prvku x, pak $0 = x^ny = x^{n-1}$. Celkově proto vidíme, že v R nejsou žádné nenulové nilpotentní prvky.

Ať opět $x \in R$ je libovolné a $y \in R$ splňuje rovnost $x^2y = x$. Pak

$$(x - xyx)^2 = x^2 - x^2yx - xyx^2 + xyx^2yx = x^2 - x^2 - xyx^2 + xyx^2 = 0.$$

Prvek $x - xyx$ je nilpotentní, a proto $x = xyx$. Dokázali jsme regularitu okruhu R.

Buď $e \in R$ idempotent a $r \in R$. Pak prvky $er(1-e)$, $(1-e)re$ jsou nilpotentní a tedy nulové. Z toho po roznásobení plyne, že $er = ere = re$. Proto je idempotent e centrální. □

Všimněme si, že podle právě dokázané ekvivalence platí díky symetrii pro okruh R ekvivalence

$$\forall_{x\in R}\exists_{y\in R}\ x^2y = x \quad \Leftrightarrow \quad \forall_{x\in R}\exists_{y\in R}\ yx^2 = x.$$

Tato ekvivalence obecně neplatí po prvcích. Uvažme například okruh endomorfismů $\mathrm{End}_K(V)$ spočetně dimenzionálního vektorového prostoru V nad tělesem K. Tvoří–li vektory $e_1, e_2, \dots \in V$ bázi prostoru V a definujeme–li $f \in \mathrm{End}_K(V)$ tak, aby $f(e_i) = e_{i+1}$ pro $i \in \mathbb{N}$, pak neexistuje $g \in \mathrm{End}_K(V)$, pro které by $f^2g = f$, protože obraz zobrazení $f^2 = f \circ f$ je roven lineárnímu obalu vektorů $e_3, e_4, \dots$, ale vektor $f(e_1) = e_2$ v něm neleží. Na druhou stranu existuje $h \in \mathrm{End}_K(V)$, že $hf^2 = f$. Stačí totiž definovat h tak, aby $h(e_1) = 0, h(e_{i+1}) = e_i$ pro $i \in \mathbb{N}$.

Zajímavá Jacobsonova věta říka, že okruh, ve kterém ke každému prvku x existuje $n \geq 2$, že $x^n = x$, je již komutativní. Uvědomme si, že každý takový okruh je speciálně silně regulární a lze ho tedy vnořit do součinu těles. Stačí

proto dokázat, že tělesa, jejichž multiplikativní grupa je torzní, jsou již komutativní. Na to je však ještě potřeba vynaložit jisté úsilí. Podrobnosti lze najít v knize od Hersteina[7] [4] na stranách 69 – 73, kde je vysloveno a dokázáno zobecnění tohoto tvrzení.

[7] Israel Nathan Herstein, 1923 – 1988

Kapitola 5

Charakterizace abelovsky regulárních okruhů

V této kapitole si uvědomíme, že v každém regulárním okruhu existuje nejmenší ideál takový, že faktorokruh podle tohoto ideálu má již všechny idempotenty centrální. Dále podáme několik ekvivalentních charakterizací abelovsky regulárních okruhů a ještě předtím dokážeme jedno pomocné tvrzení.

Tvrzení 5.1 V každém regulárním okruhu R existuje nejmenší ideál N, že R/N je již abelovsky regulární.

Důkaz Definujme množinu

$$M = \{J \subseteq R : J \text{ je oboustranný ideál a } R/J \text{ je abelovsky regulární}\}.$$

Množina M je neprázdná, protože $R \in M$. Položme $N = \bigcap M$, což je oboustranný ideál. R/N je zřejmě regulární a navíc existuje přirozeně vnoření okruhu R/N do součinu $\prod_{I \in M} R/I$. Odtud vidíme, že R/N je dokonce abelovsky regulární okruh. □

Tvrzení 5.2 Je–li R regulární okruh bez nenulových nilpotentních prvků a P minimální prvoideál, pak R/P je obor.

Důkaz Nejprve proveďme několik pozorovnání. Jsou–li $a, b \in R$ a $ab = 0$, pak $0 = b(ab)a = (ba)^2$, tedy $ba = 0$. Platí–li $a_1 \cdot \ldots \cdot a_n = 0$ pro $a_i \in R$, pak postupnou aplikací předchozí části dostáváme

$$a_2 \cdot \ldots \cdot a_n a_1 = 0,\ Ra_2 \cdot \ldots \cdot a_n a_1 = 0,\ a_1 R a_2 \cdot \ldots \cdot a_n = 0,\ \ldots,$$

až nakonec $(Ra_1R)\cdot\ldots\cdot(Ra_nR) = \{0\}$. Pokud je navíc σ permutace množiny $\{1, \ldots, n\}$, pak $(a_{\sigma 1}\cdot\ldots\cdot a_{\sigma n})^n \in (Ra_1R)\cdot\ldots\cdot(Ra_nR) = \{0\}$, proto $a_{\sigma 1}\cdot\ldots\cdot a_{\sigma n} = 0$.

Položme nyní $M = \{x_1 \cdot \ldots \cdot x_n : n \in \mathbb{N}, x_i \in R \setminus P\}$. Kdyby $0 \in M$, pak existují $x_i \in R\setminus P$, že $x_1\cdot\ldots\cdot x_n = 0$. Pak ovšem $(Rx_1R)\cdot\ldots\cdot(Rx_nR) = \{0\} \subseteq P$. A protože P je prvoideál, existovalo by $j \in \mathbb{N}$, pro které $Rx_jR \subseteq P$, tj. $x_j \in P$, což by byl spor. Takže $0 \notin M$ a vidíme, že množina M je multiplikativní. Podle Zornova lemmatu existuje maximální multiplikativní množina N obsahující M.

Definujme $Q = R\setminus N$. Ukážeme, že jde o ideál. Zvolme $a, b \in Q,\ r \in R$. Kvůli maximalitě N a díky pozorování existují $m, n \in N,\ i, j \in \mathbb{N}$, že $ma^i = 0,\ nb^j = 0$. Ovšem opět díky pozorování máme, že $mn(a + rb)^{i+j} = 0$. A protože $0 \notin N$, platí $a + rb \in R \setminus N = Q$.

Q je prvoideál, protože $R \setminus Q$ je multiplikativní množina. Nakonec díky minimalitě prvoideálu P dostáváme $P = Q,\ M = N$ a R/P je obor. □

Věta 5.3 Pro okruh R jsou následující podmínky ekvivalentní.
(i) R je abelovsky regulární.

(ii) R je silně regulární.
(iii) Každý levý i pravý konečně generovaný ideál je generován centrálním idempotentem.
(iv) R je regulární a neobsahuje nenulové nilpotentní prvky.
(v) Pro každé $x \in R$ existuje právě jedno $y \in R$, že $xyx = x$ a $yxy = y$.
(vi) R je regulární, přičemž levé a pravé ideály splývají.
(vii) R je regulární a R/P je oborem pro každý prvoideál P.
(viii) R neobsahuje nenulové nilpotentní prvky a faktorokruhy R podle prvoideálů jsou regulární.
(ix) R je regulární a svaz pravých ideálů je distributivní.
(x) Levé a pravé ideály jsou oboustranné a idempotentní.

Důkaz Podmínka (i) implikuje všechny ostatní a ekvivalence (i) $\Leftrightarrow$ (ii) byla předmětem kapitoly o silně regulárních okruzích.

(iii) $\Rightarrow$ (i) Pro libovolné $x \in R$ existuje idempotent $e \in R$, že $xR = eR$. Uvažujme $y, z \in R$, pro které $xy = e, x = ez$. Potom $xyx = ex = eez = ez = x$, čímž jsme ověřili regularitu okruhu R.

Je–li e libovolný idempotent v R, pak existuje centrální idempotent f, pro který $eR = fR$. Pak existuje $r \in R$, že $er = f$ a vynásobením prvkem e máme $er = ef$. Podobně existuje $s \in R$, že $e = fs$ a vynásobením centrálním idempotentem f dostáváme $ef = fs$. Závěrem je $e = fs = ef = er = f$, speciálně idempotent e je centrální.

(iv) $\Rightarrow$ (i) Je–li $e \in R$ idempotent, pak pro každé $r \in R$ jsou prvky $er(1-e), (1-e)re$ nilpotentní, a tedy nulové. Po roznásobení dostáváme $er = ere = re$, tedy e je centrální.

(v) $\Rightarrow$ (i) Zřejmě je okruh R regulární. Zvolme libovolně idempotent $e \in R$ a ukážeme, že $er(1-e) = 0$ pro každé $r \in R$. Z toho již vyplyne, že prvek e je centrální. Buď tedy $r \in R$ a položme $y = e + er(1-e)$. Protože $e^3 = e$, $eye = e$ a $yey = y$, plyne z jednoznačnosti, že $y = e$, neboli $er(1-e) = 0$.

(vi) $\Rightarrow$ (i) Buď $e \in R$ idempotent, ukážeme, že je centrální. Zvolme tedy $r \in R$. Protože eR je pravý a tedy i levý ideál, existuje $s \in R$, že $re = es$. Pak ovšem $(1-e)re = (1-e)es = 0$. Protože analogicky $er(1-e) = 0$, dostáváme rovnost $er = ere = re$.

(vii) $\Rightarrow$ (iv) Je–li $x \in R$ nilpotentní, pak $x + P = P$ pro každý prvoideál P, protože v oboru nejsou nenulové nilpotentní prvky. Tedy x leží v průniku všech prvoideálů. Ten je však podmožinou Jacobsonova radikálu. A podle důsledku 2.10 je $J(R) = \{0\}$.

(viii) $\Rightarrow$ (iv) Faktory R podle minimálních prvoideálů jsou podle tvrzení 5.2 obory a díky regularitě dokonce tělesa. Z toho plyne, že R/P je těleso pro libovolný prvoideál P.

Uvědomíme si, že pro oboustranný ideál I okruhu R platí, že R/I je bez nenulových nilpotentů, právě když I je poloprvoideál okruhu R. Implikace zleva doprava je zřejmá a obrácená platí díky tomu, že faktorokruh R/I můžeme vnořit do součinu těles R/P, kde P probíhá všechny prvoideály obsahující I, a tento součin neobsahuje nenulové nilpotentní prvky.

Předpokládejme pro spor, že existuje $x \in R$, že $x \notin xRx$. Uvažujme množinu

$$M = \{I \subseteq R : I \text{ ideál}, R/I \text{ neobsahuje nenulové nilpotenty}, I \cap (xRx - x) = \emptyset\}.$$

Podle předpokladů $\{0\} \in M$, proto $M \neq \emptyset$. Pro neprázdnou lineárně uspořádanou podmnožinu $C \subseteq M$ je $\bigcup C$ ideál, $\bigcup C \cap (xRx - x) = \emptyset$. Jsou–li $x \in R$,

$n \in \mathbb{N}$ taková, že $x^n \in \bigcup C$, pak existuje $I \in C$, že $x^n \in I$, ale protože R/I nemá nenulové nilpotentní prvky, dostáváme $x \in I \subseteq \bigcup C$. Proto ani $R/\bigcup C$ neobsahuje nenulové nilpotentní prvky. Celkově $\bigcup C \in M$ je horní mez C. Množina M je induktivní a podle Zornova[8] lemmatu má maximální prvek — označme ho I.

I není prvoideál. Existují tedy oboustranné ideály A, B, že $AB \subseteq I$ a $A, B \supsetneq I$. Definujme oboustranné ideály $K = \{r \in R : rB \subseteq I\}, L = \{r \in R : Kr \subseteq I\}$. Ukážeme, že K je poloprvoideál. Zvolme libovolně ideál J splňující $J^2 \subseteq K$. Dle definice je $J^2B \subseteq I$, čili také $(J \cap B)^3 \subseteq I$. A protože I byl poloprvoideál, je $J \cap B \subseteq I$, odkud $JB \subseteq I$, což znamená $J \subseteq K$. Stejnými argumenty dospějeme k závěru, že L je poloprvoideál. Snadno si uvědomíme, že $K \supseteq A$, $L \supseteq B$. Nyní máme $(K \cap L)^2 \subseteq KL \subseteq I$, odkud plyne $K \cap L \subseteq I$.

Díky maximalitě I v množině M existují $y, z \in R$, že $x - xyx \in K$, $x - xzx \in L$. Vidíme, že prvek

$$x - x(y + z - yxz)x = (x - xyx)(1 - zx) = (1 - xy)(x - xzx) \in K \cap L$$

leží v průniku $K \cap L$, tedy leží v I, čímž dostáváme spor.

(ix) $\Rightarrow$ (i) Pro idempotenty $e, f \in R$ platí $eR = eR \cap (fR + (1 - f)R) = eR \cap fR + eR \cap (1-f)R$. Existují tedy $r, s, t, u \in R$, že $e = er + es$, $er = ft$, $es = (1 - f)u$. Po úpravě $fe = fer + fes = fft + f(1 - f)u = ft = er$ dostáváme vynásobením zleva prvkem $1 - e$, že $(1 - e)fe = 0$. Podobně lze získat rovnost $ef(1 - e) = 0$. Idempotenty e, f spolu komutují, neboť $ef = efe = fe$.

Zvolíme nyní $x \in R$ libovolně a použijeme předchozí část pro idempotent $f = e + ex(1 - e)$. Vychází nám $e + ex(1 - e) = ef = fe = e$. Čili $ex(1 - e) = 0$. Podobně ovšem $(1 - e)xe = 0$. Idempotent e je centrální, neboť $ex = exe = xe$.

(x) $\Rightarrow$ (vi) Pro $x \in R$ platí $xR = Rx$ a $xR = xRxR = xRRx = xRx$, odkud plyne regularita okruhu R. □

Uvažujme nyní kladná celá čísla $n, k_1, \ldots, k_n, l_1, \ldots, l_{n-1}$, nezáporné celé číslo l_n a podmínku tvaru

$$\forall_{x \in R} \exists_{y \in R}\ x^{k_1} y^{l_1} \cdot \ldots \cdot x^{k_n} y^{l_n} = x. \qquad (\star)$$

Budeme se zabývat otázkou, kdy je třída okruhů splňujících podmínku $(\star)$ totožná s třídou všech abelovsky regulárních okruhů.

Tvrzení 5.4 Třídy splývají, právě když platí zároveň následující dvě podmínky

(i) Existuje celé $c \geq 0$, že $\sum k_i = c \cdot \sum l_i + 1$ (tj. $\sum l_i$ dělí $\sum k_i - 1$),

(ii) $\max\{k_1, \ldots, k_n\} \geq 2$.

Důkaz

($\Rightarrow$)

(i) Uvažujme těleso racionálních čísel $\mathbb{Q}$, což je speciálně abelovsky regulární okruh, a tedy podle předpokladu splňuje podmínku $(\star)$. Označme $k = \sum k_i$, $l = \sum l_i$ a zvolme $x = 2$. Pak podle $(\star)$ existuje $y \in \mathbb{Q}$, že $2^k y^l = 2$, neboli $y^l = 2^{1-k}$. Nutně proto l dělí $k - 1$, což jsme chtěli dokázat.

(ii) Předpokládejme pro spor, že $k_1 = \cdots = k_n = 1$. Pak podle již dokázané části (i) je $\sum l_i \leq \sum k_i - 1$, tedy nutně $l_1 = \cdots = l_{n-1} = 1$, $l_n = 0$. Pak

[8] Max August Zorn, 1906 – 1993

ovšem podmínku ($\star$) splňuje každý regulární okruh, a protože ne každý regulární okruh je abelovsky regulární, dostáváme spor.

($\Leftarrow$) Předpokládejme, že podmínky (i), (ii) jsou splněny. Chceme dokázat, že výše zmíněné třídy jsou totožné.

($\supseteq$) Ukážeme, že v každém abelovsky regulárním okruhu platí ($\star$). Zvolme $x \in R$ a k němu najděme $z \in R$, že $xzx = x$. Prvky x, z komutují. Ať opět $k = \sum k_i$, $l = \sum l_i$. Položme $d = \frac{k-1}{l}$ a $y = z^d$. Protože $x^k z^{k-1} = x$, dostáváme rovnost $x^k y^l = x$. Protože navíc prvky x, y komutují, splňují rovnost ($\star$).

($\subseteq$) Mějme okruh R, ve kterém platí ($\star$). Díky podmínce (ii) nejsou v R nenulové nilpotentní prvky, a proto je každý idempotent centrální. Pokud $l_n = 0$, pak díky ($\star$) pro $x \in R$ existuje $y \in R$, že

$$x(x^{k_1-1}y^{l_1} \cdot \ldots \cdot y^{l_{n-1}}x^{k_n-1})x = x.$$

Okruh R je v takovém případě regulární. Pokud $k_1 \geq 2$, pak díky ($\star$) je okruh R silně regulární. Předpokládejme tedy zbylou možnost, že $k_1 = 1$, $l_n \geq 1$. Zvolme pevně $x \in R$ a $y \in R$ ať je takové, že platí ($\star$). Označme nyní $z = x^{k_2-1}y^{l_2} \cdot \ldots \cdot x^{k_n}y^{l_n}y^{l_1}$. Pro libovolný prvoideál P je faktorokruh R/P oborem, neboť pro $a, b \in R \setminus P$ existuje $r \in R$ splňující $bra \notin P$ a díky podmínce (ii) a vztahu $bra = (bra)^{k_1}s^{l_1} \cdot \ldots \cdot (bra)^{k_n}s^{l_n} \in RabR$ pro vhodné $s \in R$ nemůže nastat $ab \in P$. Pro zjednodušení pišme dále $\bar{a} = a + P$ pro $a \in R$. Pokud $x \notin P$, pak můžeme v rovnosti

$$\bar{x}\bar{y}^{l_1} \cdot \ldots \cdot \bar{x}^{k_n}\bar{y}^{l_n} = \bar{x}$$

vykrátit zleva $\bar{x}$ a dostaneme

$$\bar{y}^{l_1}\bar{x}^{k_2}\bar{y}^{l_2} \cdot \ldots \cdot \bar{x}^{k_n}\bar{y}^{l_n} = \bar{1}.$$

Protože čísla l_1 i l_n jsou kladná, vidíme, že $\bar{y}$ je invertibilní v R/P. Tudíž násobením zleva prvkem $\bar{y}^{(-l_1)}$ a zprava prvkem $\bar{y}^{l_1}$ získáme rovnost

$$\bar{x}^{k_2}\bar{y}^{l_2} \cdot \ldots \cdot \bar{x}^{k_n}\bar{y}^{l_n}\bar{y}^{l_1} = \bar{1}$$

a po vynásobení prvkem $\bar{x}$ zprava máme $\bar{x}\bar{z}\bar{x} = \bar{x}$, nebo–li $xzx - x \in P$. Je–li $x \in P$, pak triviálně $xzx - x \in P$. Celkově proto $xzx - x$ leží v průniku všech prvoideálů okruhu R. Tento průnik je ovšem nulový, protože okruh R nemá nenulové nilpotentní prvky. Tedy $xzx - x = 0$, neboli $xzx = x$.

□

V předcházejících úvahách jsme se záměrně vyhnuli případu, kdy v podmínce ($\star$) nastane $k_1 = 0$. To znamená, že na obou stranách součinu na levé straně rovnosti se vyskytuje prvek y v kladné mocnině. Požadujeme–li, aby třída abelovsky regulárních okruhů splývala s třídou okruhů splňujících podmínku ($\star$), musí nutně platit podmínky (i), (ii) z přechozí věty. Na druhou stranu není jasné, zda okruh splňující podmínku ($\star$) již musí být abelovsky regulární. Toto lze díky větě 5.3 ekvivalentně přeformulovat na otázku, zda je každý obor R splňující ($\star$) již tělesem.

Kapitola 6

Booleova algebra na idempotentech

Definice V libovolném okruhu R definujme na množině $B(R)$ všech centrálních idempotentů binární relaci $\preceq$, unární operaci $\neg$ a binární operace $\wedge, \vee$ tak, že pro $e, f \in B(R)$ je

$$e \preceq f \;\Leftrightarrow\; e = ef, \quad \neg e = 1 - e, \quad e \wedge f = ef, \quad e \vee f = e + f - ef.$$

Tvrzení 6.1 Struktura $(B(R), \wedge, \vee, \neg, 0, 1)$ tvoří Booleovu algebru.

Důkaz Jedná se o přímočaré ověření definice Booleovy algebry. □

Připomeňme, že na Booleovu algebru $B(R)$ se můžeme dívat jako na svaz nebo jako na množinu částečně uspořádánou relací $\preceq$. Díky jednoznačné korespondenci Booleových algeber a Booleových okruhů bychom mohli mluvit o Booleových okruzích. Dáváme zde kvůli větší přehlednosti přednost terminologii Booleových algeber.

Lemma 6.2 Je–li R abelovsky regulární a $e, f \in R$ jsou takové idempotentní prvky, že $eR = fR$, pak $e = f$.

Důkaz Pokud $eR = fR$, existuje nějaké $s \in R$, že $e = fs$. Přenásobením této rovnosti prvkem f dostáváme $ef = fs$. Tedy $e = fs = ef$. Symetricky dostáváme, že $f = fe$. Celkem je proto $e = ef = fe = f$. □

Ukážeme, že Booleova algebra $B(R)$ v abelovsky regulárním okruhu R hraje velice důležitou roli. Určuje totiž například strukturu hlavních ideálů původního okruhu a svaz ideálů této algebry je izomorfní svazu ideálů původního okruhu.

Tvrzení 6.3 Je–li R abelovsky regulární okruh, pak svaz všech idempotentů okruhu R je izomorfní svazu všech hlavních ideálů okruhu R.

Důkaz Definujme zobrazení

$$\phi : B(R) \to \{rR : r \in R\}, \qquad e \mapsto eR.$$

Toto zobrazení je surjektivní díky tvrzení 2.3 a podle předchozího lemmatu 6.2 také prosté. Abychom ukázali, že ϕ je svazovým homomorfismem, stačí dokázat, že pro idempotenty $e, f \in R$ je $eR + fR = (e + f - ef)R$ a $eR \cap fR = efR$. První rovnost jsme již dokazovali v 2.3, druhá plyne z toho, že průnik ideálů se v tomto případě rovná jejich součinu, jak říká tvrzení 2.5. □

Tvrzení 6.4 Označme $B(X) = \{e \in X : e^2 = e\}$ pro libovolnou podmnožinu X abelovsky regulárního okruhu R. Pak zobrazení ϕ množiny všech ideálů

okruhu R do množiny všech ideálů v Booleově algebře $B(R)$ definované předpisem

$$\phi : I \mapsto \{e \in I : e^2 = e\} = B(I)$$

je svazovým izomorfismem.

Důkaz Zobrazení ϕ je dobře definované ($B(I)$ je ideál v $B(R)$ pro I ideál v R) a prosté. Ukážeme, že je také surjektivní. Uvažujme ideál L v Booleově algebře $B(R)$ a ať I je ideál v R generovaný množinou L. Stačí dokázat, že $\phi(I) = L$. Předpokládejme tedy, že $\sum c_i e_i \in I$ je idempotent, kde $c_i \in R, e_i \in L$. Bez újmy na obecnosti můžeme požadovat $e_i e_j = 0$ pro $i \neq j$. Máme $\sum c_i e_i = \left(\sum c_i e_i\right)^2 = \sum c_i^2 e_i$ a po vynásobení idempotentem e_j dostáváme $c_j^2 e_j = c_j e_j$ pro každé j. Nyní si stačí uvědomit, že existují $d_j \in R$, pro které $d_j c_j^2 = c_j$ a prvek

$$\sum c_i e_i = \sum d_i c_i^2 e_i = \sum d_i c_i e_i$$

leží v L.

Pro ideály $I, J \subseteq R$ je jistě $B(I \cap J) = B(I) \cap B(J)$. Označme $K = B(I) \vee B(J) \subseteq B(R)$ nejmenší ideál obsahující $B(I)$ a $B(J)$. Zřejmě $B(I + J) \supseteq K$, protože $B(I + J) \supseteq B(I)$ a $B(I + J) \supseteq B(J)$. Naopak je–li $i \in I$, $j \in J$, že $i + j$ je idempotent, pak existují $a, b \in R$, že $iai = i, jbj = j$. Prvky $ia \in I$, $jb \in J$ jsou idempotenty a $ia, jb \in K$. Pak $(ia \vee jb) \wedge (i + j) \in K$ a snadno spočítáme, že

$$(ia \vee jb) \wedge (i+j) = (ia+jb-iajb)(i+j) = iai+jbi-iajbi+iaj+jbj-iajbj = i+j.$$

Proto dohromady dostáváme $B(I + J) = B(I) \vee B(J)$. □

Kapitola 7

Topologie na spektru okruhu

Definice Je–li R okruh a $X \subseteq R$, označme

$$\mathrm{Spec}(R) = \{P \subseteq R : P \text{ prvoideál v } R\}, \quad \mathrm{Var}(X) = \{P \in \mathrm{Spec}(R) : X \subseteq P\}.$$

Tvrzení 7.1 Jsou–li I, J, I_α pro $\alpha \in A$ ideály okruhu R, pak

$$\text{(i)} \quad \bigcap_{\alpha\in A} \mathrm{Var}(I_\alpha) = \mathrm{Var}\Big(\bigcup_{\alpha\in A} I_\alpha\Big), \qquad \text{(ii)} \quad \mathrm{Var}(I) \cup \mathrm{Var}(J) = \mathrm{Var}(I \cdot J).$$

Důkaz (i) Je–li P prvoideál v R, pak

$$P \in \bigcap_{\alpha\in A} \mathrm{Var}(I_\alpha) \;\Leftrightarrow\; \forall_{\alpha\in A}\, P \in \mathrm{Var}(I_\alpha) \;\Leftrightarrow\; \forall_{\alpha\in A}\, P \supseteq I_\alpha \;\Leftrightarrow\; P \in \mathrm{Var}\Big(\bigcup_{\alpha\in A} I_\alpha\Big).$$

(ii) ($\subseteq$) Je–li prvoideál $P \in \mathrm{Var}(I) \cup \mathrm{Var}(J)$, pak $P \supseteq I$ nebo $P \supseteq J$. To znamená, že také $P \supseteq I \cdot J$, neboli $P \in \mathrm{Var}(I \cdot J)$.

($\supseteq$) Pro prvoideál $P \in \mathrm{Var}(I \cdot J)$ je $P \supseteq I \cdot J$ a z vlastností prvoideálu buď $P \supseteq I$ nebo $P \supseteq J$. Proto je $P \in \mathrm{Var}(I) \cup \mathrm{Var}(J)$. □

Poznámka Je–li R okruh, $X \subseteq R$ a $I \subseteq R$ ideál generovaný množinou X, pak je zřejmě $\mathrm{Var}(X) = \mathrm{Var}(I)$.

Definice Je–li R okruh, definujme na množině $\mathrm{Spec}(R)$ všech prvoideálů okruhu R Zariského[9] topologii τ tak, že uzavřené množiny budou tvaru $\mathrm{Var}(I)$ pro nějaký ideál $I \subseteq R$.

Podle předchozího tvrzení jde skutečně o topologii na množině $\mathrm{Spec}(R)$, neboť systém τ je uzavřený na libovolné průniky, konečná sjednocení a obsahuje $\emptyset = \mathrm{Var}(R)$ a celý prostor $\mathrm{Spec}(R) = \mathrm{Var}(\{0\})$.

Tvrzení 7.2 Prostor $\mathrm{Spec}(R)$ se Zariského topologií τ je kompaktní pro libovolný okruh R.

Důkaz Jsou–li $\mathrm{Var}(I_\alpha)$ pro $\alpha \in A$ libovolné uzavřené množiny s prázdným průnikem, pak $\emptyset = \bigcap_{\alpha\in A} \mathrm{Var}(I_\alpha) = \mathrm{Var}\Big(\bigcup_{\alpha\in A} I_\alpha\Big)$. To nastane právě v případě, že množina $\bigcup_{\alpha\in A} I_\alpha$ generuje ideál R. To znamená, že existuje $n \in \mathbb{N}$, $\alpha_1, \ldots, \alpha_n \in A$ a $r_1 \in I_{\alpha_1}, \ldots, r_n \in I_{\alpha_n}$, že $1 = r_1 + \cdots + r_n$. Pak je ovšem $\bigcap_{j=1}^{n} \mathrm{Var}(I_{\alpha_j}) = \mathrm{Var}\Big(\bigcup_{j=1}^{n} I_{\alpha_j}\Big) = \mathrm{Var}(R) = \emptyset$. □

[9] Oscar Zariski, 1899 – 1986

Tvrzení 7.3 Je–li R abelovsky regulární okruh, pak prostor $\mathrm{Spec}(R)$ se Zariského topologií τ je T_1 (tj. jednobodové množiny jsou uzavřené). Tento topologický prostor je dokonce Hausdorffův[10] a totálně nesouvislý.

Důkaz Stačí si uvědomit, že pro $P \in \mathrm{Spec}(R)$ je $\mathrm{Var}(P) = \{P\}$ uzavřená množina, protože podle tvrzení 2.4 je každý prvoideál zároveň maximálním ideálem.

Nechť $P, Q \in \mathrm{Spec}(R)$ jsou dva různé prvoideály. V následujícím najdeme disjunktní otevřené množiny $U, V \subseteq \mathrm{Spec}(R)$, že $P \in U, Q \in V$. Protože ideály P, Q jsou maximální a různé, existuje idempotent $e \in Q \setminus P$. Položme $F = \mathrm{Var}(eR), H = \mathrm{Var}\big((1-e)R\big)$. To jsou uzavřené množiny s vlastnostmi $P \notin F, Q \notin H$,

$$F \cup H = \mathrm{Var}(eR) \cup \mathrm{Var}\big((1-e)R\big) = \mathrm{Var}\big(eR \cap (1-e)R\big) = \mathrm{Var}\big(\{0\}\big) = \mathrm{Spec}(R).$$

Stačí jen položit $U = F^c, V = H^c$. Prostor $\mathrm{Spec}(R)$ je proto Hausdorffův.

Předpokládejme nyní pro spor, že dva různé body $P, Q \in \mathrm{Spec}(R)$ leží ve stejné komponentě souvislosti. Pak stejně jako v předchozím najdeme uzavřené množiny $F = \mathrm{Var}(eR), H = \mathrm{Var}\big((1-e)R\big)$. Protože každý ideál $P \in \mathrm{Spec}(R)$ obsahuje podle lemmatu 2.6 právě jeden z idempotentů $e, 1-e$, je $F \cap H = \emptyset$. Protože navíc $F \cup H = \mathrm{Spec}(R)$, jsou množiny F, H uzavřené i otevřené, což je spor s tím, že body P, Q leží ve stejné komponentě souvislosti. □

Definice Pro libovolnou Booleovu algebru B a $e \in B$ označme $\widehat{e} = \{U \in \mathrm{Ult}(B) : e \in U\}$. Definujme na prostoru $\mathrm{Ult}(B)$ všech ultrafiltrů na B topologii tak, že báze otevřených množin bude $\{\widehat{e} : e \in B\}$.

Poznámka Tento systém opravdu tvoří bázi nějaké topologie, protože pro $e, f \in B$ a $U \in \widehat{e} \cap \widehat{f}$ libovolné, je $U \in \widehat{e \wedge f} \subseteq \widehat{e} \cap \widehat{f}$. (Daný systém je dokonce uzavřený na konečné průniky.)

Stejnou topologii na $Ult(B)$ lze zadat také tak, že uzavřené množiny budou právě tvaru $\{U \in \mathrm{Ult}(B) : F \subseteq U\}$ pro nějaký filtr F.

Máme–li zadaný nějaký okruh R, můžeme uvažovat topologii definovanou na ultrafiltrech na Booleově algebře všech centrálních idempotentů $\mathrm{Ult}\big(B(R)\big)$, nebo topologii definovanou na spektru prvoideálů $\mathrm{Spec}(R)$. Tyto topologie jsou obecně různé. V případě, že okruh R je abelovsky regulární, obě topologie splývají, což vidíme z následujícího tvrzení.

Tvrzení 7.4 Pro abelovsky regulární okruh R je topologický prostor $\mathrm{Spec}(R)$ se Zariského topologií homeomorfní prostoru $\mathrm{Ult}\big(B(R)\big)$ všech ultrafiltrů na Booleově algebře všech idempotentů okruhu R.

Důkaz Jde o důsledek existence svazového izomorfismu mezi ideály okruhu R a Booleovy algebry $B(R)$ (viz tvrzení 6.4) a jednoznačné korespondence maximálních ideálů v $B(R)$ a ultrafiltrů. □

Příklad Buď p prvočíslo, $2 \leq n \in \mathbb{Z}$. Okruh $\mathbb{Z}_{p^n}$ není abelovsky regulární, ale topologické prostory na ultrafiltrech na Booleově algebře idempotentů a na spektru prvoideálů jsou jednoprvkové, a proto homeomorfní.

[10] Felix Hausdorff, 1868 – 1942

Literatura

[1] Anderson F. W.: K. R. Fuller, *Rings and Categories of Modules*, Springer, New York, 1992.

[2] Goodearl K. R.: *Von Neumann Regular Rings*, Krieger, Malabar, 1991.

[3] Herstein I. N.: *Noncommutative Rings*, The Mathematical Association of America, Spojené státy americké, 1960.

[4] Roman S.: *Field Theory*, Springer, New York, 1995.

[5] Sikorski R.: *Boolean Algebras*, Springer, Berlin, 1969.