Univerzita Karlova v Praze
Filozofická fakulta
Katedra logiky

Katrin Přikrylová

POJEM IDEÁLU A FILTRU V ALGEBŘE A LOGICE
IDEALS AND FILTERS IN ALGEBRA AND LOGIC

Bakalářská práce

Vedoucí práce: Mgr. Radek Honzík, Ph.D.

2013

Poděkování

Ráda bych tímto poděkovala svému vedoucímu panu doktoru Radku Honzíkovi, a to nejen za odborné rady, tematické nasměrování a technické tipy ohledně sazebního programu LaTeX, ale také za jeho trpělivost v průběhu celého vedení mé bakalářské práce.

Prohlášení

Prohlašuji, že jsem bakalářskou práci *Pojem ideálu a filtru v algebře a logice* vypracovala samostatně, že jsem řádně citovala všechny použité prameny a literaturu a že práce nebyla využita v rámci jiného vysokoškolského studia či k získání jiného nebo stejného titulu.

V Praze, 25. dubna 2013

Katrin Přikrylová

Abstrakt

Bakalářská práce *Pojem ideálu a filtru v algebře a logice* je sumarizací základního použití těchto pojmů, a to ve vybraných oblastech algebry (okruhy, Booleovy algebry) a logiky. Čtenář v ní nalezne definice i příklady užití v konkrétních důkazech či konstrukcích. Součástí práce je také historický exkurz, který mapuje zavedení pojmu *ideál* do matematiky, a to na pozadí hledání důkazu Velké Fermatovy věty.

Klíčová slova: ideál, filtr, logika, ideální čísla.

Abstract

Bachelor thesis *Ideals and Filters in Algebra and Logic* is a summary of the basic use of these concepts, namely in selected parts of algebra (rings, Boolean algebra) and logic. Readers can find the definitions and examples of the use of specific proofs and structures in the thesis. The work also contains a historical excursion which maps the introduction of the concept of *ideal* in mathematics on the background of searching for a proof of the Fermat's Last Theorem.

Keywords: ideal, filter, logic, ideal numbers.

Obsah

Kapitola 0

Úvod

Do rukou se vám dostala bakalářská práce, jejímž cílem je představení pojmů *ideál* a *filtr* v algebře a logice. Protože se jedná o velmi širokou oblast zájmu, není možné, abychom zde zaváděli všechny potřebné termíny. V následující sekci jsou tedy nastíněny předpokládané znalosti, které by měl již čtenář mít, aby bez potíží porozuměl samotné práci.

Jelikož se jedná především o sumarizační práci, předestíráme, že všechny uvedené důkazy byly již dříve dokázány a jsou ve většině případů nalezitelné v uvedené literatuře (důkazy, které v literatuře nejsou, vycházely ze znalostí autorky nabytých během studia – byly předneseny v semestrálních kurzech či se jedná o velmi triviální záležitosti, jejichž důkaz autoři použité literatury „nechávají na čtenáři“ či „za cvičení“). Podoba důkazu v literatuře a v této práci nemusí být absolutní – je možné, že se v práci užilo kompilace více technik z různých důkazů apod. – vždy však z uvedených zdrojů (či znalostí autorky).

0.1 Předpokládané znalosti

Tato práce si neklade za cíl představit problematiku ideálů a filtrů naprostému laikovi. Předpokládáme proto u čtenáře již nějaké počáteční znalosti.

A to zejména v oblasti klasické logiky (výrokové a predikátové) – práce s logickými spojkami a znalost vět (lépe i důkazu) o úplnosti a kompaktnosti.

Nadále zde bez nějakého širšího úvodu budeme hovořit o zobrazeních (zde by čtenář měl znát pojmy *isomorfismus*, *homomorfismus* apod.), o množinách (základní operace, de Morganovy zákony) a uspořádání.

Předpokládáme také základní znalosti z algebry, především co se týče vlastností struktur a operací na nich.

Všechny další pojmy by měly být řádně před použitím zadefinované. Abychom se vyhnuli případným nejasnostem či nedorozuměním, připojujeme níže stručnou tabulku s přehledem užitých symbolů.

0.2 Notační poznámky

V této práci budeme užívat následující symboly s těmito významy:

$+$	sčítání, aditivní operace
$\cdot$	násobení, multiplikativní operace
$\forall$	universální kvantifikátor
$\exists$	existenční kvantifikátor
$\subseteq$	podmnožina
$\subset$	vlastní podmnožina
$\emptyset$	prázdná množina
$\in$	být prvkem
$\cup$	sjednocení
$\cap$	průnik
$\equiv$	relace ekvivalence
$\wedge$	konjunkce
$\vee$	disjunkce
$\neg$	negace
$\rightarrow$	implikace
$\leftrightarrow$	ekvivalence

$\Rightarrow$	metajazyková implikace
$\Leftrightarrow$	metajazyková ekvivalence
$[a]$	ekvivalenční třída
R/I	rozklad
$\leq$	menší/rovno, relace uspořádání (neostrý predikát)
$<$	menší, relace uspořádání (ostrý predikát)
$\sqcup$	spojení
$\sqcap$	průsek
$\mathcal{P}(X)$	potence na množině X
$\bot$	spor
$\top$	tautologie
$\vdash$	predikát dokazování
$\models$	predikát vyplývání

0.3 Motivace

Ideály a filtry mají v logice a především v algebře své nezastupitelné místo. Využívá se jich k důkazům mnoha zásadních vět, a to v podstatě napříč několika matematickými obory. Tato práce by měla v omezené míře uvést čtenáře do této problematiky, představit pojem ideálu a filtru a nastínit základní využití v oblasti algebry a logiky. Jejich použití je však velmi široké a tato práce proto rozhodně neposkytuje ani zdaleka úplný výčet.

V kapitole 1 a 2 jsou představeny ideály a filtry v algebře – nejprve v okruzích, kde hrají významnou roli v tzv. větách o isomorfismu okruhů, a pak ve svazech – konkrétně v Booleových algebrách, v nichž se užívají pro dokázání Stoneovy věty.

Následující kapitola 3 se zabývá užitím filtrů v logice, konkrétně alternativním důkazem věty o úplnosti.

Součástí práce je také vhled do historie a zmapování zavedení ideálů do matematiky. Kapitola 4 tedy ukazuje cestu od tzv. *ideálních čísel*, která stála na počátku, přes motivaci zavedení ideálů až k samotné definici.

Kapitola 1

Ideály v okruzích

První oblastí, v níž si představíme použití ideálů, je algebra, konkrétně teorie okruhů. V ní ideály označují jistý podsystém okruhu s „žádoucími“ vlastnostmi, jichž se následně využívá při důkazu vět o isomorfismu okruhů. Než se však k těmto větám dostaneme, definujme si základní pojmy, s nimiž budeme pracovat.

1.1 Základní pojmy

Prvotním pojmem této kapitoly je *okruh*, jímž míníme algebraickou strukturu se dvěma binárními operacemi splňujícími určité axiomy.

Definice 1.1 (Okruh (komutativní)) *Množina R s binárními operacemi $+$, $\cdot$ a konstantami 1 a 0, předpokládejme $1 \neq 0$, (zapisujeme jako $\boldsymbol{R} = \langle R, +, \cdot, 1, 0 \rangle$) se nazývá* komutativní okruh, *jestliže pro všechny $x, y \in R$ platí:*

(a) Operace $\cdot$, $+$ jsou komutativní:

$x + y = y + x$;

$x \cdot y = y \cdot x$.

(b) Operace $\cdot$, $+$ jsou asociativní:

$(x + y) + z = x + (y + z)$;

$(x \cdot y) \cdot z = x \cdot (y \cdot z)$.

(c) Neutrální prvek pro operaci $+$:

$x + 0 = x$.

(d) Neutrální prvek pro operaci $\cdot$:

$x \cdot 1 = x$.

(e) Inverzní prvek pro operaci $+$: $\exists z \in R : (x + z = 0)$, značíme $z = -x$.

(f) Distributivita: $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

Pro opačný prvek jsme zavedli značení $-x$. Pro další použití si zavedeme také binární operaci $-$: Nechť $x, y \in R$, pak zápisem $x - y$ rozumíme $x + (-y)$.

Pokud bychom požadovali, aby struktura měla kromě inverzního prvku k $+$ také inverzní prvek k $\cdot$, vzniklo by nám již těleso:

Definice 1.2 (Těleso) *Nechť $\boldsymbol{R} = \langle R, +, \cdot, 1, 0 \rangle$ je komutativní okruh. Pak struktura $\boldsymbol{R}$ je také* těleso, *pokud pro všechny $x, y \in R$ platí:*

(a) $x \cdot y = 0 \Rightarrow x = 0 \vee y = 0$ (toto je dostačující podmínka pro tzv. obor integrity*).*

(b) Jestliže $y \neq 0$, pak existuje z takové, že $z \cdot y = 1$.

Dalším důležitým pojmem je *ideál*. Jeho definice se v okruzích a v následující kapitole zavedených svazech poněkud liší (po formální stránce). Uveďme si proto obě definice zvlášť a nejprve tu užívanou pro okruhy.

Definice 1.3 (Ideál v okruhu) *Množina $I \subseteq R$, kde R je okruh, se nazývá* ideál, *jestliže platí:*

(a) $I \neq \emptyset$,

(b) $\forall a, b \in I : a - b \in I$,

(c) $\forall a \in I, \forall r \in R : a \cdot r \in I$.

Budeme-li po ideálu požadovat ještě další vlastnosti, můžeme definovat speciální ideály:

Definice 1.4 *Nechť I je ideál, pak:*

(a) ***(Vlastní ideál)*** *Ideál I se nazývá* vlastní, *jestliže $1 \notin I$.*

(b) ***(Hlavní ideál)*** *Ideál I se nazývá* hlavní, *jestliže existuje $x \in R$ takové, že $I = \{x \cdot r | r \in R\}$. (Poznámka: Hlavní ideál je tedy takový, který je možno generovat jediným prvkem z okruhu.)*

(c) ***(Prvoideál)*** *Vlastní ideál I se nazývá* prvoideál, *jestliže $x \cdot y \in I$ implikuje, že buď $x \in I$, nebo $y \in I$.*

(d) ***(Maximální ideál)*** *Vlastní ideál I se nazývá* maximální, *jestliže neexistuje žádný vlastní ideál J takový, že $I \subset J$.*

1.2 Základní věty o ideálech

V duchu historického pojetí ideálních čísel i ideály odráží myšlenku seskupení prvků, které se liší jen velmi málo od určitého prvku dané algebry. Konkrétně u vlastního ideálu se v číselném okruhu jedná o čísla blízká k nule – v okruhu totiž nemají (stejně jako nula) multiplikativní inverz. Pokud by k $x \in I$ existovalo y takové, že $x \cdot y = 1$, pak z definice ideálu $1 \in I$ a $I = R$ a ideál by tedy nebyl vlastní.

Historický vývoj nám nabídl celkem tři věty o isomorfismu okruhů, k jejichž důkazu se využívá právě ideálů. Dokažme si tedy nejprve tvrzení potřebná k následným důkazům vět o isomorfismu okruhů.

Protože ideál I je podmnožinou okruhu, můžeme ukázat, že se ve skutečnosti chová dokonce jako jeho podgrupa:

Lemma 1.5 *Ideál I s operacemi $+$, $-$ a neutrálním prvkem 0 tvoří podgrupu $(R, +, -, 0)$.*

Důkaz: Dokážeme, že I je uzavřen na operace $+$ a $-$ a že obsahuje neutrální prvek.

- Uzavřenost operace $+$: Plyne triviálně z (a) definice 1.3.
- Uzavřenost operace $-$: Jestliže $x, y \in I$, pak z bodu (c) definice 1.3 plyne $y \cdot (-1) = -y$, $-y \in I$, a tedy $x + (-y) \in I$.
- $0 \in I$: Jestliže $I \neq \emptyset$, pak pro všechny $x \in I$ platí, že $x \cdot 0 = 0$. A podle bodu (b) z definice 1.3 je tedy $0 \in I$.

QED

Nyní si ještě zaveďme rozklad okruhu: Nechť pro každé $x \in R$ platí: $x + I = \{x + i | i \in I\}$. Pak systém $\mathcal{P} = \{x + I | x \in R\}$ tvoří rozklad okruhu R.

$$\bigcup \mathcal{P} = R$$

A navíc platí-li $x + I \neq y + I$, pak $x + I \cap y + I = \emptyset$. Definujme pro $x, y \in R$:

$$x \equiv_I y \Leftrightarrow x + I = y + I.$$

Je zřejmé, že $\equiv_I$ je ekvivalence na R.

Dokažme o právě definované ekvivalenci následující tvrzení:

Tvrzení 1.6 *Pro všechna $x, y \in R$ platí:*

(a) $x \equiv_I y \Leftrightarrow x - y \in I \Leftrightarrow y - x \in I$.

(b) Relace $\equiv_I$ je vzhledem k operacím v R kongruentní. Tedy můžeme utvořit rozklad R/I, který bude komutativním okruhem.

Důkaz: (a) Ze zavedení ekvivalence $\equiv_I$ víme $x + I = y + I$, tedy existují nějaká i a i' taková, že $x + i = y + i'$, tedy $x - y = i' - i$. A protože je ideál I uzavřen na operaci $-$, je zřejmé $i' - i \in I$.

Pokud naopak $x - y \in I$, pak existuje nějaké $i \in I$ takové, že $x - y = i$, tedy $x + 0 = y + i$. Protože 0 a i jsou prvku ideálu I, dostáváme: $x + I \cap y + I \neq \emptyset$.

A protože $\mathcal{P}$ je rozklad, platí $x + I = y + I$. Obdobně bychom tvrzení dokázali pro $y - x$.

(b) Předpokládejme, že $x \equiv_I x'$ a $y \equiv_I y'$. Dokážeme uzavřenost pro jednotlivé operace:

- Uzavřenost operace $+$: Chceme ukázat $x + y \equiv_I x' + y'$. To je však ekvivalentní s tvrzením $(x - x') + (y - y') \in I$, což platí z našeho předpokladu, že $x - x' \in I$ a $y - y' \in I$.

- Uzavřenost operace $-$: Chceme ukázat $-x \equiv_I -x'$, což je ekvivalentní s tvrzením $((-x) - (-x')) \in I$. Z definice ideálu plyne

$$(x - x') \in I \Rightarrow (-1) \cdot (x - x') = ((-x) - (-x')) \in I.$$

- Uzavřenost operace $\cdot$: Chceme ukázat: $x \cdot y \equiv_I x' \cdot y'$, což je opět ekvivalentní s $xy - x'y' \in I$. Z distributivity dostáváme

$$xy - x'y' = (x - x') \cdot y + x' \cdot (y - y') \in I.$$

  Což už platí na základě definice ideálu.

Můžeme tedy definovat faktorizaci okruhu R podle ideálu I, tj. R/I, takto:

- Definiční obor: $\mathcal{P} = \{x + I | x \in R\}$,
- $1_{R/I} = 1 + I$,
- $0_{R/I} = I$,
- $(x + I) + (y + I) = (x + y) + I$,
- $-(x + I) = (-x) + I$,
- $(x + I) \cdot (y + I) = x \cdot y + I$.

Nakonec stačí ověřit, že R/I je okruh. To je však již zřejmé z definice okruhu a z definice operací v R/I.
QED

1.3 Věty o isomorfismu okruhů

Věty o isomorfismu okruhů tvoří základní tvrzení pro další matematické konstrukce. Představují tak jednu z významných oblastí matematiky, v níž se ideály uplatňují.

Ačkoliv jsme v úvodu této práce předpokládali, že čtenář zná pojem *homomorfismus* (a související), zaveďme si řádnou definici. Budeme se k ní totiž často odkazovat v dalších důkazech.

Definice 1.7 *Nechť f je funkce z okruhu S do okruhu R ($f : S \to R$). Pak f je* homomorfismus, *pokud splňuje:*

(a) $f(1) = 1$,

(b) $f(0) = 0$,

(c) $f(x + y) = f(x) + f(y)$,

(d) $f(x \cdot y) = f(x) \cdot f(y)$,

(e) $f(-x) = -f(x)$.

Protože se však nepohybujeme v „obecné“ algebře, ale soustředíme se jen na okruhy, můžeme si vystačit s mírnějšími podmínkami:

Lemma 1.8 *Nechť R a S jsou okruhy a $f : R \to S$ je funkce, pak:*

(a) Aby f byl homomorfismus, postačují podmínky $\forall x, y \in R$:

- $f(1) = 1$,
- $f(x + y) = f(x) + f(y)$,
- $f(x \cdot y) = f(x) \cdot f(y)$.

(b) Jestliže f není konstantní funkce s hodnotou 0 a navíc S je obor integrity, pak je postačující podmínkou pouze $\forall x, y \in R$:

- $f(x + y) = f(x) + f(y)$,

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

Důkaz: (a) K důkazu postačuje ukázat, že $f(0) = 0$ a $f(-x) = -f(x)$. Protože S a R jsou okruhy, můžeme konstantu 0 a operaci $-$ definovat pomocí zbylých operací:

- $f(0) = 0$: $f(0) = (-f(0) + f(0)) + f(0) = -f(0) + f(0+0) = 0$,
- $f(-x) = -f(x)$: $f(-x) + f(x) = f(-x+x) = f(0) = 0$.

(b) Vyberme $x, y \in R$ takové, že $f(x) \neq 0$. Pak stačí vzhledem k důkazu v (a) ukázat, že $f(1) = 1$: $f(x) = f(1x) = f(1)f(x)$, tedy (protože S je obor integrity) $f(1) \neq 0$. Pro spor dále předpokládejme, že $f(1) \neq 1$. Ukážeme, že 1 je dělitel nuly, což v oboru integrity vede ke sporu:

$$1 \cdot 1 = 1 \Leftrightarrow f(1)f(1) = f(1) \Leftrightarrow f(1)f(1) - f(1) = 0 \Leftrightarrow f(1)(f(1) - 1) = 0,$$

kde $f(1)$ je nenulové, a protože jsme předpokládali $f(1) \neq 1$, je také $f(1) - 1$ nenulové, našli jsme tedy dělitele nuly v oboru integrity, což není možné, tedy $f(1) = 1$.
QED

Definice 1.9 *Nechť $f : R \to S$ je okruhový homomorfismus. Pak:*

(a) Jádro homomorfismu f *je množina* $ker(f) = \{x \in R | f(x) = 0\}$.

(b) Obraz homomorfismu f *je množina* $Im(f) = \{f(x) | x \in R\}$.

Nyní již víme vše potřebné, abych mohli pronést a dokázat jednotlivé věty o isomorfismu okruhů.

Věta 1.10 (První věta o isomorfismu okruhů) *Nechť $f : R \to S$ je okruhový homomorfismus na komutativních okruzích. Pak $ker(f)$ je ideál okruhu R a navíc platí $R/ker(f)$ je isomorfní s $Im(f)$.*

Důkaz: Nejdříve ukážeme, že $ker(f)$ je ideál okruhu R. Protože f je surjektivní, je $ker(f)$ neprázdné, tedy existuje nějaké $x \in R$ takové, že $f(x) = 0$. Jestliže dále $x, y \in ker(f)$, pak $f(x+y) = f(x) + f(y) = 0$, tedy $x + y \in ker(f)$. Když $r \in R$ a $x \in ker(f)$, pak také $f(r \cdot x) = f(r) \cdot f(x) = 0$, a tedy $r \cdot x \in ker(f)$. Ideál $ker(f)$ je navíc vlastní, protože $f(1) = 1 \neq 0$.

Definujme homomorfismus $h : R/ker(f) \to S$ takto: $h(x + ker(f)) = f(x)$. Ověříme, že se jedná o homomorfismus:

- Konstanta 0: $h(0 + ker(f)) = f(0) = 0$.
- Konstanta 1: $h(1 + ker(f)) = f(1) = 1$.
- Operace $-$: $h(-(x + ker(f)) = f(-x) = -f(x) = -h(x + ker(f))$.
- Operace $+$: $h((x + ker(f)) + (y + ker(f))) = h((x + y) + ker(f)) = = f(x + y) = f(x) + f(y) = h(x + ker(f)) + h(y + ker(f))$.
- Operace $\cdot$: $h((x + ker(f)) \cdot (y + ker(f))) = h(x \cdot y + ker(f)) = = f(x \cdot y) = f(x) \cdot f(y) = h(x + ker(f)) \cdot h(y + ker(f))$.

Funkce h je navíc prostá: $h(x + ker(f)) = h(y + ker(f)) \Leftrightarrow f(x) = f(y) \Leftrightarrow \Leftrightarrow f(x) - f(y) = 0 \Leftrightarrow f(x - y) = 0 \Leftrightarrow x - y \in ker(f) \Leftrightarrow x + ker(f) = = y + ker(f)$. Protože $Im(h) = \{h(x + ker(f)) | x \in R/ker(f)\} = \{f(x) | x \in R\}$, je $f : R/ker(f) \to Im(f)$ isomorfismus.
QED

Věta 1.11 (Druhá věta o isomorfismu okruhů) *Nechť R je okruh a S podokruh okruhu R a nechť I je ideál okruhu R. Pak platí:*

- *$S + I = \{s + i | s \in S, i \in I\}$ je podokruh okruhu R.*
- *$S \cap I$ je ideál podokruhu S.*
- *$(S + I)/I$ je isomorfní s $S/(S \cap I)$.*

Důkaz: Uvažujme zobrazení $f : S \to (S+I)/I$, kde $f(s) = s + I$. Z již dokázaného je zřejmé, že se jedná o okruhový homomorfismus, navíc o surjektivní: $(s+i)+I \in (S+I)/I$, kde $s \in S, i \in I \Rightarrow f(s) = s+I = s+(i+I) = (s+i)+I$.

Z první věty o isomorfismu okruhů plyne, že $S/ker(f)$ je isomorfní s $(S+I)/I$. Stačí nám tedy ukázat, že $ker(f) = S \cap I$.

Nechť $x \in ker(f)$. Pak $I = f(x) = x+I$, tedy $x \in I$. Dále platí $ker(f) \subseteq S$, tedy $x \in S$. Proto $x \in S \cap I$, a tedy $ker(f) \subseteq S \cap I$.

Pro opačný směr uvažujme $x \in S \cap I$. Pak $x \in I$, tedy $f(x) = x + I = I$. Proto platí $x \in ker(f)$ a také $S \cap I \subseteq ker(f)$.
QED

Věta 1.12 (Třetí věta o isomorfismu okruhů) *Nechť R je okruh a I, J jsou ideály okruhu R takové, že platí: $J \subseteq I \subseteq R$. Pak I/J je ideál faktorizace R/J a okruh $(R/J)/(I/J)$ je isomorfní s R/I.*

Důkaz: Uvažujme zobrazení $f : R/J \to R/I$, kde $f(x+J) = x+I$. Jedná se o dobře definované zobrazení, neboť $x+J = y+J$ implikuje $x-y \in J \subseteq I$, tedy z definice zobrazení: $f(x) = x+I = y+I = f(y)$. Ukážeme, že f je surjektivní homomorfismus.

Zvolme $x+J$, $y+J \in R/J$. Pak platí $f((x+J)(y+J)) = f(xy+J) =$ $= xy+I = (x+I)(y+I) = f(x)f(y)$ pro násobení a $f((x+J)+(y+J)) =$ $= f((x+y)+J) = (x+y)+I = (x+I)+(y+I) = f(x)+f(y)$ pro sčítání. Zřejmě platí $f(x+J) = x+I = 0+I \Leftrightarrow x \in I$, tedy $x \in ker(f) \Leftrightarrow x \in I/J$. Můžeme tedy použít první větu o isomorfismu okruhů, z níž už je důkaz zřejmý.
QED

Věty o isomorfismu okruhů jsou jen speciálním případem obecných vět o isomorfismu (které je možné konkretizovat nejen pro okruhy, ale také pro grupy a moduly). Kromě tří výše uvedených vět bývá k dispozici dávána ještě jedna věta – anglicky označována jako *Lattice theorem* či prostě čtvrtá věta o isomorfismu. Nevztahuje se však už čistě k okruhům, nýbrž právě ke grupám.

Jedním z praktických příkladů využití vět o isomorfismu je například konstrukce komplexních čísel na základě zobrazení $f : \mathbb{R}[X] \to \mathbb{C}$.

Kapitola 2

Ideály a filtry ve svazech

V této kapitole se blíže seznámíme s funkcí ideálů a filtrů ve svazech, především na Booleových algebrách. Než však k této problematice přistoupíme, představíme si v návaznosti na předchozí kapitolu *Booleovy okruhy*.

2.1 Booleovy okruhy

Vycházejíce z definice okruhu v předchozí kapitole, definujme nejmenší netriviální okruh, tedy okruh se dvěma prvky – 0 a 1. Jejich chování ve spojení s operacemi + a · zachycují následující tabulky:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

V okruhu se dvěma prvky je každý z prvků svým inverzem pro sčítání: $x + x = 0$ a současně je vzhledem k násobení idempotentní, tj. platí $x \cdot x = x$. Okruh, jehož všechny prvky jsou vzhledem k násobení idempotentní prvky, nazvěme *idempotentní okruh*.

Definice 2.1 (Booleův okruh) *Idempotentní okruh s jednotkovým prvkem je* Booleův okruh.

Nejjednodušším Booleovým okruhem je právě výše představený okruh se dvěma prvky {0,1}.

Protože jsme v definici Booleova okruhu požadovali, aby byl idempotentní, získali jsme jako důsledek další zajímavou vlastnost: Booleovy okruhy jsou vždy komutativní okruhy.

Tvrzení 2.2 *Booleův okruh je komutativní okruh, tedy operace $\cdot$ je komutativní a platí $x \cdot y = y \cdot x$.*

Důkaz: Spočítejme v okruhu výraz $(x+y)^2$. Díky idempotenci a distributivitě víme, že

$$x + y = (x + y)^2 = x^2 + x \cdot y + y \cdot x + y^2 = x + x \cdot y + y \cdot x + y,$$

tedy zkráceně vztah

$$x + y = x + x \cdot y + y \cdot x + y.$$

Po přičtení inverzního prvku k x zleva a přičtení inverzního prvku k y zprava dostáváme, že

$$0 = x \cdot y + y \cdot x. \tag{1}$$

Za použití idempotence a dosazením $x = y$ do výrazu v (1) získáme $x+x = x^2+x^2 = 0$. A protože má Booleův okruh charakteristiku 2 (tj. nejmenší počet sečtení jednotkového prvku okruhu k získání nulového prvku okruhu je 2), získáváme, že každý prvek je roven svému inverzu, tedy také $x \cdot y = -(x \cdot y)$. Přičteme-li proto k rovnici (1) na levou stranu $x \cdot y$ a na pravou $-(x \cdot y)$ získáme vztah

$$x \cdot y = x \cdot y + y \cdot x + (-(x \cdot y)) = y \cdot x + 0 = y \cdot x.$$

QED

Jako důsledek můžeme speciálně pro Booleovy okruhy upravit jeden bod definice okruhu. Konkrétně vztah $x + (-x) = 0$ můžeme psát jako $x + x = 0$.

Vztah mezi Booleovými okruhy a Booleovými algebrami bude předveden dále, ve větě 2.17.

2.2 Základní definice

Než se dostaneme k samotné definici svazu, popř. ideálu ve svazech, seznámíme se s několika dalšími termíny, které budeme v této kapitole (a dalších) využívat.

Definice 2.3 *Nechť X je množina a $Y \neq \emptyset$, $Y \subseteq X$. Pak:*

(a) ***(Horní závora)*** *Prvek $a \in X$ je* horní závora *množiny Y, jestliže* $\forall x \in Y : x \leq a$.

(b) ***(Dolní závora)*** *Prvek $a \in X$ je* dolní závora *množiny Y, jestliže* $\forall x \in Y : a \leq x$.

(c) ***(Maximální prvek)*** *Prvek $a \in Y$ je* maximální prvek *množiny Y, jestliže* $\neg\exists x \in Y : x > a$.

(d) ***(Minimální prvek)*** *Prvek $a \in Y$ je* minimální prvek *množiny Y, jestliže* $\neg\exists x \in Y : x < a$.

Poznámka: Maximální ani minimální prvek není v množině jednoznačně určen, tedy množina může mít těchto prvků více.

(e) ***(Největší prvek)*** *Prvek $a \in Y$ je* největší prvek *množiny Y, jestliže je jeho horní závorou.*

(f) ***(Nejmenší prvek)*** *Prvek $a \in Y$ je* nejmenší prvek *množiny Y, jestliže je jeho dolní závorou.*

(Poznámka: Největší (popř. nejmenší) prvek se od horní (popř. dolní) závory liší svoji příslušností k podmnožině – od horní (dolní) závory podmnožiny Y nepožadujeme, aby byla v podmnožině Y obsažena.)

(g) ***(Supremum)*** *Prvek $a \in X$ je* supremum *množiny Y, jestliže je to nejmenší horní závora.*

(h) ***(Infimum)*** *Prvek $a \in X$ je* infimum *množiny Y, jestliže je to největší dolní závora.*

Pomocí termínů definovaných výše již můžeme definovat pojem svazu. Definici je možné vést buď pomocí termínů užívaných v teorii množin, nebo pomocí algebraických termínů. Obě definice jsou zaměnitelné (důkaz vizte v [8]).

Definice 2.4 (Svaz)

(a) Množinově: Svaz *je uspořádaná množina, v níž má každá dvojice prvků* (x, y) *supremum i infimum.*

(b) Algebraicky: Definujme dvě binární operace – $\sqcup$ (spojení) *a* $\sqcap$ (průsek). *Pak* svaz *je struktura* $(S, \sqcup, \sqcap)$ *taková, že jsou splněny následující axiomy:*

(i) Idempotence: $x \sqcup x = x$; $x \sqcap x = x$.

(ii) Komutativita: $x \sqcup y = y \sqcup x$; $x \sqcap y = y \sqcap x$.

(iii) Asociativita: $x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$; $x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z$.

(iv) Absorpce: $x \sqcup (x \sqcap y) = x$; $x \sqcap (x \sqcup y) = x$.

Na základě definice svazu můžeme definovat také uspořádání $\leq$.

Definice 2.5 (Kanonické uspořádání) *Relace kanonického uspořádání* $\leq$ *je definována takto:*

$$x \leq y \Leftrightarrow x \sqcap y = x \Leftrightarrow x \sqcup y = y.$$

Pokud ještě přidáme podmínku distributivity, získáme *distributivní svaz.*

Definice 2.6 (Distributivní svaz) *Jestliže binární operace svazu jsou k sobě distributivní:*

$$x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z),$$

$$x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z),$$

pak se jedná o distributivní svaz.

Označíme-li nejmenší prvek svazu jako 0 a největší prvek jako 1, můžeme definovat komplementární svaz:

Definice 2.7 (Komplementární svaz) *Svaz, který má ke každému prvku komplement ve smyslu*

$$x \sqcup -x = 1,$$

$$x \sqcap -x = 0,$$

je komplementární svaz.

Stejně jako pro svaz existují dvě různé definice, můžeme dvojím způsobem definovat také *Booleovu algebru*:

Definice 2.8 (Booleova algebra)

(a) Algebraicky: Booleova algebra *je distributivní a komplementární svaz.*

(b) Množinově: Booleova algebra *je množina s nejmenším prvkem* 0*, největším prvkem* 1*, binárními operacemi* ($\sqcup$ *a* $\sqcap$*) a unární operací* ($-$)*, pro kterou platí následující axiomy:*

(i) Idempotence: $x \sqcup x = x$; $x \sqcap x = x$.

(ii) Komutativita: $x \sqcup y = y \sqcup x$; $x \sqcap y = y \sqcap x$.

(iii) Asociativita: $x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z$; $x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z$.

(iv) Absorpce: $x \sqcup (x \sqcap y) = x$, $x \sqcap (x \sqcup y) = x$.

(v) Distributivita: $x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z)$; $x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z)$.

(vi) $x \sqcup 0 = x$; $x \sqcap 0 = 0$,
$x \sqcap 1 = x$; $x \sqcup 1 = 1$.

(vii) Komplementy: $x \sqcup -x = 1$; $x \sqcap -x = 0$.

Booleova algebra, která má pouze jeden prvek (ten tedy zastává funkci nejmenšího i největšího prvku, tedy $1 = 0$), je triviální. Ve zbytku práce budeme předpokládat, že užívané Booleovy algebry triviální nejsou.

2.3 Definice ideálu a filtru ve svazu

Nyní již můžeme zavést také pojem *ideál* – a na rozdíl od okruhů také duální (jak ukážeme) pojem *filtr*.

Definice 2.9 (Ideál) *Nechť S je svaz, pak* ideál *I svazu S je neprázdná podmnožina množiny S, pro kterou platí:*

(a) $\forall x, y \in S : (x \in I \wedge y \in I) \Rightarrow x \sqcup y \in I$.

(b) $\forall x, y \in S : (x \in I \wedge y \leq x) \Rightarrow y \in I$.

- ***(Vlastní ideál)*** *Ideál I svazu S se nazývá* vlastní, *jestliže $I \neq S$.*
- ***(Maximální ideál)*** *Ideál I svazu S se nazývá* maximální, *jestliže neexistuje žádný vlastní ideál J takový, že $I \subset J$.*
- ***(Prvoideál)*** *Ideál I svazu S se nazývá* prvoideál, *jestliže $x \sqcap y \in I$ implikuje, že buď $x \in I$, nebo $y \in I$.*

K výše uvedeným pojmům můžeme definovat také duální pojmy filtru, vlastního filtru, maximálního filtru a ultrafiltru:

Definice 2.10 (Filtr) *Nechť S je svaz, pak* filtr *F svazu S je neprázdná podmnožina množiny S, pro kterou platí:*

(a) $\forall x, y \in S : (x \in I \wedge y \in I) \Rightarrow x \sqcap y \in I$.

(b) $\forall x, y \in S : (x \in I \wedge x \leq y) \Rightarrow y \in I$.

- ***(Vlastní filtr)*** *Filtr F se nazývá* vlastní, *jestliže $F \neq S$.*
- ***(Maximální filtr)*** *Filtr F se nazývá* maximální, *jestliže neexistuje žádný vlastní filtr G takový, že $F \subset G$.*
- ***(Ultrafiltr)*** *Filtr F se nazývá* ultrafiltr, *jestliže pro všechna $x \in S$ platí buď $x \in F$, nebo $-x \in F$.*

- ***(Prvofiltr)*** *Filtr F se nazývá* prvofiltr, *jestliže pro všechna $x, y \in F$ platí $x \sqcup y \in F$ právě tehdy, když $x \in F$, nebo $y \in F$.*

Obecná definice filtru si však na Booleových algebrách vystačí s mnohem slabšími podmínkami, jak ukazuje následující lemma.

Lemma 2.11 *K tomu, aby F byl filtr na Booleově algebře B, jsou postačující tyto podmínky:*

(a) $1 \in F$,

(b) $x \sqcap y \in F \Leftrightarrow x \in F \wedge y \in F$.

Důkaz: Nechť F je filtr na Booleově algebře. Pakliže $x \sqcap y \in F$, pak platí $x \sqcap y \leq x$ a také $x \sqcap y \leq y$. Tedy z definice filtru platí $x \in F$ a $y \in F$.

Pro důkaz druhé implikace předpokládejme, že $x \in F$ a $x \leq y$. Tedy $y \in F$. Protože však $x \leq y$ je ekvivalentní s $x \sqcap y = x$, dostáváme, že $x \sqcap y \in F$ a také $x \sqcap y \leq y$.

QED

Poněkud slabším termínem, než je filtr, je tzv. *centrovaný systém*. Ukážeme si však, že je pro konstrukci některých důkazů nezbytnou součástí, neboť (jak říká lemma 2.13) může být do filtru rozšířen.

Definice 2.12 (Centrovaný systém) *Podmnožina X Booleovy algebry B je* centrovaný systém, *jestliže pro všechna přirozená čísla n a všechny posloupnosti $x_0, x_1, \ldots, x_n \in X$ platí:*

$$x_0 \sqcap x_1 \sqcap \ldots \sqcap x_n \neq 0.$$

Lemma 2.13 *Každá podmnožina X Booleovy algebry B, která je centrovaným systémem, může být rozšířena do vlastního filtru F.*

Důkaz: Definujme množinu F následujícím způsobem:

$$F = \{y | \exists \text{ přirozené číslo } n \text{ a } x_0, \ldots x_n \in X \text{ taková, že } x_0 \sqcap \ldots \sqcap x_n \leq y\}.$$

Je-li F centrovaný systém, žádný z jeho prvků se nerovná nule, tedy F je vlastní. Jestliže $x, y \in F$, pak $x \geq x_0 \sqcap \ldots \sqcap x_n$ a $y \geq y_0 \sqcap \ldots \sqcap y_m$ a prvky $x_0, \ldots, x_n, y_0, \ldots, y_m \in X$.

Protože $x \sqcap y$ je větší než $x_0 \sqcap \ldots \sqcap x_n \sqcap y_0 \sqcap \ldots \sqcap y_m$, je také prvkem množiny F. A jestliže $y \geq x$ pro nějaké $x \in F$, pak $y \geq x \geq x_0 \sqcap \ldots \sqcap x_n$ pro nějaké $x_0, \ldots, x_n \in F$. Tím jsme ověřili, že F je skutečně vlastním filtrem.
QED

V Booleových algebrách (jakožto speciálním případu svazů) se samozřejmě ideály a filtry chovají stejným způsobem jako ve svazech. Nadto však ještě získávají speciální vlastnosti.

Dualitu obou pojmů si můžeme nejlépe ukázat na lemmatu 2.15.

Lemma 2.14 *Nechť $x, y \in B, B$ je Booleova algebra, pak*

$$-(x \sqcup y) = -x \sqcap -y,$$

$$-(x \sqcap y) = -x \sqcup -y,$$

a současně

$$y \leq x \Rightarrow -x \leq -y.$$

Důkaz: Na základě axiomů (konkrétně o distributivitě, asociativitě a jednotce a nule) platí tyto rovnosti a řetězec implikací:

$$(x \sqcup y) \sqcup (-x \sqcap -y) = (x \sqcup y \sqcup -x) \sqcap (x \sqcup y \sqcup -y) = (1 \sqcup y) \sqcap (1 \sqcup x) = 1 \sqcap 1 = 1,$$

$$(x \sqcap y) \sqcap (-x \sqcup -y) = (x \sqcap y \sqcap -x) \sqcup (x \sqcap y \sqcap -y) = (y \sqcap 0) \sqcup (x \sqcap 0) = 0 \sqcup 0 = 0,$$

$$y \leq x \Rightarrow y \sqcup 1 \leq x \sqcup 1 \Rightarrow y \sqcup (x \sqcup -x) \leq x \sqcup (y \sqcup -y) \Rightarrow$$

$$\Rightarrow (y \sqcup x) \sqcup -x \leq (x \sqcup y) \sqcup -y \Rightarrow -x \leq -y.$$

QED

Nyní již můžeme ukázat, že pojem ideálu a filtru je duální:

Lemma 2.15 *Nechť I je ideál Booleovy algebry B. Množina $F = \{-x | x \in I\}$ pak tvoří filtr Booleovy algebry B.*

Důkaz: Ukážeme, že množina F splňuje definici filtru. Nechť $x, y \in I$, pak z definice 2.9 $x \sqcup y \in I$, tedy z definice množiny F: $-x, -y \in F$ a také $-(x \sqcup y) \in F$. Ovšem $-(x \sqcup y)$ je dle lemmatu výše rovno $-x \sqcap -y$, což jsme chtěli ukázat.

V případě, že $x \in I$ a $y \leq x$, pak z definice ideálu $y \in I$, tedy $-y \in F$. Z lemmatu výše však také platí $y \leq x \Rightarrow -x \leq -y$, což jsme požadovali. Obě podmínky jsou tedy splněny.
QED

Obdobným postupem bychom dokázali, že množina $I = \{-x | x \in F\}$ tvoří k filtru F duální ideál I.

Další zajímavé (a především praktické, jak dále uvidíme) vztahy panují mezi jednotlivými druhy filtrů (popř. ideálů). Následující věta ukazuje, že v Booleových algebrách můžeme pojmy maximálního filtru, ultrafiltru a prvofiltru zaměňovat (a stejně tak mezi sebou jejich duální ideály).

Věta 2.16 *Nechť F je vlastním filtrem Booleovy algebry B, pak jsou následující tvrzení mezi sebou ekvivalentní:*

(a) F je maximální filtr.

(b) F je ultrafiltr.

(a) F je prvofiltr.

Důkaz: (a) $\Rightarrow$ (b) Když F je maximální filtr, pak je také ultrafiltr: Nechť $x \notin F$ je dáno. Protože F je maximální, musí existovat nějaké $y \in F$ takové, že $x \sqcap y = 0$. To je však ekvivalentní tvrzení, že $y \leq -x$, tedy $-x \in F$, čímž jsme splnili podmínku ultrafiltru.

(b) $\Rightarrow$ (c) Když F je ultrafiltr, pak je také prvofiltr: Chceme ukázat, že pokud F je ultrafiltr, platí následující ekvivalence:

$$x \sqcup y \in F \Leftrightarrow x \in F \vee y \in F.$$

Implikace zprava doleva plyne z definice filtru. Nechť je pro důkaz opačné implikace dáno $x \sqcup y \in F$. Předpokládejme, že $x \notin F$, tedy (protože F je ultrafiltr) $-x \in F$. Pak však také $-x \sqcap (x \sqcup y) = -x \sqcap y \in F$. Z lemmatu 2.11 pak už přímo plyne, že $y \in F$.

(c) $\Rightarrow$ (a) Když je F prvofiltr, pak je také maximální filtr: Nechť $x \notin F$ je dáno. Kdyby F byl maximální filtr, pak by $F \cup \{x\}$ nebyl vlastní – existovalo by totiž takové $x' \in F$, že $x' \sqcap x = 0$, což plyne z faktu, že každý centrovaný systém může být rozšířen do vlastního filtru. Tedy nám stačí najít nějaké $y \in F$ takové, že $x \sqcap y = 0$. Protože $x \sqcup -x \in F$ a F je navíc prvofiltr, platí, že buď $x \in F$, nebo $-x \in F$. Předpokládali jsme však, že $x \notin F$, proto $-x \in F$, našli jsme tedy $y = -x$, protože $x \sqcap -x = 0$.
QED

Obdobné tvrzení platí také pro ideály. Duálním pojmem ultrafiltru je prvoideál a vlastnost definující prvofiltr je možné použít také pro určité ideály.

Na závěr této části se vraťme k Booleovým okruhům a ukažme, že vztah mezi ideály v Booleových algebrách a Booleových okruzích je velmi těsný.

Zaveďme vztah pro svazové a okruhové operace:

$$x + y = (x \sqcap -y) \sqcup (-x \sqcap y),$$

$$x \cdot y = x \sqcap y.$$

Věta 2.17 *Nechť I je podmnožinou Booleovy algebry B. Pak platí, že I je ideál v Booleově algebře právě tehdy, když I je ideálem v odpovídajícím Booleově okruhu.*

Důkaz: Nechť I je ideál v Booleově algebře a nechť x, y jsou libovolné prvky z Booleovy algebry. Pak nám stačí ukázat implikace:

$$x \in I \wedge \ y \in I \Rightarrow x + y \in I,$$

$$x \in I \Rightarrow x \cdot y \in I.$$

Nechť tedy $x, y \in B$, předpokládejme nadále $x \in I$ a $y \in I$. Současně platí $x \sqcap -y \leq x$ a $-x \sqcap y \leq y$. Přijměme jako fakt platnost nerovnosti $(x \sqcap -y) \sqcup (-x \sqcap y) \leq x \sqcup y$. Ze zavedení operací výše dostáváme $x + y \leq x \sqcup y$. A protože $x \sqcup y \in I$, tak také $x + y \in I$.

Pro druhou implikaci předpokládejme $x \in I$ a $r \in B$. Víme, že $x \sqcap y \leq x$ a ze zavedení operací rovnou máme $x \cdot y \in I$.
QED

2.4 Stoneova věta o reprezentaci

Pravděpodobně nejznámějším využitím filtrů v Booleově algebře je důkaz Stoneovy věty o reprezentaci. Důkaz však vyžaduje využití axiomu výběru, respektive jeho ekvivalentního tvrzení – Principu maximality. (Důkaz ekvivalence je možno najít např. v [1].) Ten nám říká, že v každé množině s částečným uspořádáním takové, že každý její řetězec je shora omezený, existuje nad každým prvkem minimálně jeden maximální prvek.

Abychom tedy mohli aplikovat Princip maximality, potřebujeme pracovat s množinou, jejíž každá lineárně uspořádaná podmnožina má horní mez.

Lemma 2.18 *Je-li $\mathcal{F}'$ lineárně uspořádaná podmnožina množiny všech vlastních filtrů $\mathcal{F}_B$ na Booleově algebře B, pak $\mathcal{F}'$ má horní mez.*

Důkaz: Ukážeme, že $F = \bigcup \mathcal{F}'$ je vlastní filtr. Jestliže $x, y \in F$, pak $x \in F_x$ a $y \in F_y$ pro nějaké filtry z $\mathcal{F}$'. Bez újmy na obecnosti nechť $F_x \subseteq F_y$, tedy $x, y \in F_y$ a $x \sqcap y \in F_y$, a proto $x \sqcap y \in F$. Jestliže $x \in F$ a $y \geq x$, pak $y \in F_x$ pro každé F_x z $\mathcal{F}'$ obsahující x. 0 nemůže být prvkem žádného $F' \in \mathcal{F}'$, protože $\mathcal{F}'$ je množina vlastních filtrů, tedy i F je vlastní. F je tedy naší hledanou horní mezí, a to dokonce supremem. Protože F je sjednocením přes všechny vlastní filtry Booleovy algebry, jsou všechny filtry obsažené v $\mathcal{F}'$ menší než F.

A protože jsme ukázali, že se jedná o vlastní filtr na Booleově algebře B, jedná se o nejmenší horní mez.
QED

Následující věta je stěžejním poznatkem pro důkaz Stoneovy věty. V anglofonním světě se označuje jako *Boolean prime ideal theorem* – v překladu tedy přibližně „věta o booleovském prvoideálu“. Její název odráží historické pojetí a fakt, že prvoideál je duálním pojmem k ultrafiltru.

Věta 2.19 (Boolean prime ideal theorem) *Každá podmnožina $X \subseteq B$, která je centrovaný systém, může být rozšířena do ultrafiltru.*

Důkaz: V důkazu využijeme Principu maximality. Nechť $\mathcal{F}_B$ je množina vlastních filtrů na B, pak podle předchozího lemmatu má $\mathcal{F}' \subseteq \mathcal{F}_B$ horní mez, tedy z Principu maximality má $\mathcal{F}_B$ maximální prvek, tedy existuje nějaký maximální filtr U (s ohledem na relaci $\subseteq$). Podle lemmatu 2.13 rozšíříme centrovaný systém X na vlastní filtr X'. Platí zřejmě $X' \in U$. A protože platí, že „být maximálním filtrem“ je ekvivalentní s „být ultrafiltrem“ (z věty 2.16), je U ultrafiltr.
QED

A konečně si definujme poslední potřebné termíny – *atom* a *hlavní ideál*.

Definice 2.20 (Atom) *Prvek x z Booleovy algebry je* atom, *jestliže jediné y, pro které platí $y < x$, je $y = 0$.*

Definice 2.21 (Hlavní filtr) *Filtr F je* hlavní filtr, *jestliže pro všechny $0 < x \in B$ platí $F = \{y \in B | x \leq y\}$.*

Lemma 2.22 *Nechť B je Booleova algebra, pak:*

(a) Hlavní filtr Booleovy algebry je vlastní filtr.

(b) Nechť $0 < x$ je dáno, pak hlavní filtr $F = \{y \in B | x \leq y\}$ je ultrafiltr právě tehdy, když x je atom v B.

Důkaz: (a) Pro každé $x > 0$ platí, že $\{x\}$ je centrovaný systém, tedy F je vlastní filtr.

(b) Nechť F je ultrafiltr, zvolme nějaké y takové, že $0 \leq y < x$. Chceme ukázat, že $y = 0$. Zřejmě platí $x = y \sqcup (x \sqcap -y)$, a protože $x \in F$, musí být y nebo $x \sqcap -y$ prvkem ultrafiltru F. Avšak $x \not\leq y$, tedy $y \notin F$, a proto $x \sqcap -y \in F$. Z toho však také plyne $x \leq x \sqcap -y$ a očividně také $x \leq -y$, což implikuje $x \sqcap y = 0$. Předpokládali jsme však, že $y < x$ a $x \sqcap y = y$, musí tedy platit $y = 0$.

Pro opačnou implikaci předpokládejme, že x je atom, pak pro každé y platí $x \leq y$ nebo $x \leq -y$, tedy F obsahuje buď y, nebo $-y$, je tedy ultrafiltrem.
QED

Věta 2.23 (Stoneova věta o reprezentaci) *Každá Booleova algebra B je isomorfní s nějakou algebrou množin.*

Důkaz: Označme si $Ult(B)$ množinu všech ultrafiltrů na B. Definujme zobrazení $S : B \to \mathcal{P}(Ult(B))$ takto: $S(x) = \{U \in Ult(B) | x \in U\}$.

Tvrdíme, že S je isomorfismus mezi B a algebrou množin $S[B] \subseteq \mathcal{P}(Ult(B))$. Nejprve ověříme, že S je homomorfismu:

- $S(1) = Ult(B)$,
- $S(0) = \emptyset$,
- $S(x \sqcap y) = S(x) \cap S(y)$, což je zřejmé z lemmatu 2.11,
- $S(-x) = -S(x)$, což plyne z definice ultrafiltru,
- $S(x \sqcup y) = S(x) \cup S(y)$, což plyne z ekvivalence ultrafiltru a prvofiltru.

Zbývá ukázat, že S je prostá. Nechť $x \neq y$, $x, y \in B$, což implikuje buď $x \not\leq y$, nebo $y \not\leq x$, bez újmy na obecnosti zvolme první z nich. Pak platí $x \sqcap -y \neq 0$, tedy $\{x, -y\}$ je centrovaný systém. Z *Boolean prime ideal theorem* dostáváme ultrafiltr U, který obsahuje x a $-y$, z čehož plyne, že $U \in S(x)$ a $U \notin S(y)$. Tedy S$(x) \neq S(y)$.

S tedy je prostý homomorfismus, tedy B je isomorfní s $S[B]$.
QED

Marshall Harvey Stone dokázal tuto větu v roce 1936. Pro tehdejší matematický svět znamenala prostředek k hlubšímu pochopení Booleových algeber. Ukazuje totiž, že každá Booleova algebra je isomorfní s nějakou algebrou množin, což už je pro větší počet matematiků jistě mnohem uchopitelnější termín.

Kapitola 3

Ideály a filtry v logice

Důkazy, které využívají vlastností filtrů, najdeme také v logice. Zde je pravděpodobně nejvýznamnější důkaz úplnosti výrokové logiky, avšak jinou cestou, než je standardně předkládáno.

Než přistoupíme k samotnému důkazu, definujme si nejdříve tzv. Lindenbaum-Tarského algebry, jichž se v důkazu využívá.

3.1 Lindenbaum-Tarského algebry

Uvažujme prvořádovou teorii T nad nějakým jazykem L a definujme pro formule φ a ψ v jazyce L následující relaci:

$$\varphi \equiv \psi \Leftrightarrow T \vdash \varphi \leftrightarrow \psi.$$

Protože relace $\equiv$ je ekvivalence, můžeme $[\varphi]$ označit jako ekvivalentní třídu formule φ. Pak $B(T) = \{[\varphi] | \varphi \text{ je formule v jazyce } L\}$ je množina všech ekvivalentních tříd.

Definujme dále operace následujícím způsobem:

(a) $[\varphi] \sqcap [\psi] = [\varphi \wedge \psi]$,

(b) $[\varphi] \sqcup [\psi] = [\varphi \vee \psi]$,

(c) $-[\varphi] = [\neg\varphi]$,

(d) $1 = [\varphi \to \varphi]$,

(e) $0 = [\varphi \wedge \neg\varphi]$.

Tvrzení 3.1 $\boldsymbol{B} = \langle B(T), \sqcap, \sqcup, -, 0, 1\rangle$ *je Booleova algebra s korektně definovanými operacemi.*

Důkaz: Nejprve ukážeme, že definované operace jsou kongruentní. Nechť platí $\alpha \equiv \varphi$ a $\beta \equiv \psi$, pak:

1. $[\varphi \wedge \psi] = [\alpha \wedge \beta]$: Plyne z faktu, že $((\alpha \leftrightarrow \varphi) \wedge (\beta \leftrightarrow \psi)) \to (\alpha \wedge \beta \leftrightarrow \varphi \wedge \psi)$ je výroková tautologie.

2. $[\varphi \vee \psi] = [\alpha \vee \beta]$: Plyne z faktu, že $((\alpha \leftrightarrow \varphi) \wedge (\beta \leftrightarrow \psi)) \to (\alpha \vee \beta \leftrightarrow \varphi \vee \psi)$ je výroková tautologie.

3. $[\neg\varphi] = [\neg\alpha]$: Plyne z faktu, že $(\alpha \leftrightarrow \varphi) \to (\neg\alpha \leftrightarrow \neg\varphi)$ je výroková tautologie.

4. $1 = [\alpha]$: Plyne z faktu, že $(\alpha \leftrightarrow \varphi) \to (\alpha \leftrightarrow (\varphi \to \varphi))$ je výroková tautologie.

5. $0 = [\alpha]$: Plyne z faktu, že $(\alpha \leftrightarrow \varphi) \to (\alpha \leftrightarrow (\varphi \wedge \neg\varphi))$ je výroková tautologie.

Abychom, dokázali, že $B(T)$ je Booleova algebra, je potřeba ukázat, že splňuje všechny její axiomy. To je však zřejmé již z toho, že výrokové spojky nad množinou $\{0, 1\}$ tvoří samy Booleovu algebru. Axiom komutativity tedy platí například z následujícího: $[\alpha] \sqcup [\beta] = [\beta] \sqcup [\alpha]$ odpovídá $\alpha \vee \beta \leftrightarrow \beta \vee \alpha$, což je výroková tautologie.
QED

Speciální podalgebrou $B(T)$ je tzv. Lindenbaum-Tarského algebra, označme ji $LT(T)$ a definujme jako:

$$LT(T) = \{[\sigma] | \sigma \text{ je sentence v jazyce L}\}$$

Můžeme lehce ověřit, že 1 a 0 můžeme reprezentovat sentencemi a že $LT(T)$ splňuje podmínky tvrzení 3.1, a tedy že se jedná o Booleovu algebru.

Abychom mohli ukázat vztah mezi filtry a Lindenbaum-Tarského algebrami, a tedy se nakonec úspěšně propracovat k důkazu věty o úplnosti, budeme potřebovat znát ještě další pojmy:

Definice 3.2 (Zúplnění teorie) *Nechť T je prvořádová teorie nad jazykem L. Říkáme, že T^* je* zúplnění *teorie T, když T^* je teorie nad jazykem L, dále $T \subseteq T^*$ a T^* je maximálně bezesporná, což je právě tehdy, když je bezesporná a pro každou sentenci $\sigma \notin T^*$ existuje formule $\varphi \in T^*$ taková, že $T \cup \{\varphi, \sigma\} \vdash \bot$.*

Tvrzení 3.3 *Nechť T je teorie a T^* její zúplnění, pak pro každou sentenci σ platí:*

$$T^* \vdash \sigma \Rightarrow \sigma \in T^*.$$

Důkaz: Jestliže σ je sentence, platí

$$T \cup \{\sigma\} \vdash \bot \Leftrightarrow T \vdash \neg\sigma. \tag{2}$$

Pro spor předpokládejme, že $T^* \vdash \sigma$ a současně $\sigma \notin T^*$. Pak však existuje nějaké $\varphi \in T^*$ takové, že $T \cup \{\varphi, \sigma\} \vdash \bot$, což je ekvivalentní tvrzení $T \cup \{\varphi\} \vdash \neg\sigma$. Z toho však plyne $T^* \vdash \neg\sigma \wedge \sigma$, takže T^* není bezesporná, což je ve sporu s předpokladem, že T^* je zúplnění.

Lemma 3.4 *Nechť T je teorie a $LT(T)$ Lindenbaum-Tarského algebra. Pak platí:*

(a) Když T^* je zúplnění teorie T, pak $F = \{[\sigma] | \sigma \in T^*\}$ je ultrafiltr nad LT(T).

(b) Mezi množinou všech zúplnění T^* a množinou všech ultrafiltrů F algebry $LT(T)$ existuje bijekce.

Důkaz: (a) Z tvrzení ve (2) víme, že zúplnění T^* obsahuje všechny tautologie, je uzavřené na pravidlo modus ponens a na konjunkci. Současně také neobsahuje

spor, jinak by nebylo bezesporné. Tyto podmínky jsou už dostačující pro to, aby F byl vlastní filtr: přítomnost všech tautologií implikuje, že $1 \in F$, nepřítomnost sporu naopak $0 \notin F$. Uzavřenost na modus ponens odpovídá $[\sigma] \in F$ a $[\sigma] \leq [\sigma']$, pak také $[\sigma'] \in F$. A konečně uzavřenost na konjunkci nám říká, když $[\sigma] \in F$ a $[\sigma'] \in F$, pak také $[\sigma] \wedge [\sigma'] \in F$.

Filtr F je však také maximální. To plyne s věty 2.16 (z argumentace v bodě (c)) a z podmínky maximality, která tvrdí, že $T \cup \{\sigma, \varphi\} \vdash \bot$, což je ekvivalentní $T \vdash \sigma \wedge \varphi \leftrightarrow \bot$, a to zase je ekvivalentní s tvrzením $[\sigma] \wedge [\varphi] = 0$, které využívá faktu ve zmíněné větě. Z věty 2.16 však také přímo dostáváme, že F je ultrafiltr (protože je maximální).

(b) Nechť T je bezesporná teorie. Sama o sobě ještě nemusí být uzavřená na modus ponens ani na konjunkci. Platí však, že $F = \{[\sigma] | \sigma \in T\}$ je centrovaný systém, tedy může být z lemmatu 2.13 rozšířen do filtru F', který v podstatě odpovídá rozšíření T^*. A z věty 2.19 může být rozšířen do ultrafiltru $U = \{[\sigma] | \sigma \in T^*\}$. Pokud navíc jsou T_1^* a T_2^* dvě různá zúplnění taková, že pro nějaké σ platí $\sigma \in T_1^*$ a zároveň $\sigma \notin T_2^*$, dostáváme z definice zúplnění, že $\neg\sigma \in T_1^*$, tedy ultrafiltry pro zúplnění T_1^* a T_2^* jsou rozlišitelné sentencí σ. Funkce je tedy prostá a pro každý centrovaný systém F, respektive pro každý ultrafiltr, je možné nalézt odpovídající zúplnění, funkce je tedy surjektivní.

Naopak chceme: F je ultrafiltr algebry $LT(T)$, pak $T^* = \{\sigma | [\sigma] \in F\}$ je zúplnění teorie T. Z výrokové logiky víme, že když platí $T \vdash \sigma$, pak platí také $T \vdash \sigma \leftrightarrow \top$, a tedy $[\sigma] = 1$, a proto také $1 \in F$. Proto T^* obsahuje všechny formule z T. Dále ukážeme, že T^* je bezesporná. Pro spor předpokládejme, že $T^* \vdash \bot$, tedy existuje nějaká posloupnost formulí $\sigma_0, \sigma_1, \ldots, \sigma_n \in T^*$ taková, že $T \cup \{\sigma_0, \sigma_1, \ldots, \sigma_n\} \vdash \bot$. A tedy $[\sigma = \sigma_0 \wedge \sigma_1 \wedge \ldots \wedge \sigma_n] \in F$ (protože F je uzavřen na konjunkci). Platí tak tvrzení $T \vdash \neg\sigma \leftrightarrow \top$, což je ekvivalentní $-[\sigma] = 1 \in F$. Z toho však vyplývá, že také $0 = [\sigma] \wedge -[\sigma] \in F$, což je ovšem spor s předpokladem, že F je vlastní filtr.

Nakonec stačí ukázat, že T^* je maximální bezesporná: Jestliže $\sigma \notin T^*$, pak $[\sigma] \notin F$ a z definice ultrafiltru $-[\sigma] = [\neg\sigma] \in F$, navíc platí, že $\neg\sigma \in T^*$. To však

znamená také $T \cup \{\neg\sigma, \sigma\} \vdash \bot$, čímž jsme splnili definici maximální bezesporné množiny.

Navíc máme-li dva ultrafiltry $F \neq F'$, musí nutně existovat nějaká σ taková, že $[\sigma] \in F$ a současně $-[\sigma] \in F'$, tedy právě σ dokáže tyto dva ultrafiltry rozlišit (a současně také zúplnění, která se k daným ultrafiltrům vážou).
QED

3.2 Úplnost výrokové logiky

Věta o úplnosti, ve standardním znění *„je-li T množina formulí, pak T je splnitelná právě tehdy, když T je bezesporná“*, případně zkráceně „$T \vdash \varphi \Leftrightarrow T \models \varphi$“, je jednou ze základních vět výrokového kalkulu. Standardní důkaz (k nahlédnutí např. ve [5] na str. 34.) si zde předvádět nebudeme. Místo toho dokážeme větu o úplnosti pro výrokovou logiku právě pomocí filtrů.

Připomeňme si, že výrokový kalkul můžeme reprezentovat například axiomy Hilbertova kalkulu:

H1 $\varphi \to (\psi \to \varphi)$,

H2 $[\varphi \to (\psi \to \theta)] \to [(\varphi \to \psi) \to (\varphi \to \theta)]$,

H3 $(\neg\psi \to \neg\varphi) \to (\varphi \to \psi)$.

Víme, že implikace může být definovaná pomocí negace a disjunkce, tedy $\varphi \to \psi$ je ekvivalentní s $\neg\varphi \vee \psi$. Všechny formule tedy mohou být přepsány do podoby jen s těmito dvěma spojkami, čímž dostaneme jazyk Booleovy algebry. Dokažme teď tedy větu o úplnosti.

Lemma 3.5 *Nechť F je ultrafiltr na Booleově algebře B. Pak funkce $f : B \to \{0, 1\}$ definovaná předpisem $f(x) = 1$, když $x \in F$, a $f(x) = 0$, když $x \notin F$, je homomorfismus z Booleovy algebry B na Booleovu algebru $\{0, 1\}$.*

Důkaz: F je vlastní filtr, platí tedy $f(0) = 0$, $f(1) = 1$ a podle lemmatu 2.11 také $f(x \sqcap y) = f(x) \sqcap f(y)$. Z vlastností ultrafiltru dostáváme také

$f(-x) = -f(x)$ a z vlastnosti prvofiltru (který je podle věty 2.16 ekvivalentní ultrafiltru) také $f(x \sqcup y) = f(x) \sqcup f(y)$. Tedy jsme splnili podmínky a funkce f je homomorfismus.

QED

Věta 3.6 (Úplnost výrokové logiky) *Nechť T je množina výrokových formulí. Pak $T \vdash \varphi \Leftrightarrow T \models \varphi$.*

Důkaz: Důkaz implikace zleva doprava se nijak neliší od standardního důkazu. Podívejme se proto na opačný směr. Zřejmě platí vztah $T \cup \varphi \vdash \psi \wedge \neg\psi \Leftrightarrow$ $\Leftrightarrow T \vdash \neg\varphi$. Ukážeme, že z $T \nvdash \varphi$ plyne $T \not\models \varphi$. Zřejmě je $T \nvdash \varphi$ ekvivalentní s tím, že $T \vdash \neg\varphi$ je bezesporná. Ukážeme, že jestliže $T \vdash \neg\varphi$ je bezesporná, pak má model.

Protože všechny formule ve výrokové logice jsou sentence, můžeme Booleovu algebru nad výrokovou logikou ztotožnit s Lindenbaum-Tarského algebrou $LT(T) = \{\varphi] | \varphi$ je výroková formule$\}$. Jak jsme již dříve ukázali (v lemmatu 3.4 v bodě (a)), existuje k této algebře ultrafiltr F. Z lemmatu výše víme, že existuje homomorfismus $f : LT(T) \to \{0, 1\}$ takový, že se všechny prvky ultrafiltru F zobrazí na prvek 1. Model teorie T pak zkonstruujeme indukcí dle délky formule. Výrokové proměnné p přiřadíme hodnotu 1 právě tehdy, když $[p] \in F$. Indukční krok pro negaci a disjunkci je pak už zřejmý: $\neg\varphi$ přiřadíme hodnotu 1 právě tehdy, když φ přiřadíme 0. A formuli $\varphi \vee \psi$ přiřadíme hodnotu 1, když φ přiřadíme 1 nebo ψ přiřadíme 1. Našli jsme tedy způsob, jak pomocí ultrafiltrů zkonstruovat model, čímž jsme ukázali, že $T \cup \{\neg\varphi\}$ je bezesporná, tedy $T \nvdash \varphi$ implikuje $T \not\models \varphi$.
QED

Obdobným způsobem (za pomoci ultrafiltru) by bylo možné zkonstruovat také důkaz věty o úplnosti klasické predikátové logiky. Je však mnohem složitější – je potřeba pracovat s nekonečnými operacemi a zkonstruovat tak mimo jiné speciální filtr, který bude nekonečné operace zohledňovat. Důkaz je k nahlédnutí např. v [10].

Kapitola 4

Od pojmu ideálního čísla k ideálu

Ačkoli se dnes pojmu *ideál* užívá v matematických důkazech zcela běžně, k jeho zavedení vedla poměrně dlouhá cesta. Její začátek se pojí s Velkou Fermatovou větou. Právě při jednom z pokusů o její důkaz bylo poprvé užito tzv. *ideálního čísla*, které dalo později vzniknout pojmu *ideál*.

4.1 Stručný úvod k Velké Fermatově větě

Velká Fermatova věta se řadí k nejznámějším matematickým větám. A to zejména pro své jednoduché zadání a současně dlouhou dobu, po kterou se nikomu nedařilo ji dokázat.

Pierre Fermat žil v 17. století a pracoval jako parlamentární rada. Jeho zájem o matematiku byl ryze soukromý, dalo by se říci i amatérský. Nikdy matematiku nestudoval a věnoval se jí jen ve volném čase. Díky svému talentu si však nijak nezadal s největšími matematiky tehdejší doby. Další informace o životě Pierra Fermata jsou k dispozici v [3].

Velká Fermatova věta zní:

$$\neg\exists x, y, z \in N : x^n + y^n = z^n,$$

kde $n > 2$ a $x, y, z \neq 0$.

Fermat napsal znění této věty na okraj knihy *Aritmetika* od Diofanta a připsal k ní poznámku, že okraj stránky je příliš malý, než aby se na něj ve-

šel i důkaz. To, zda Fermat skutečně větu dokázal, není dodnes známo. Tato poznámka však byla provokací pro mnoho dalších generací matematiků. Nespočet teoretiků čísel se snažilo najít buď původní Fermatův důkaz (pokud vůbec existuje), nebo přijít s vlastním řešením.

Velká Fermatova věta však odolávala všem pokusům více než tři sta let. Teprve v roce 1994 ji za pomoci poznatků z moderní matematiky dokázal britský matematik Andrew Wiles. Důkaz se opíral o tzv. *Tanijamovu-Šimurovu domněnku*, která propojuje dvě vzdálená odvětví matematiky – eliptické křivky a modulární formy, tedy záležitost ve Fermatově době ještě neznámou. Bližší informace o úloze Tanijamovy-Šimurovy domněnky v důkazu Velké Fermatovy věty naleznete v [3]. Velká Fermatova věta tedy i dnes v sobě ukrývá skrytou výzvu – nalezne někdo původní Fermatův důkaz?

Ačkoliv sama Fermatova věta nepřináší matematice žádné zásadní poznání, marné snahy o její dokázání (a koneckonců i Wilesův důkaz) obohatily matematiku mnoha cennými poznatky. A mezi takové patří také ideální čísla.

4.2 Chyby v důkazech Cauchyho a Lamého

Mezi stovkami matematiků, kteří se snažili Velkou Fermatovu větu dokázat, patřili také Gabriel Lamé a Augustin Louis Cauchy. Oba žili v 19. století a nebyli to jen současníci, ale také velcí rivalové. Oba totiž přistupovali v téže době k řešení důkazu Velké Fermatovy věty obdobným způsobem. Zdálo se, že mají důkaz už na dosah. Avšak prvenství nalezení důkazu mohlo připadnout jen jednomu. Proto oba nezávisle na sobě zveřejnili části svých důkazů. Více informací o jejich „matematickém souboji“ se můžete dočíst v [3].

Zatímco většina matematické obce se s nadějí upínala na dokončení těchto důkazů, německý matematik Ernst Kummer odhalil ve zveřejněných fragmentech důkazů zásadní chyby.

Cauchyho i Lamého důkaz byl totiž založen na jednoznačné faktorizaci tzv. *Gaussových celých čísel*. Kummer však ukázal, že faktorizace nemusí být vždy (tj. pro všechny prvky) jednoznačná.

Definice 4.1 (Gaussova celá čísla) *Gaussova celá čísla jsou komplexní čísla tvaru $a + bi$, kde a, b jsou celá čísla.*

Pro další práci se seznamme blíže ještě s pojmem *algebraického prvočísla.* Definujme si nejdříve *algebraické číslo*:

Definice 4.2 (Algebraické číslo) *Komplexní číslo, které je kořenem nějakého polynomu s racionálními koeficienty, je algebraické číslo.*

Dalším důležitým pojmem je *algebraické celé číslo.* Podmnožinou těchto čísel jsou již definovaná Gaussova celá čísla.

Definice 4.3 (Algebraické celé číslo) *Algebraické číslo, které je kořenem polynomu $x^n + a_1 x^{n-1} + \cdots + a_n = 0$, kde $a_1, \ldots, a_n$ jsou celá čísla, je* algebraické celé číslo.

Seznamme se nyní blíže s tělesem $\mathbb{Q}(\sqrt{d})$.

Definice 4.4 (Těleso $\mathbb{Q}(\sqrt{d})$) *Množina všech čísel tvaru $a+b\sqrt{d}$, kde a, b jsou racionální čísla a d je celé číslo, tvoří nosič tělesa $\mathbb{Q}(\sqrt{d}) = \langle Q(\sqrt{d}), +, \cdot, 1, 0\rangle$.*

Značením „$\mathbb{Q}(\sqrt{d})$“ naznačujeme, že jsme k tělesu $\mathbb{Q}$ přidali nový prvek, a to $\sqrt{d}$. Těleso $\mathbb{Q}(\sqrt{d})$ je tedy nejmenší těleso obsahující $\mathbb{Q}$ a současně nové číslo k takové, že $k^2 = d$.

Celá čísla tohoto tělesa jsou tvaru $a + b\sqrt{d}$, kde a, b jsou celá čísla. Takto utvořená tělesa označme jako *kvadratická.* Celá čísla tohoto tělesa tvoří obor integrity $\mathbb{Z}(\sqrt{d})$.

Obdobně jako v oboru integrity celých čísel, můžeme definovat „speciální dělitelnost“ na celých číslech kvadratického tělesa.

Definice 4.5 (Dělitelnost celých čísel kvadratického tělesa) *Nechť a, b jsou celá algebraická čísla kvadratického tělesa T. Pak číslo a je dělitelné číslem b, pakliže existuje celé algebraické číslo c takové, že platí: $a = b \cdot c$. Říkáme, že „b dělí a“.*

A na základě této dělitelnosti můžeme definovat také *jednotku* tělesa:

Definice 4.6 (Jednotka kvadratického tělesa) *Každé celé algebraické číslo x kvadratického tělesa T, které dělí číslo* 1*, nazýváme* jednotkou *kvadratického tělesa T.*

Například jednotkové prvky tělesa $\mathbb{Q}(\sqrt{-5})$ jsou ± 1.

A konečně nyní už můžeme definovat algebraické prvočíslo, jehož budeme v další práci hojně využívat.

Definice 4.7 (Algebraické prvočíslo) *Algebraické celé číslo, které je dělitelné pouze sebou samým a jednotkami tělesa, je* algebraické prvočíslo.

Věta o jednoznačné faktorizaci pro přirozená čísla byla dokázána již ve 4. století př. n. l. Eukleidem. I Gaussova čísla je možné faktorizovat – namísto klasických prvočísel se využívají algebraická prvočísla. Důkaz tohoto tvrzení je možné nahlédnout v [2]. Rozklad Gaussova celého čísla α se rovná součinu algebraických prvočísel $\pi_1, \pi_2, \ldots, \pi_n$: $\alpha = \pi_1 \cdot \pi_2 \cdot \ldots \cdot \pi_n$.

Faktorizace však nemusí být jednoznačná v každém tělese. A právě této chyby se dopustili Lamé a Cauchy. Když oba představili svoji verzi důkazu, vznesl proti nim Kummer námitku. Jednoznačnost rozkladu neplatí například pro číslo $k = 21$ v tělese $\mathbb{Q}(\sqrt{-5})$. Platí totiž

$$21 = 3 \cdot 7 = (1 + 2\sqrt{-5}) \cdot (1 - 2\sqrt{-5}).$$

Sám Kummer proto navrhl používat pro jednoznačnou faktorizaci tzv. *ideální komplexní čísla.*

4.3 Zavedení ideálních čísel

Kummer samozřejmě nezůstal jen u nalezení chyby v důkazech. Problematice jednoznačné faktorizace algebraických celých čísel se věnoval i nadále a podařilo se mu ji vyřešit. Zavedl tzv. *ideální čísla*, pomocí kterých je možné rozklad

realizovat. Sám dokonce dokázal s využitím nově zavedených ideálních čísel Fermatovu větu pro určité exponenty (konkrétně pro tzv. *regulární prvočísla*).

Pro další důkazy budeme užívat tzv. *normu*, která má své pevné místo v mnoha odvětvích matematiky.

Pro naše potřeby však postačí, když si definujeme normu pro čísla tvaru $a + b\sqrt{-5}$.

Definice 4.8 (Norma v tělese $\mathbb{Q}(\sqrt{-5})$) *Norma čísla $a + b\sqrt{-5}$ je číslo $a^2 + 5b^2$.*

Ne všechna celá algebraická čísla v tělese $\mathbb{Q}(\sqrt{-5})$ však mají jednoznačný rozklad. Příkladem takového čísla je již zmíněné číslo 21. Existují dokonce tři dvojice celých algebraických čísel z tohoto tělesa, jejichž součin dává požadované číslo, a to $3 \cdot 7 = (1+2\sqrt{-5}) \cdot (1-2\sqrt{-5}) = (4+\sqrt{-5}) \cdot (4-\sqrt{-5})$. Všechna tato čísla jsou nejen navzájem různá, ale jsou také algebraickými prvočísly tělesa. To můžeme dokázat sporem pro každé číslo zvlášť.

Nechť 3 není algebraické prvočíslo, pak existují čísla a, b, c, d taková, že $3 = (a + b\sqrt{-5})(c - d\sqrt{-5})$. Pokud bychom počítali s normou, získáme

$$9 = (a^2 + 5b^2)(c^2 + 5d^2).$$

Protože je norma vždy celé číslo, musí být $a^2 + 5b^2$ rovno některému z dělitelů čísla 9, tedy $1, 3, 9$. Žádná z rovnic

$$a^2 + 5b^2 = 1,$$

$$a^2 + 5b^2 = 3,$$

$$a^2 + 5b^2 = 9,$$

však nedává celočíselné řešení anebo nového dělitele. Číslo tři je tedy algebraické prvočíslo. Obdobným způsobem bychom dokázali algebraickou prvočíselnost i u dalších čísel. Ukázali jsme tedy, že rozklad v tělese $\mathbb{Q}(\sqrt{-5})$ skutečně není jednoznačný.

Jako důsledek dokázaného tvrzení dostáváme, že v tomto tělese neplatí ani další vlastnosti typické pro aritmetiku celých čísel. Platí sice, že $3|21$, tedy

$3|(4+\sqrt{-5})\cdot(4-\sqrt{-5})$, ale rozhodně už neplatí $3|(4+\sqrt{-5})$ ani $3|(4-\sqrt{-5})$. Algebraická prvočísla tedy nejsou v jistém smyslu základními prvky tohoto tělesa. Kummerovým cílem bylo tyto prvky nalézt. Hledal tedy společné dělitele algebraických prvočísel. Z definice (algebraického) prvočísla však v tělese žádný jeho netriviální dělitel neexistuje. Najít jej tedy budeme muset mimo těleso.

Vraťme se k rozkladu čísla 21. Hledáme taková čísla x_1, x_2, x_3, x_4, že

$$x_1 \cdot x_2 = 3,$$

$$x_3 \cdot x_4 = 7,$$

$$x_1 \cdot x_3 = (1 + 2\sqrt{-5}),$$

$$x_2 \cdot x_4 = (1 - 2\sqrt{-5}).$$

Rozklad celého čísla 21 v tělese $\mathbb{Q}(\sqrt{-5})$ pak bude jednoznačný, totiž $21 = x_1 \cdot x_2 \cdot x_3 \cdot x_4$. Tato čísla – která mají vlastnosti klasických prvočísel, ale nejsou prvky tělesa – nazval Kummer jako *ideální*.

4.4 Dedekind a zavedení teorie ideálů

Pro těleso $\mathbb{Q}(\sqrt{-5})$ nabývají čísla x_1, x_2, x_3, x_4 tvaru $\sqrt{a + b\sqrt{-5}}$. Tato čísla však už neleží v našem tělese, což může být v některých případech nevýhodou. Další snaha tedy vedla k tomu, abychom ideální čísla byli schopni vyjádřit pouze pomocí prvků z dané struktury. Pro reprezentaci ideálního čísla byl zvolen následující postup: ideální číslo x bude charakterizováno jako množina všech čísel $a_1, a_2, ...a_n$ takových, že x je dělitel těchto čísel.

Jestliže tato množina již obsahuje čísla a, b, pak obsahuje také číslo $a \cdot c + b \cdot d$, kde $c, d \in \mathbb{Q}(\sqrt{-5})$. Množiny s těmito vlastnostmi nazval později (v roce 1871) Richard Dedekind, německý matematik, jako *ideály*, a to ve svém díle *Über die Komposition der binären quadratischen Formen* [11].

Pracujme v této sekci nadále v oboru integrity celých čísel $\mathbb{Z}$. Na tomto oboru ukážeme, jak je možné přesně definovat ideály a jak vypadá základní práce s nimi.

Definice 4.9 (Ideál) *Nechť $a_1, a_2, \ldots, a_k$ jsou celá čísla (tedy prvky oboru integrity $\mathbb{Z}$), kde alespoň jedno z nich je různé od nuly. Pak množinu všech čísel tvaru*

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k,$$

kde za $x_1, x_2, \ldots, x_k$ můžeme dosadit libovolná čísla z $\mathbb{Z}$, nazveme ideálem oboru $\mathbb{Z}$.

Zkráceně budeme zapisovat $A = [a_1, a_2, \ldots, a_k]$.

Ideál [5] tak bude značit množinu všech čísel $5 \cdot x$ takových že $x \in \mathbb{Z}$. Platí tedy: $[5] = \{0, \pm 5, \pm 10, \pm 15, \ldots\}$.

Poznámka: Obdobně bychom mohli definovat také ideály oboru integrity $\mathbb{Z}(\sqrt{d})$, tedy například oboru integrity $\mathbb{Z}(\sqrt{-5})$:

Definice 4.10 (Ideál) *Nechť $a_1, a_2, \ldots, a_k$ jsou prvky $\mathbb{Z}(\sqrt{d})$), kde alespoň jedno z nich je různé od nuly. Pak množinu všech čísel tvaru*

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k,$$

kde za $x_1, x_2, \ldots, x_k$ můžeme dosadit libovolná čísla z $\mathbb{Z}(\sqrt{d})$, nazveme ideálem oboru $\mathbb{Z}(\sqrt{d})$.

Je zřejmé, že ideál A má tyto vlastnosti:

- Jestliže $a_1, a_2 \in A$, pak také $a_1 + a_2 \in A$.
- Jestliže $a_1 \in A$ a $x_1 \in \mathbb{Z}$, pak také $a_1 \cdot x_1 \in A$.
- Jestliže $a_1, a_2 \in A$ a $x_1, x_2 \in \mathbb{Z}$, pak také $a_1 \cdot x_1 + a_2 \cdot x_2 \in A$.

Definice 4.11 *Ideály A a B se sobě rovnají, jestliže platí $A = B$ v množinovém smyslu.*

Definice 4.12 (Hlavní ideál) *Ideál A nazveme hlavním ideálem, jestliže jsou všechna čísla ideálu A násobky jediného čísla d. Platí tedy $A = [d]$.*

Věta 4.13 *Každý ideál A oboru integrity $\mathbb{Z}$ je hlavní ideál, tedy je možné jej zapsat jako $A = [d]$.*

Důkaz: Nechť $A = [a_1, a_2, \ldots, a_k]$ a d je největší společný dělitel čísel $a_1, a_2, \ldots, a_k$. Chceme dokázat, že $A = [d]$. Ideál A je množina všech čísel tvaru $a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_k \cdot x_k$, kde $x_1, x_2, \ldots, x_k \in \mathbb{Z}$. Můžeme zapsat:

$$a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_k \cdot x_k = d \cdot \Big(\frac{a_1}{d} \cdot x_1 + \frac{a_2}{d} \cdot x_2 + \cdots + \frac{a_k}{d} \cdot x_k\Big).$$

Pro vhodně zvolená čísla $x_1, x_2, \ldots, x_k$ nabývá závorka hodnoty 1. Při volbě jiných $x_1, x_2, \ldots, x_k$ tedy bude postupně nabývat všech celočíselných hodnot. Výraz $a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_k \cdot x_k$ tedy nabývá právě hodnot dělitelných číslem d.
QED

Číslo d je jednoznačně určené až na znaménko. Zřejmě však platí $[d] = [-d]$. Skutečnost, že $A = [d]$ budeme označovat jako: *Číslo d generuje ideál A.*

Definice 4.14 *Nechť M a N jsou dva ideály. Pak množina všech součinů $m \cdot n$ takových, že $m \in M$ a $n \in N$, je součinem ideálů $M \cdot N$.*

Věta 4.15 *Součin ideálu $M = [m]$ a ideálu $N = [n]$ je ideál $m \cdot n = [mn]$.*

Důkaz: Množina $M \cdot N$ obsahuje právě všechny součiny tvaru $mx \cdot ny$, kde $x, y \in \mathbb{Z}$, tedy čísla tvaru $xy \cdot mn$. Za xy je možné dosadit libovolný prvek ze $\mathbb{Z}$. Každé číslo z $M \cdot N$ je tedy dělitelné číslem mn. A obráceně – každé číslo dělitelné mn je prvkem množiny $M \cdot N$. Proto platí $M \cdot N = [mn]$.
QED

Definice 4.16 (Norma ideálu) *Nechť $D = [d]$ a $d > 0$. Potom číslo d je* norma ideálu D. *Značíme $\mathcal{N}(D) = d$.*

Jako důsledek věty 4.15 dostáváme vztah:

$$\mathcal{N}(M \cdot N) = \mathcal{N}(M) \cdot \mathcal{N}(N).$$

Ke každému číslu $d > 0$ jsme tak získali přiřazený právě jeden ideál, a to $D = [d]$. A naopak ke každému ideálu D máme určené právě jedno celé číslo, a to

jeho normu. Pro obor integrity celých čísel tedy může být vybudována aritmetika ideálů, která se v zásadě chová podle pravidel aritmetiky celých kladných čísel. Ideály je totiž možné v tomto oboru jednoznačně reprezentovat celými kladnými čísly a z definice zavedených pojmů je zřejmé, že jsme při jejich zavádění brali ohled právě na pravidla celočíselné aritmetiky. Můžeme tak například zavést také pojem dělitelnosti ideálů:

Definice 4.17 *Ideál A je dělitelný ideálem B právě tehdy, když existuje ideál C takový, že $A = B \cdot C$.*

Pro značení dělitelnosti ideálů použijme běžně užívaný znak dělitelnosti a pišme $B|A$.

Protože v oboru $\mathbb{Z}$ existuje jednotkový ideál, je každý ideál dělitelný sám sebou a právě jednotkovým ideálem.

Definice 4.18 (Prvoideál) *Nechť ideál A je dělitelný pouze sám sebou a jednotkovým ideálem. Pak je ideál A* prvoideál.

Věta 4.19 *A je prvoideál právě tehdy, když jeho norma je prvočíslo.*

Důkaz: Větu dokážeme sporem. Předpokládejme tedy, že norma ideálu P je složené číslo $mn > 1$, kde $m > 1$ a $n > 1$. Platí $P = [mn]$, a tedy také $P = [m] \cdot [n]$, kde $[m]$ ani $[n]$ není jednotkový ideál. Pak by ovšem byl ideál P dělitelný ideály $[m] \neq P$ a $[n] \neq P$. To je ovšem spor s předpokladem, že prvoideál je dělitelný pouze jednotkovým ideálem a sám sebou.

Opačná implikace je zřejmá – pokud ideál $[p]$ má normu p takovou, že p je prvočíslo, pak z jednoznačného přiřazení není dělitelný žádný jiným ideálem než sám sebou a jednotkovým, tedy se jedná o prvoideál.
QED

Věta 4.20 *Každý nejednotkový ideál oboru integrity $\mathbb{Z}$ je možné zapsat jako jednoznačný součin konečného počtu prvoideálů.*

Důkaz: Základní věta aritmetiky říká, že každé celé kladné číslo je možné jednoznačně rozložit na součin prvočísel. Z faktu, že umíme každému ideálu

v okruhu $\mathbb{Z}$ jednoznačně přiřadit celé kladné číslo, plyne, že umíme jednoznačně rozložit také nejednotkový ideálu okruhu $\mathbb{Z}$.
QED

Ukázali jsme tedy – alespoň na oboru integrity celých čísel –, že je možné vybudovat systém ideálních čísel, se kterými je možné zacházet jako s dalšími prvky okruhu, a přitom získat zcela nové řešení některých početních úkonů.

Výše dokázaná věta má také své obecné znění. Nazývá se jako *Základní věta teorie ideálů* a její důkaz je možno nahlédnout v [12].

Ideály dokázaly vyřešit mnohé z historických problémů – ačkoliv k důkazu Velké Fermatovy věty nakonec nevedly; Kummer však na základě svých ideálních čísel dokázal, že Velká Fermatova věta platí pro každý exponent, který je tzv. regulárním prvočíslem. V kvadratických tělesech představují ideály možnost, jak prvky tělesa jednoznačně rozložit na součin ireducibilních prvků (nenulových prvků, které nejsou rovny jednotce ve struktuře a jsou dělitelné pouze jednotkou a samy sebou) – tedy jak je jednoznačně faktorizovat.

Kapitola 5

Závěr

Cílem této bakalářské práce bylo vytvořit základní přehled o práci s ideály a filtry v algebře a logice. Protože se jedná o širokou problematiku, nebylo možné se věnovat všem jednotlivým oblastem. V práci proto byly zpracovány pouze okruhy vybrané s ohledem na záběr zájmu běžného studenta logiky, respektive začátečníka v této oblasti matematiky/logiky.

V první kapitole jsme se proto věnovali ideálům v okruzích – jejich definici, základním větám a nakonec větám o isomorfismu okruhů, které představují důležité stavební kameny pro další matematické konstrukce. Čtenář měl možnost seznámit se také se základní prací nad okruhy.

Druhá kapitola se věnovala ideálům a filtrům ve svazech, konkrétně v Booleových algebrách. Zde jsme si ukázali základní větu o ultrafiltrech a především Stoneovu větu o reprezentaci, která mimo jiné přináší čtenářovi hlubší vhled do pochopení Booleových algeber. Zjistili jsme také, že mezi speciálními okruhy (Booleovými) a algebrami existuje těsný vztah, dokonce možnost převodu jednoho systému na druhý.

Ve třetí kapitole jsme poté představili Lindenbaum-Tarského algebry a pomocí nich (a práce s ultrafiltry) jsme dokázali větu o úplnosti výrokové logiky – prezentovali jsme tak důkaz úplnosti odlišný od toho, který se běžně vyučuje v kurzech klasické logiky.

A konečně v poslední kapitole jsme se podívali do historie a snažili se vypát-

rat, jak byl do matematiky (potažmo logiky) zaveden pojem *ideál*. Tato část se snažila podat ucelený sled událostí včetně historického pozadí, které za vznikem tohoto pojmu stálo. Vzhledem k náročnosti dané problematiky a především vzhledem k relevantnosti tématu neobsahuje tato kapitola všechny důkazy, které byly na cestě v zavedení pojmu *ideál* použity. Některé důkazy byly zjednodušeny nebo nebyly představeny v celém svém znění. Pro základní představu o problému to však ani nebylo potřeba.

Jak již bylo zmíněno – tato práce není rozhodně vyčerpávajícím materiálem pro seznámení se s problematikou filtrů a ideálů. Studentovi logiky, matematiky či jiného oboru však zajisté poslouží jako vhodný materiál pro ucelení znalostí z této oblasti a jistě i jako inspirace pro další (samo)studium. Další témata, na která bohužel v této práci již nezbylo místo, jsou například čtvrtá věta o isomorfismu okruhů, alternativní důkaz úplnosti predikátové logiky či standardní důkaz základní věty teorie ideálů (tj. bez zjednodušení na konkrétní okruh – v našem případě na obor integrity celých čísel). Stejně tak by si zasloužila větší pozornost také teorie modelů, na jejímž základě je pomocí ultrafiltrů (a ultraproduktu) vystavěn alternativní důkaz věty o kompaktnosti.

Literatura

[1] Bohuslav BALCAR, Petr ŠTĚPÁNEK: *Teorie množin.* Academia, Praha, 1986, ISBN 80-200-0470-X.

[2] Štefan SCHWARZ: *Algebraické čísla.* Přírodovědecké nakladatelství, Praha, 1950.

[3] Simon SINGH: *Velká Fermatova věta.* Academia, Praha, 2002, ISBN 978-80-200-1483-2.

[4] Jiří ROSICKÝ: *Algebra: Grupy a okruhy.* Masarykova univerzita, Brno, 2000, ISBN 80-210-2303-1.

[5] Vítězslav ŠVEJDAR: *Logika – neúplnost, složitost a nutnost.* Academia, Praha, 2002, ISBN 80-200-1005-X.

[6] Jan KOPKA: *Svazy a Booleovy algebry.* Univerzita J. E. Purkyně, Ústí nad Labem, 1991, ISBN 978-80-200-1483-2.

[7] Steven GIVANT, Paul HALMOS: *Introduction to Boolean Algebras.* Springer Science+Business Media, New York, 2009, ISBN 978-0-387-40293-2.

[8] Radek HONZÍK: *Boolean Algebras – Booleovy algebry: Lecture Notes.* 2012

[9] Radek HONZÍK: *Introduction to Mathematics, II – Úvod do matematiky II: Lecture Notes.* 2011

[10] Lech POLKOWSKI: *Approximate Reasoning by Parts: An Introduction to Rough Mereology.* Springer-Verlag, Berlin, 2011, ISBN 978-3-642-22279-5.

[11] Richard DEDEKIND: *On the composition of binary quadratic forms.* V překladu Jeremyho Avigada, 2004.
Dostupné online z *http://www.andrew.cmu.edu/user/avigad/Papers/ideals71.pdf* [cit. 2013-04-03]

[12] Helmut KOCH: *Introduction to Classical Mathematics: From the quadratic reciprocity law to the uniformization theorem. 1.* Springer, London, 1991, ISBN 978-0-792-31231-4.