doc. Libor Polák

Algebra II.

zpracoval Aleš Křenek
11. května 1995

Obsah

1 Ideály a faktorové okruhy

Definice 1.1
Nechť $\mathfrak{R} = (R, +, .)$ je okruh, $\emptyset \neq I \subseteq R$ nazveme *ideálem,* platí-li

$$a, b \in I \implies a + b \in I$$
$$a \in I, r \in R \implies ra, ar \in I$$

Ideál je zejména normální podgrupa $(R, +)$, nejmenší a největší ideály jsou tzv. *nevlastní* $\{0\}$ a R. Průnik libovolného neprázdného systému ideálů je opět ideál – můžeme hovořit o generování.

Umíme utvořit faktorgrupu $(R/I, +) = \{a + I \mid a \in R\}$, sčítání definujeme $(a + I) + (b + I) = (a + b) + I$. Podobně definujeme násobení $(a + I)(b + I) = (ab) + I$. Je nutné ověřit korektnost – nezávislost na volbě reprezentanta.

Lemma 1.2
$\mathfrak{R}/I = (R/I, +, .)$ je okruh. Zobrazení $\iota\colon a \mapsto a + I$ je surjektivní homomorfismus $\mathfrak{R} \to \mathfrak{R}/\mathfrak{I}$. □

Definice 1.3
$\mathfrak{R}/I$ se nazývá *faktorový okruh* okruhu $\mathfrak{R}$ podle ideálu I.

Zabývejme se dále strukturou $R[x]/(f)$, kde R je těleso, $f \in R[x]$ nekonstantní polynom. Definujeme

$$R[x]/(f) = \{g + (f) \mid g \in R[x]\}$$

Klademe $g + (f) = h + (f)$, platí-li $f \mid g - h$, tedy g, h dávají po dělení polynomem f stejný zbytek. Označme $n = \deg f$. Lze psát

$$R[x]/(f) = \{g + (f) \mid g \in R[x], \deg g < n\}$$

kde už je každý prvek zastoupen právě jednou. Zobrazení $a_{n-1}x^{n-1} + \cdots + a_1x + a_0 + (f) \mapsto (a_0, \ldots, a_{n-1})$ je zřejmě bijekce $R[x]/(f) \to R^n$. Definujeme operace sčítání a násobení

$$(a_0, \ldots, a_{n-1}) + (b_0, \ldots, b_{n-1}) = (a_0 + b_0, \ldots, a_{n-1} + b_{n-1})$$
$$(a_0, \ldots, a_{n-1})(b_0, \ldots, b_{n-1}) = (c_0, \ldots, c_{n-1})$$

kde $c_{n-1}x^{n-1} + \cdots + c_1x + c_0$ je zbytek po dělení polynomu $(a_{n-1}x^{n-1} + \cdots + a_1x + a_0)(b_{n-1}x^{n-1} + \cdots + b_1x + b_0)$ polynomem f.

Zobrazení $\iota\colon a \mapsto a + (f)$ je prostý homomorfismus $R \to R[x]/(f)$, budeme ztotožňovat R a $\iota(R)$. R lze potom považovat za podtěleso okruhu $R[x]/(f)$.

Věta 1.4
Polynom f má kořen $x + (f)$ v $R[x]/(f)$.

Důkaz: Polynom $f \in R[x]$ chápeme jako polynom nad $R[x]/(f)$ s koeficienty $a_0 + (f), \ldots, a_{n-1} + (f)$. Přímým dosazením dostáváme $\cdots = f + (f) = 0$. □

Věta 1.5
$R[x]/(f)$ je těleso právě tehdy, když f je ireducibilní.

Důkaz: Zprava doleva plyne z Bezoutovy rovnosti, zleva doprava vedeme nepřímo, faktory f jsou dělitelé nuly. □

2 Rozšíření těles

Definice 2.1

Okruh $\mathfrak{R}$ se nazývá *podtělesem* tělesa $\mathfrak{T}$, je-li podokruhem a pro každé $0 \neq a \in R$ platí $a^{-1} \in R$ (inverzní prvek chápaný v $\mathfrak{T}$). Jinak říkáme, že $\mathfrak{T}$ je *rozšířením* $\mathfrak{R}$, píšeme $\mathfrak{T}/\mathfrak{R}$.

Definice 2.2

Nechť $\mathfrak{T}$ je rozšířením $\mathfrak{R}$. Prvek $a \in T$ se nazývá *algebraický* prvek nad $\mathfrak{R}$, je-li kořenem nenulového polynomu nad R, v opačném případě *transcedentní.*

Věta 2.3

Nechť $\mathfrak{T}$ je rozšířením $\mathfrak{R}$, $a \in T$ algebraický. Pak existuje jediný normovaný ireducibilní polynom $f \in R[x]$, ktarý má a za kořen.

Důkaz: Existence. Nechť $f \in R[x]$ je nejmenšího stupně mezi normovanými s kořenem a. Kdyby nebyl ireducibilní, dostáváme spor s minimalitou stupně.

Jednonačnost. Nechť $g \in R[x]$, $g(a) = 0$. Dělením dostáváme $g = qf + r$, $\deg r < \deg f$. Z $g(a) = f(a) = 0$ a minimality stupně f plyne už $r = 0$. Uvažme nějaké jiné $\bar{f}$. Musí platit $f|\bar{f}$ podle předchozího a zároveň $\bar{f}|f$. Odtud $f = \bar{f}$, protože oba jsou normované. □

Poznámka 2.4 KONEČNÁ TĚLESA

1. Pro prvočíslo p a $n \in \mathbb{N}$ existuje těleso o p^n prvcích.
2. Libovolné konečné těleso má p^n prvků.
3. Libovolná dvě konečná tělesa o stejném počtu prvků jsou isomorfní.

Definice 2.5

Pro těleso $\mathfrak{R}$ píšeme zkráceně $R[x_1, \ldots, x_n] = (\cdots((R[x_1])[x_2])\cdots)$. Polynom $f \in R[x_1, \ldots, x_n]$ se nazývá *symetrický,* nemění-li se při libovolné permutaci proměnných.

Uvažme tzv. *elementární symetrické polynomy*

$$\begin{aligned}
\sigma_1 &= x_1 + \cdots + x_n \\
\sigma_2 &= x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_{n-1}x_n \\
&\vdots \\
\sigma_k &= \sum_{1 \leq i_1 < \cdots < i_k \leq n} x_{i_1} \ldots x_{i_k} \\
&\vdots \\
\sigma_n &= x_1 \ldots x_n
\end{aligned}$$

Věta 2.6

Každý symetrický polynom lze vyjádřit právě jedním způsobem jako polynom v elementárních symetrických polynomech. □

3 Teorie svazů

3.1 Dvojí definice

Definice 3.1

Nechť $\mathfrak{A} = (A, \leq)$ je uspořádaná množina. $\mathfrak{A}$ se nazývá sup-*polosvaz* (spojový, horní), existuje-li $\sup_{\mathfrak{A}}\{a, b\}$ pro libovolná $a, b \in A$. Analogisky definujeme inf-*polosvaz* (průsekový, dolní). $\mathfrak{A}$ je svaz, existuje-li současně $\sup_{\mathfrak{A}}\{a, b\}$ i $\inf_{\mathfrak{A}}\{a, b\}$. Svaz je úplný, existuje-li $\sup X$ i $\inf X$ pro libovolnou $X \subseteq A$.

Věta 3.2

Je-li $\mathfrak{A}$ uspořádaná a pro všechny $X \subseteq A$ existuje $\inf X$. Pak $\mathfrak{A}$ je úplný.

Důkaz: Vezmeme $a = \inf Y = \inf\{y \in A \mid y \geq x, \forall x \in X\}$. Je to horní závora X a každá jiná je prvkem Y, a je tedy $\sup X$. □

Definice 3.3

Binární operace na množině A se nazývá *idempotentní,* platí-li $a \cdot a = a$ pro každé $a \in A$.

Definice 3.4

$\mathfrak{S} = (S, .)$ se nazývá *algebraicky definovaný polosvaz,* je-li operace asociativní, komutativní a idempotentní. $\mathfrak{L} = (L, \wedge, \vee)$ je *algebraicky definovaný svaz,* jsou-li $(L, \wedge)$ a $(L, \vee)$ algebraicky definované polosvazy a platí tzv. *absorbční zákony*

$$a \wedge (a \vee b) = a \qquad a \vee (a \wedge b) = a$$

Operace $\wedge, \vee$ se běžně nazývají *průsek* a *spojení.*

Označme korespondenci mezi dvojí definicí polosvazu

$$\begin{aligned} \mathfrak{A} = (A, \leq) &\mapsto \mathfrak{A}_{\mathfrak{s}} = (\mathfrak{A}, .) \qquad ab := \sup\{a, b\} \\ \mathfrak{S}^{s} = (S, \leq) &\mapsto \mathfrak{S} = (\mathfrak{S}, .) \qquad a \leq b \Leftrightarrow ab = b \end{aligned}$$

Věta 3.5

1. Pro sup-polosvaz $\mathfrak{A}$ je $\mathfrak{A}_{\mathfrak{s}}$ algebraicky definovaný polosvaz.
2. Pro algebraicky definovaný polosvaz $\mathfrak{S}$ je $\mathfrak{S}^{\mathfrak{s}}$ sup-polosvaz a $\sup_{\mathfrak{S}^s}\{a, b\} = ab$ pro všechna $a, b \in S$.
3. Pro sup-polosvaz $\mathfrak{A}$ platí $(\mathfrak{A}_{\mathfrak{s}})^{\mathfrak{s}} = \mathfrak{A}$.
4. Pro algebraicky definovaný polosvaz $\mathfrak{S}$ platí $(\mathfrak{S}^{s})_{s} = \mathfrak{S}$.

Věta 3.6

Nechť $\mathfrak{A} = (A, \leq)$ je svaz. Definujeme

$$\begin{aligned} \mathfrak{A}_{i} &= (A, \wedge) \qquad a \wedge b := \inf\{a, b\} \\ \mathfrak{A}_{s} &= (A, \vee) \qquad a \vee b := \sup\{a, b\} \end{aligned}$$

Takto definované $\wedge, \vee$ jsou vázány absorbčními zákony. Naopak nechť $\mathfrak{L} = (L, \wedge, \vee)$ je algebraicky definovaný svaz. Definujeme uspořádání

$$a \leq^{i} b \iff a \wedge b = a \qquad a \leq^{s} b \iff a \vee b = b$$

Uspořádání $\leq^{i}, \leq^{s}$ jsou stejná, tedy $(L, \leq)$ je svaz. □

3.2 Morfismy

Definice 3.7

Nechť $\mathfrak{A} = (A, \leq), \mathfrak{B} = (\mathfrak{B}, \leq)$ jsou uspořádané množiny. Zobrazení $\alpha\colon A \to B$ se naývá *isotonní,* platí-li pro všechna $a, a' \in A$ $a \leq a' \implies \alpha(a) \leq \alpha(a')$. Isotonní zobrazení je *vnoření,* pokud navíc platí $\alpha(a) \leq \alpha(a') \implies a \leq a'$. Konečně *isomorfismus* (uspořádaných množin) je surjektivní vnoření.

Definice 3.8

Nechť $\mathfrak{A}, \mathfrak{B}$ jsou svazy, zobrazení $\alpha\colon A \to B$ se nazývá $\vee$-*homomorfismus* (spojový), pokud $\alpha(a \vee a') = \alpha(a) \vee \alpha(a')$. Analogicky definujeme $\wedge$-*homomorfismus* (průsekový). Zobrazení je *homorfismus* je-li současně $\vee$- i $\wedge$-homomorfismus. Konečně *isomorfismus* (svazů) je bijektivní homomorfismus.

Lemma 3.9

Nechť $\mathfrak{A}, \mathfrak{B}$ jsou svazy, $\alpha\colon A \to B$ zobrazení. Potom

1. α je $\vee$-homomorfismus znamená, že α je isotonní.
2. α je isomorfismus uspořádaných množin právě tehdy, když je isomorfismus svazů.

□

Věta 3.10 Slabá

Pro libovolnou uspořádanou množinu $\mathfrak{A}$ existuje úplný svaz $\mathfrak{B} = (B, \leq)$ a vnoření $\alpha\colon A \to B$.

Důkaz: Definujme $(a] := \{x \in A \mid x \leq a\}$. Potom zobrazení $\iota\colon a \mapsto (a]$ je hledané vnoření do svazu $(2^A, \subseteq)$. □

Definice 3.11

Nechť $\mathfrak{A} = (A, \leq)$ je uspořádaná množina. Množinu $\emptyset \neq J \subseteq A$ nazýváme ideál, platí-li

1. Jestliže $a \in J, x \in A, x \leq a$, potom $x \in J$ (analogie násobení).
2. Pro všechna $i \in I$ je $a_i \in J$. Potom existuje $\sup\{a_i \mid i \in I\}$ (analogie sčítání).

Věta 3.12 Lepší

Pro libovolnou uspořádanou množinu $\mathfrak{A}$ existuje úplný svaz $\mathfrak{B} = (B, \leq)$ a vnoření $\alpha\colon A \to B$ zachovávající všechna existující infima a suprema.

Důkaz: Předpokládejme, že $\mathfrak{A}$ má nejmenší prvek (pokud ne, přidáme takový). Struktura $\mathfrak{J}(\mathfrak{A}) = (\mathfrak{J}(\mathfrak{A}), \subseteq)$ je úplný svaz všech ideálů v $\mathfrak{A}$. Zobrazení $\iota\colon a \mapsto (a]$ je hledané vnoření $A \to J(\mathfrak{A})$. □

Ideály mohou reprezentovat reálná čísla. Přidáme k racionálním číslům nejmenší prvek $-\infty$, potom nevlastní ideály jsou $\{-\infty\}$ a $\mathbb{Q} \cup \{-\infty\}$, vlastní jsou $\{\{x \in \mathbb{Q} \cup \{-\infty\} \mid x \leq a\} \mid a \in \mathbb{R}\}$ a ty odpovídají přesně reálným číslům.

Věta 3.13 O pevném bodu

Nechť $\mathfrak{L} = (L, \leq)$ je úplný svaz, $\alpha\colon L \to L$ isotonní zobrazení. Pak existuje $a \in L$ takové, že $\alpha(a) = a$.

Důkaz: Uvažujme $X = \{x \in L \mid \alpha(x) \geq x\}$ a označme $a = \sup X$. Z vlastností suprema a isotonie se ukáže, že $\alpha(a)$ je horní závora X, tedy platí $a \leq \alpha(a)$. Odtud $\alpha(a) \leq \alpha(\alpha(a))$, tedy $\alpha(a) \in X$ a platí také $\alpha(a) \leq a$. □

3.3 Nerovnosti

Věta 3.14
V libovolném svazu $\mathfrak{L} = (L, \wedge, \vee)$ platí pro $a, b, c \in L$

$$\left.\begin{array}{l} a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c) \\ a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c) \end{array}\right\} \text{distributivní nerovnosti}$$

$$a \leq c \implies a \vee (b \wedge c) \leq (a \vee b) \wedge c \quad \text{modulární nerovnost}$$

$$(a \wedge b) \vee (a \wedge c) \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c) \wedge (b \vee c) \quad \text{mediální nerovnost}$$

□

Definice 3.15
Svaz $\mathfrak{L} = (L, \wedge, \vee)$ se nazývá *modulární,* platí-li pro $a, b, c \in L$ $a \leq c \implies a \vee (b \wedge c) = (a \vee b) \wedge c$; *distributivní,* platí-li $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$

Lemma 3.16
Každý distributivní svaz je modulární. □

3.4 Modulární svazy

Lemma 3.17
Svaz je modulární právě tehdy, když platí $a \vee (b \wedge (c \vee a)) = (a \vee b) \wedge (c \vee a)$. □

Věta 3.18
Svaz $\mathfrak{L} = (L, \wedge, \vee)$ je modulární právě tehdy, když platí pro všechna $a, b, c \in L$

$$a \leq b, a \wedge c = b \wedge c, a \vee c = b \vee c \implies a = b$$

Důkaz: Zleva doprava plyne z absorbčních zákonů a modulární rovnosti, stačí rozepsat $a = a \vee (a \wedge c)$. Obráceně vezmeme $x, y, z \in L, x \leq z$ a chceme pro ně splnit modulární rovnost. Do tvrzení věty stačí dosadit $a = x \vee (y \wedge z)$, $b = (x \vee y) \wedge z$ a $c = y$. □

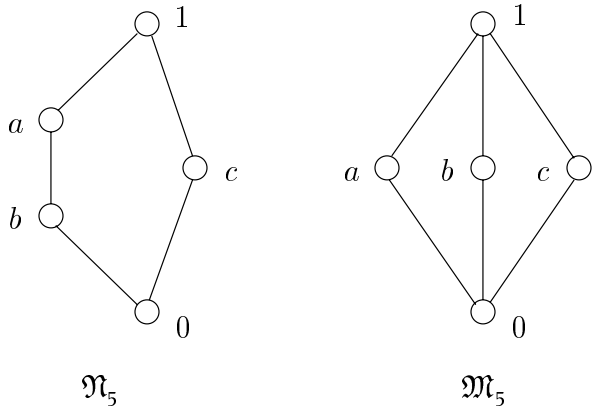
Definice 3.19
Svaz $\mathfrak{L} = (L, \wedge_L, \vee_L)$ nazýváme *podsvazem* svazu $\mathfrak{K} = (K, \wedge_K, \vee_K)$ je-li $L \subseteq K$ a pro každé $a, b \in L$ platí

$$a \wedge_L b = a \wedge_K b$$
$$a \vee_L b = a \vee_K b$$

Modulární a distributivní svazy lze charakterizovat podle toho, jestli některý ze svazů z obrázku 1 je jejich podsvazem. $\mathfrak{N}_5$ není modulární, $\mathfrak{M}_5$ modulární je, ale není distributivní.

Věta 3.20
Svaz $\mathfrak{L} = (L, \wedge, \vee)$ je modulární právě tehdy, když neobsahuje podsvaz isomorfní s $\mathfrak{N}_5$.

Důkaz: Zleva doprva je tvrzení zřejmé. Pokud $\mathfrak{L}$ není modulární, musí podle předchozí věty existovat $a, b, c \in L$ takové, že $a < b, a \wedge c = b \wedge c, a \vee c = b \vee c$. Tedy c musí být s a, b nesrovnatelné, dostáváme už $\mathfrak{N}_5$. □



Obrázek 1: Zlobivé svazy

Lemma 3.21
Svaz $\mathfrak{L} = (L, \wedge, \vee)$ je distributivní právě tehdy, když pro každé $a, b, c \in L$ platí $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$. □

Věta 3.22
Svaz $\mathfrak{L} = (L, \wedge, \vee)$ je distributivní právě tehdy, když platí pro všechna $a, b, c \in L$

$$a \wedge c = b \wedge c, a \vee c = b \vee c \implies a = b$$

□

Věta 3.23
Svaz $\mathfrak{L} = (L, \wedge, \vee)$ je distributivní právě tehdy, když neobsahuje podsvaz isomorfní s $\mathfrak{N}_5$ nebo $\mathfrak{M}_5$. □

Definice 3.24
Nechť $\mathfrak{A} = (A, \leq)$ je uspořádaná množina. Množina $X \subseteq A$ se nazývá *dědičná,* platí-li pro všechna $x \in X, a \in A$

$$a \leq x \implies a \in X$$

Značíme $H\mathfrak{A}$ množinu všech dědičných podmnožin množiny $\mathfrak{A}$, podobně $\mathcal{H}\mathfrak{A} = (H\mathfrak{A}, \subseteq)$.

Definice 3.25
Nechť $\mathfrak{L} = (L, \wedge, \vee)$ je svaz. Prvek $a \in L$ se nazývá *spojově ireducibilní,* platí-li pro všechna $b, c \in L$

$$a = b \vee c \implies a = b \text{ nebo } a = c$$

Označujeme $J\mathfrak{L}$ množinu všech spojově ireducibilních prvků svazu $\mathfrak{L}$ s vyjímkou nejmenšího (pokud existuje) a $\mathcal{J}\mathfrak{L} = (J\mathfrak{L}, \wedge, \vee)$.

Věta 3.26
Nechť $\mathfrak{L} = (L, \wedge, \vee)$ je konečný distributivní. Pak platí $\mathfrak{L} \cong \mathcal{H}(\mathcal{J}\mathfrak{L})$.

Důkaz: Hledaným isomorfismem je zobrazení $\alpha \colon a \mapsto \{x \in J\mathfrak{L} \mid x \leq a\}$. Poměrně snadno se ukáže, že je to bijekce a zachovává operace $\wedge, \vee$. □

Definice 3.27

Okruhem množin nad nějakou množinou A je libovolný systém jejích podmnožin uzavřený na operace $\cap, \cup$.

Důsledek 3.28

Libovolný okruh množin je isomorfní $\mathcal{H}(\mathcal{J}(\mathcal{L}, \wedge, \vee))$ pro vhodný konečný svaz $(L, \wedge, \vee)$.

Důkaz: Libovolný okruh množin je distributivní svaz. □

3.5 Booleovy svazy

Definice 3.29

Svaz $\mathfrak{L} = (L, \wedge, \vee)$ se nazývá *omezený,* pokud má nejmenší a největší prvek. Standardně je značíme 0,1. Dále nechť $a, b \in L$ jsou prvky omezeného svazu. Říkáme, že b je *komplement* prvku a, platí-li $a \wedge b = 0, a \vee b = 1$.

Prvek omezeného svazu může mít žádný, jeden i více komplementů (viz $\mathfrak{M}_5$). 1 je vždy komplement 0 a naopak.

Definice 3.30

Komplementární svaz je omezený svaz, ve kterém má každý prvek právě jeden komplement. *Booleův svaz* je distributivní komplementární svaz.

Věta 3.31

Nechť $\mathfrak{L} = (L, \wedge, \vee)$ je distributivní svaz.

1. Každé $a \in L$ má nejvýše jeden komplement.
2. Nechť $a \leq x \leq b$ a x má komplement. Potom má x komplement i v intervalu $[a, b] = \{y \in L \mid a \leq y \leq b\}$.

Důkaz: (1) plyne z vlastností komplementu, absorbčních zákonů a distributivity. (2) nechť y je komplement x ve svazu $\mathfrak{L}$. Označíme $z = (y \vee a) \wedge b$. Potom z je komplement x v intervalu $[a, b]$ – ukážeme $x \wedge z = a, x \vee z = b$. □

Definice 3.32

Booleova algebra je šestice $\mathfrak{B} = (B, \wedge, \vee, 0, 1, ')$, kde $(B, \wedge, \vee)$ je Booleův svaz a pro každé $a \in B$ platí

$$a \vee 0 = a \qquad a \vee a' = 1$$
$$a \wedge 1 = 1 \qquad a \wedge a' = 0$$

Lemma 3.33

V libovolné Booleově algebře platí

$$(a \vee b)' = a' \wedge b'$$
$$(a \wedge b)' = a' \vee b'$$

□

Definice 3.34

Pole množin nad množinou A je okruh množin nad A uzavřený na operaci rozdílu.

Věta 3.35

Libovolná konečná Booleova algebra $\mathfrak{B}$ je isomorfní $(2^A, \cap, \cup, \emptyset, A, {}^{\complement})$ pro vhodnou konečnou A, přitom operaci komplementu definujeme $X^{\complement} = A \setminus X$.

Důkaz: Definujeme relaci *pokrývání*

$$a \supset\!\!- b \iff \forall a, b, c \in A a \geq c > b \Rightarrow a = c$$

Prvky $a \supset\!\!- 0$ nazýváme *atomy.* Snadno se ukáže (věta 3.31), že prvky $J\mathfrak{B}$ jsou právě atomy. Tedy $\mathcal{J}\mathfrak{B}$ je protiřetězec, každá jeho podmnožina je dědičná. Stačí vzít $A = J\mathfrak{B}$, potom $2^A = \mathcal{H}(\mathcal{J}\mathfrak{B})$ a tvrzení plyne z předchozích vět. □

Důsledek 3.36

Libovolná Booleova algebra je isomorfní vhodnému poli množin. □

Struktura	typ	op. symboly
svaz	$(2,2)$	$(\wedge,\vee)$
grupa	(2)	$(\cdot)$
grupa s 1 a inverzí	$(2,0,1)$	$(\cdot,1,^{-1})$
vekt. prost. nad R	$(2,(1)_{r\in R})$	$(+,(\lambda_r)_{r\in R})$

Tabulka 1: Jazyky konkrétních struktur

4 Univerzální algebra

4.1 Pojem τ-algebry, kongruence

Definice 4.1

Systém $(n_\sigma)_{\sigma\in\Sigma}$ nezáporných celých čísel nazveme *typem,* množinu Σ chápeme jako množinu indexů. S každým typem uvažujeme systém operačních symbolů $(f_\sigma)_{\sigma\in\Sigma}$. *Jazykem* nazýváme uspořádanou dvojici

$$\big((n_\sigma)_{\sigma\in\Sigma},(f_\sigma)_{\sigma\in\Sigma}\big)$$

Algebra typu τ (τ-algebra) je potom uspořádaná dvojice

$$\mathfrak{A}=\big(A,(f_\sigma^{\mathfrak{A}})_{\sigma\in\Sigma}\big)$$

kde A je množina a pro každé $\sigma\in\Sigma$ je $f_\sigma^{\mathfrak{A}}$ n_σ-ární operace na A, kde n-ární operace znamená zobrazení $A^n\to A$, včetně $A^0=\{\emptyset\}$ dávající výběr prvku.

Jazyky pro konkrétní algebraické struktury ukazuje tabulka 1. Operace λ_r znamená násobení skalárem $r\in R$. Je-li těleso R nekonečné, je nekonečný i daný jazyk.

Definice 4.2

Nechť $\mathfrak{A}=(A,(f_\sigma^{\mathfrak{A}})_{\sigma\in\Sigma})$ je τ-algebra. Relace ρ na množině A se nazývá *kongruence* τ-algebry $\mathfrak{A}$, platí-li pro každé $\sigma\in\Sigma, a_1,b_1,\dots,a_{n_\sigma},b_{n_\sigma}\in A$

$$a_1\ \rho\ b_1,\dots,a_{n_\sigma}\ \rho\ b_{n_\sigma}\implies f_\sigma^{\mathfrak{A}}(a_1,\dots,a_{n_\sigma})\ \rho\ f_\sigma^{\mathfrak{A}}(b_1,\dots,b_{n_\sigma})$$

Potom je možné definovat *faktorovou algebru* algebry $\mathfrak{A}$ podle kongruence ρ

$$\mathfrak{A}/\rho:=\big(A/\rho,(f_\sigma^{\mathfrak{A}/\rho})_{\sigma\in\Sigma}\big)\quad\text{kde } f_\sigma^{\mathfrak{A}/\rho}([a_1]_\rho,\dots,[a_{n_\sigma}]_\rho):=\big[f_\sigma^{\mathfrak{A}}(a_1,\dots,a_{n_\sigma})\big]_\rho$$

Korektnost takové definice je zaručena požadavkem na kongruenci.

V grupách kongruence odpovídají normálním podgrupám, faktorizovat podle kongruence znamená totéž, jako podle normální podgrupy. V okruzích hrají stejnou roli ideály. Značíme $Con\,\mathfrak{A}$ množinu všech kongruencí algebry $\mathfrak{A}$ a $E(A)$ množinu všech ekvivalencí na množině A.

Věta 4.3

$(Con\,\mathfrak{A},\subseteq)$ je úplný podsvaz svazu $(E(A),\subseteq)$.

Důkaz: $D_A := \{[a,a] \mid a \in A\}$ je nejmenší, $A \times A$ největší prvek $(Con\,\mathfrak{A}, \subseteq)$. Uvažujme libovolný systém $\rho_i \in Con\,\mathfrak{A}$ pro $i \in I \neq \emptyset$. Zřejmě $\bigcap_{i\in I} \in Con\,\mathfrak{A}$. Dále platí

$$\sup_{Con\,\mathfrak{A}}\{\rho_i \mid i \in I\} \supseteq \sup_{E(A)}\{\rho_i \mid i \in I\}$$

Označme pravou stranu ρ. Stačí ukázat, že je to kongruence. ρ je tranzitivní obal $\bigcup_{i\in I} \rho_i$. Uvažme libovolné $\sigma \in \Sigma$ a označme $n := n_\sigma$. Vezměme libovolná $a_1, \ldots, a_n, b_1, \ldots, b_n \in A$ taková, že $a_1\ \rho\ b_1, \ldots, a_n\ \rho\ b_n$. Chceme ukázat

$$f_\sigma^{\mathfrak{A}}(a_1, \ldots, a_n)\ \rho\ f_\sigma^{\mathfrak{A}}(b_1, \ldots, b_n)$$

Z konstrukce ρ plyne

$$\begin{aligned}
a_1 &= c_{1,1}\ \rho_{i_{1,1}}\ c_{1,2}\ \rho_{i_{1,2}}\ c_{1,3} \cdots \rho_{i_1,m_1-1}\ c_{1,m_1} = b_1\\
a_2 &= c_{2,1}\ \rho_{i_{2,1}}\ c_{2,2}\ \rho_{i_{2,2}}\ c_{2,3} \cdots \rho_{i_2,m_2-1}\ c_{2,m_2} = b_2\\
&\vdots \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \vdots\\
a_n &= c_{n,1}\ \rho_{i_{n,1}}\ c_{n,2}\ \rho_{i_{n,2}}\ c_{n,3} \cdots \rho_{i_n,m_n-1}\ c_{2,m_2} = b_2
\end{aligned}$$

kde $m_1, \ldots, m_n \in \mathbf{N}, c_{\alpha,\beta} \in A, i_{\alpha,\beta} \in I$. Z prvního řádku dostáváme

$$\begin{aligned}
f_\sigma^{\mathfrak{A}}(a_1, \ldots, a_n)\ \rho_{i_{1,1}}\ f_\sigma^{\mathfrak{A}}(c_{1,2}, \ldots, a_n) \implies\\
f_\sigma^{\mathfrak{A}}(a_1, \ldots, a_n)\ \rho\ f_\sigma^{\mathfrak{A}}(c_{1,2}, \ldots, a_n) \implies\\
\cdots\ f_\sigma^{\mathfrak{A}}(a_1, \ldots, a_n)\ \rho\ f_\sigma^{\mathfrak{A}}(b_1, \ldots, a_n)
\end{aligned}$$

Z druhého řádku analogicky

$$f_\sigma^{\mathfrak{A}}(a_1, \ldots, a_n)\ \rho\ f_\sigma^{\mathfrak{A}}(b_1, b_2, \ldots, a_n)$$

atd. □

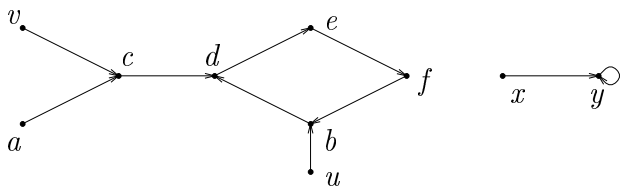
Poznámka 4.4

Uvažujme-li typ (1), dostaneme tzv. 1-unární algebry $\mathfrak{A} = (A, f)$, kde $f\colon A \to A$. Ty leze poměrně přehledně znázornit diagramem (obrázek 2).

Poznámka 4.5

V případě svazů platí následující tvrzení: Nechť $\mathfrak{L} = (L, \wedge, \vee)$ je svaz. Potom $\rho \in Con\,\mathfrak{L}$ právě tehdy, když je to ekvivalence a pro všechna $a, b, c \in L$ platí

$$(a \wedge c)\ \rho\ (b \wedge c) \tag{1}$$
$$(a \vee c)\ \rho\ (b \vee c) \tag{2}$$



Obrázek 2: 1-unární algebra

Důkaz: Přímo z definice kongruence $\rho \in Con\,\mathfrak{L}$ právě tehdy, když je to ekvivalence a pro všechna $a, b, c, d \in L$ platí

$$a\ \rho\ b, c\ \rho\ d \implies \begin{matrix}(a \wedge c)\ \rho\ (b \wedge d)\\ (a \vee c)\ \rho\ (b \vee d)\end{matrix}$$

Odsud dosazením $d := c$ plyne tvrzení.

Naopak předpokládejme $a\ \rho\ b, c\ \rho\ d$. Na základě platnosti (1) a komutativity $\wedge$ je možné psát

$$(a \wedge c)\ \rho\ (b \wedge c) = (c \wedge b)\ \rho\ (d \wedge b) = (b \wedge d)$$

Důkaz pro $\vee$ se vede analogicky. □

Poznámka 4.6

Podobně lze dokázat následující vlastnosti

$$a\ \rho\ b \implies (a \wedge b)\ \rho\ (a \vee b)$$
$$a \leq b \leq c, a\ \rho\ c \implies a\ \rho\ b$$

4.2 Podalgebry

Definice 4.7

Nechť $\mathfrak{A} = \left(A, (f_\sigma^{\mathfrak{A}})_{\sigma\in\Sigma}\right)$ je τ-algebra. Algebru $\mathfrak{B} = \left(B, (f_\sigma^{\mathfrak{B}})_{\sigma\in\Sigma}\right)$ nazveme *podalgebrou* algebry $\mathfrak{A}$, jestliže $B \subseteq A$ a pro všechna $\sigma \in \Sigma, b_1, \ldots, b_{n_\sigma} \in B$ platí

$$f_\sigma^{\mathfrak{A}}(b_1, \ldots, b_{n_\sigma}) = f_\sigma^{\mathfrak{B}}(b_1, \ldots, b_{n_\sigma})$$

Píšeme $\mathfrak{B} \leq \mathfrak{A}$ a $f_\sigma^{\mathfrak{B}} = f_\sigma^{\mathfrak{A}}|B^{n_\sigma}$ (tj. $f_\sigma^{\mathfrak{A}}$ na B^{n_σ} dopadne stejně, jako $f_\sigma^{\mathfrak{B}}$, restrikce funkce)

Lze ovšem jít i z druhé strany

Definice 4.8

Množina $B \subseteq A$ se nazývá nosič podalgebry algebry $\mathfrak{A}$, platí-li pro každé $\sigma \in \Sigma, b_1, \ldots, b_{n_\sigma} \in B$

$$f_\sigma^{\mathfrak{A}}(b_1, \ldots, b_{n_\sigma}) \in B$$

Píšeme $B \leq \mathfrak{A}$.

Je-li $\mathfrak{B} \leq \mathfrak{A}$, potom zřejmě $B \leq \mathfrak{A}$. Naopak, je-li $B \leq \mathfrak{A}$, potom $\left(B, (f_\sigma^{\mathfrak{A}}|B^{n_\sigma})_{\sigma\in\Sigma}\right) \leq \mathfrak{A}$

Věta 4.9

Množina všech podalgeber algebry $\mathfrak{A}$ je vzhledem k $\subseteq$ úplný svaz.

Důkaz je přímočarý. □

Poznámka 4.10

Začneme-li uvažovat podalgebry, plně se projeví formální rozdíl mezi např. Booleovskými svazy a Booleovskými algebrami.

4.3 Homomorfismy

Definice 4.11

Zobrazení $\alpha\colon A \to B$ se nazývá *homomorfismus* τ-algebry $\mathfrak{A} = (A, (f_\sigma^{\mathfrak{A}})_{\sigma\in\Sigma})$ do algebry $\mathfrak{B} = (B, (f_\sigma^{\mathfrak{B}})_{\sigma\in\Sigma})$ platí-li pro každá $\sigma \in \Sigma, a_1, \ldots, a_{n_\sigma} \in A$

$$\alpha\left(f_\sigma^{\mathfrak{A}}(a_1, \ldots, a_{n_\sigma})\right) = f_\sigma^{\mathfrak{B}}\big(\alpha(a_1), \ldots, \alpha(a_{n_\sigma})\big)$$

Implicitně předpokládáme, že obě algebry jsou téhož typu. Homomorfismus značíme $\alpha\colon \mathfrak{A} \to \mathfrak{B}$. *Izomorfismem* rozumíme bijektivní homomorfismus, o dvou algebrách řekneme, že jsou *izomorfní,* pokud mezi nimi existuje izomorfismus.

Poznámka 4.12

Pro libovolnou kongruenci $\rho \in Con\,\mathfrak{A}$ zavádíme označení $\underline{\mathrm{nat}\,\rho}$ pro zobrazení $A \to A/\rho$ takové, že $a \mapsto [a]_\rho$. Jedná se o surjektivní homomorfismus $\mathfrak{A}$ na $\mathfrak{A}/\rho$.

Poznámka 4.13

Pokud $\mathfrak{B} \leq \mathfrak{A}$, značíme standardně $\iota\colon b \mapsto b$ vnoření algebry $\mathfrak{B}$ do $\mathfrak{A}$. Je to prostý homomorfismus.

Lemma 4.14

Relace $\ker\alpha := \{(a, a') \in A \times A \mid \alpha(a) = \alpha(a')\}$ je kongruence na algebře $\mathfrak{A}$.

Důkaz: Z definice $\ker\alpha$ je zřejmé, že se jedná o ekvivalenci. Uvažme libovolné $\sigma \in \Sigma$ a pišme $n = n_\sigma$. Vezměme libovolná $a_1, \ldots, a_n, b_1, \ldots, b_n$ tak, že $a_1 \ \rho\ b_1, \ldots, a_n \ \rho\ b_n$. Potom $\alpha(a_1) = \alpha(b_1), \ldots, \alpha(a_n) = \alpha(b_n)$. Protože α je homomorfismus, lze psát

$$\alpha\left(f_\rho^{\mathfrak{A}}(A_1, \ldots, a_n)\right) = f_\rho^{\mathfrak{B}}\big(\alpha(a_1), \ldots, \alpha(a_n)\big) = f_\rho^{\mathfrak{B}}\big(\alpha(b_1), \ldots, \alpha(b_n)\big) = \alpha\left(f_\rho^{\mathfrak{A}}(b_1, \ldots, b_n)\right)$$

□

Věta 4.15 O HOMOMORFISMU

Nechť $\alpha\colon \mathfrak{A} \to \mathfrak{B}$ je homomorfismus. Označme $\bar\alpha\colon A\ker\alpha \to \alpha(A)$ takové, že $[a]_{\ker\alpha} \mapsto \alpha(a)$. Potom $\alpha(A) \leq \mathfrak{B}$ (je to nosič podalgebry), $\bar\alpha$ je izomorfismus $\mathfrak{A}/\ker\alpha$ na $\alpha(\mathfrak{A})$ a platí $\alpha = \iota \cdot \bar\alpha \cdot \mathrm{nat}\ker\alpha$, viz diagram. Navíc, pokud je α surjektivní, $\mathfrak{B}$ je izomorfní s $\mathfrak{A}/\ker\alpha$.

$$\begin{array}{ccc} A & \xrightarrow{\ \alpha\ } & B \\ {\scriptstyle \mathrm{nat}\ker\alpha}\downarrow & & \uparrow{\scriptstyle \iota} \\ A/\ker\alpha & \xrightarrow{\ \bar\alpha\ } & \alpha(A) \end{array}$$

Důkaz: Z předchozího důkazu je zřejmé, že má smysl uvažovat $\ker\alpha$ – je to kongruence. Dokažme dále:

Množina $\alpha(A)$ je nosič podalgebry. Vezměme libovolná $\sigma \in \Sigma, b_1, \ldots, b_n \in \alpha(A)$. Potom existují jejich vzory $a_1, \ldots, a_n \in A$. Platí

$$f_\sigma^{\mathfrak{B}}(b_1, \ldots, b_n) = f_\sigma^{\mathfrak{B}}\big(\alpha(a_1), \ldots, \alpha(a_n)\big) = \alpha\big(f_\sigma^{\mathfrak{A}}(a_1, \ldots, a_n)\big) \in \alpha(A)$$

Zobrazení $\bar{\alpha}$ je bijekce. Zřejmě je surjektivní a pro libovolná $a, b \in A$ platí $\alpha(a) = \alpha(b) \implies [a]_{\ker\alpha} = [b]_{\ker\alpha}$.
Zobrazení $\bar{\alpha}$ je homomorfismus. Označme $\rho := \ker\alpha$. Pro libovolná $\sigma \in \sigma, a_1, \ldots, a_n \in A$ pišme

$$\begin{aligned}\bar{\alpha}\big[f_\sigma^{\mathfrak{A}/\rho}\big([a_1]_\rho, \ldots, [a_n]\rho\big)\big]_\rho \\ = \alpha\big(f_\sigma^{\mathfrak{A}}(a_1, \ldots, a_n)\big) = f_\sigma^{\mathfrak{B}}\big(\alpha(a_1), \ldots, \alpha(a_n)\big) \\ = f_\sigma^{\alpha(\mathfrak{A})}\big(\bar{\alpha}([a_1]_\rho), \ldots, \bar{\alpha}([a_n]_\rho)\big)\end{aligned}$$

Zobrazení α je složení $\iota \cdot \bar{\alpha} \cdot nat\, ker\alpha$. Pro každé $a \in A$

$$(\iota \cdot \bar{\alpha} \cdot \mathrm{nat}\ker\alpha)(a) = (\iota \cdot \bar{\alpha})([a]_{\ker\alpha}) = \iota(\alpha(a)) = \alpha(a)$$

□

Definice 4.16
Algebra $\mathfrak{B}$ je homomorfní obraz algebry $\mathfrak{A}$, existuje-li surjektivní homomorfismus $\mathfrak{A} \to \mathfrak{B}$.

Důsledek 4.17
Libovolný homomorfní obraz $\alpha(\mathfrak{A})$ je izomorfní s faktoralgebrou $\mathfrak{A}/\ker\alpha$.

4.4 Součiny

Definice 4.18
Nechť $\mathfrak{A}_i = (A_i, (f_\sigma^{\mathfrak{A}_i})_{\sigma\in\Sigma})$ je τ-algebra pro $i \in I$ (i nespočetnou). Na množině $A := \prod_{i\in I} A_i$ definujeme pro $\sigma \in \Sigma$ n_σ-ární operaci $f_\sigma^{\mathfrak{A}}$ takto

$$f_\sigma^{\mathfrak{A}}\big((a_i^1)_{i\in I}, \ldots, (a_i^{n_\sigma})_{i\in I}\big) := \big(f_\sigma^{\mathfrak{A}_i}(a_i^1, \ldots, a_i^{n_\sigma})\big)_{i\in I}$$

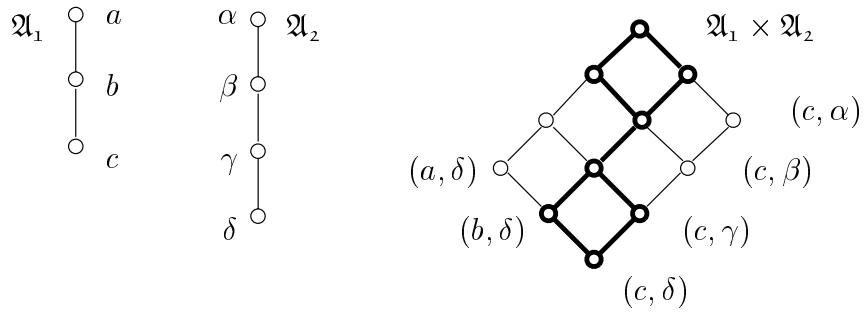
Algebru $\mathfrak{A} = \prod_{i\in I}\mathfrak{A}_i = (A, (f_\sigma^{\mathfrak{A}})_{\sigma\in\Sigma})$ nazveme *součinem* systému algeber $\mathfrak{A}_i$.

Poznámka 4.19
Zobrazení $\epsilon_i \colon A \to A_i$ takové, že $(a_j)_{j\in I} \mapsto a_i$ je surjektivní homomorfismus $\mathfrak{A}$ na $\mathfrak{A}_i$ – přirozená i-tá projekce. Důkaz pro obecnou množinu I vyžaduje axiom výběru.

Definice 4.20
Nechť $(\mathfrak{A}_i)_{i\in I}$ je systém τ-algeber. Algebra $\mathfrak{B} \le \prod_{i\in I}\mathfrak{A}_i$ se nazývá *podpřímý součin* systému $(\mathfrak{A}_i)_{i\in I}$, je-li pro každé $i \in I$ projekce $\epsilon_i|B$ (ϵ_i zúžená na B) surjektivní. Viz obrázek 3 – příklad na svazech.

Věta 4.21
Nechť $\mathfrak{B}$ je podpřímým součinem systému $(\mathfrak{A}_i)_{i\in I}$, $I \neq \emptyset$. Pak $\bigcap_{i\in I}\ker(\epsilon_i|B) = \Delta_A$ (diagonální relace na A).

Důkaz: Nechť $((a_j)_{j\in I}, (b_j)_{j\in I}) \in \bigcap_{i\in I}\ker(\epsilon_i|B)$. Pro každé $i \in I$ platí $((a_j)_{j\in I}, (b_j)_{j\in I}) \in \ker(\epsilon_i|B)$. Tedy $\epsilon_i((a_j)_{j\in I}) = \epsilon_i((b_j)_{j\in I})$, tj. $a_i = b_i$. □



Obrázek 3: Podpřímý součin

Věta 4.22

Nechť $\mathfrak{A} = (A, \dots)$ je τ-algebra, $(\rho_i)_{ß \in I}, I \neq \emptyset$ systém kongruencí takový, že $\bigcap_{i\in I} \rho_i = \Delta_A$. Pak $\mathfrak{A}$ je izomorfní s podpřímým součinem systému $(\mathfrak{A}/\rho_i)_{i\in I}$.

Důkaz: Hledaným izomorfismem je

$$\begin{aligned} \alpha\colon A &\to \textstyle\prod_{i\in I} A/\rho_i \\ a &\mapsto \left([a]_{\rho_i}\right)_{i\in I} \end{aligned}$$

Jedná se zřejmě o surjekci, dokážeme dále vše potřebné.

Zobrazení α je prosté. Nechť $\left([a]_{\rho_i}\right)_{i\in I} = \left([b]_{\rho_i}\right)_{i\in I}$. Pro každé $i \in I$ platí $[a]_{\rho_i} = [b]_{\rho_i}$, tedy $(a,b) \in \rho_i$, to znamená $(a,b) \in \bigcap_{i\in I} \rho_i = \Delta_A$.

Zobrazení α je homomorfismus. Uvažme tradičně $\sigma \in \Sigma, n = n\sigma, a_1, \dots, a_n \in A$. Potom podle definic zobrazení α, operace na součinu a faktoralgebře můžeme psát

$$\begin{aligned} f_\sigma^{\prod_{i\in I}\mathfrak{A}/\rho_i}\left(\alpha(a_1),\dots,\alpha(a_n)\right) &= f_\sigma^{\cdots}\left(\left([a_1]_{\rho_i}\right)_{i\in I},\dots,\left([a_n]_{\rho_i}\right)_{i\in I}\right) \\ &= \left(f_\sigma^{\mathfrak{A}/\rho_i}\left([a_1]_{\rho_i},\dots,[a_n]_{\rho_i}\right)\right)_{i\in I} = \left(\left[f_\sigma^{\mathfrak{A}}(a_1,\dots,a_n)\right]_{\rho_i}\right)_{i\in I} \end{aligned}$$

To už je, opět podle definice α, $\alpha\left(f_\sigma^{\mathfrak{A}}(a_1,\dots,a_n)\right)$.

Množina $\alpha(A)$ je podpřímý součin. Máme ukázat, že zobrazení

$$\epsilon_i|\alpha(\mathfrak{A})\colon \prod_{j\in I} \mathfrak{A}/\rho_j \to \mathfrak{A}/\rho_i$$

je surjektivní. Vezměme libovolný prvek A/ρ_i, tj. $[a]_{\rho_i}$ pro vhodné $a \in A$. To už je ale obrazem $\alpha(a)$.

□

Definice 4.23

Algebra $\mathfrak{A} = (A, (f_\sigma^{\mathfrak{A}_i})_{\sigma\in\Sigma})$ se nazývá podpřímo rozložitelná, existuje-li systém kongruencí $(\rho_i)_{i\in I}$, $I \neq \emptyset$ takový, že

$$\bigcap_{i\in I} \rho_i = \Delta_A \qquad \text{a zároveň } \rho_i \neq \Delta_A \text{ pro každé } i \in I$$

Například na obrázku 3 je podpřímý součin tří- a čtyřprvkového lineárního svazu, tříprvkový lineární svaz je podpřímým součinem dvou dvouprvkových. Oproti tomu $\mathfrak{M}_5$ je podpřímo nerozložitelný.

Věta 4.24 (AC)
Každá netriviální[1] τ-algebra $\mathfrak{A}$ je izomorfní podpřímému součinu vhodného neprázdného systému $(\mathfrak{A})_{i\in I}$ podpřímo nerozložitelných τ-algeber. Přitom každá $\mathfrak{A}_i$ je faktoralgebrou $\mathfrak{A}$.

Lemma 4.25 Zornovo
Nechť $\mathfrak{A} = (A, \leq)$ je taková uspořádaná množina, že každý řetězec v $\mathfrak{A}$ má horní závoru. Potom pro libovolné $a \in A$ existuje maximální prvek $\bar{a}$ v $\mathfrak{A}$ takový, že $a \leq \bar{a}$.

Toto lemma je ekvivalentní axiomu výběru. Důkaz věty je poněkud ošklivý, označen jako nepovinný. Využívá právě Zornovo lemma.

Věta 4.26
Libovolný netriviální podpřímo nerozložitelný svaz je izomorfní  .

Důkaz: Svaz  je zřejmě podpřímo nerozložitelný. Jiný dvouprvkový neexistuje. Uvažme tedy $|L| \geq 3$. Existuje $a \in L$, které není ani největší, ani nejmenší. Pro $x, y \in L$ definujme relace ρ, τ

$$x \ \rho \ y \overset{\text{def}}{\iff} x \wedge a = y \wedge a$$
$$z \ \tau \ y \overset{\text{def}}{\iff} x \vee a = y \vee a$$

Jsou to kongruence. Nechť $x, y, z \in L$, $x \ \rho \ y$. Chceme ukázat $(x \wedge z) \ \rho \ (y \wedge z)$ a $(x \vee z) \ \rho \ (y \vee z)$. Víme, že $x \wedge a = y \wedge a$. Tvrzení $x \wedge z \wedge a = y \wedge z \wedge a$ je zřejmé z vlastností svazů. Z distributivity plyne

$$(x \vee z) \wedge a = (x \wedge a) \vee (z \wedge a) = (y \wedge a) \vee (z \wedge a) = (y \vee z) \wedge a$$

Relace ρ je definována pomocí rovnosti, je tedy zřejmě ekvivalencí. Duálně se dokáže, že τ je kongruence.

Zřejmě platí $\rho \cap \tau = \Delta_L$, přitom $\rho, \tau \neq \Delta_L$, protože existují $b < a < c$, odkud $a \ \rho \ c$, $a \ \tau \ b$. Tedy $\mathfrak{L}$ je podpřímo rozložitelný podle věty 4.22, což je spor. □

Důsledek 4.27
Z věty 4.24 a předchozího plyne, že každý netriviální distributivní svaz je izomorfní $\mathfrak{K}$ – podpřímému součinu systému $\prod_{i\in I}$ 

Věta 4.28 (AC)
Libovolný distributivní svaz je izomorfní okruhu množin.

Důkaz: Hledaným izomorfismem je

$$\begin{aligned} u\colon \quad \mathfrak{K} &\to \left(2^I, \cap, \cup\right) \\ (a_i)_{i\in I} &\mapsto \{i \in I \mid a_i = 1\} \end{aligned}$$

Zobrazení u je bijekce díky tomu, že $\mathfrak{K}$ je podpřímý součin, operace $\wedge, \vee$ v $\mathfrak{K}$ odpovídají zřejmě $\cap, \cup$ v 2^I. □

[1] alespoň dvouprvková

Věta 4.29 (AC)
Libovolný Booleův svaz je izomorfní poli množin.

Důkaz: Nechť $(a_i)_{i\in I}$ je nejmenší prvek $\mathfrak{B}$. Připustme, že existuje $i \in I$ tak, že $a_i = 1$. Potom libovolný prvek v B má na i-té složce 1 – nejedná se o podpřímý součin, což je spor. Tedy $(0)_{i\in I} \in B$, analogicky $(1)_{i\in I} \in B$. □

4.5 Termy a identity

Definice 4.30
Nechť $\tau = (n_\sigma)_{\sigma\in\Sigma}$ je typ, $(f_\sigma)_{\sigma\in\Sigma}$ systém operačních symbolů a M libovolná množina. *Jazykem* $\mathfrak{L}$ rozumíme $\left(\tau, (f_\sigma)_{\sigma\in\Sigma}\right)$. Induktivně definujeme množinu $F_{\mathfrak{L}}(M)$

1. $M \subseteq F_{\mathfrak{L}}(M)$
2. Pro $\sigma \in \Sigma,\ w_1, \dots, w_{n_\sigma} \in F_{\mathfrak{L}}(M)$ je $f_\sigma(w_1, \dots, w_{n_\sigma}) \in F_{\mathfrak{L}}(M)$
3. Do $F_{\mathfrak{L}}(M)$ patří právě to, co vzniklo v konečném počtu kroků z 1. a 2.

Prvky $F_{\mathfrak{L}}(M)$ nazýváme *slova nad* M. Definujme dále

$$f_\sigma^{\mathfrak{F}_{\mathfrak{L}}(M)}(w_1, \dots, w_{n_\sigma}) := f_\sigma(w_1, \dots, w_{n_\sigma})$$

Algebru

$$\mathfrak{F}_{\mathfrak{L}}(M) = \left(F_{\mathfrak{L}}(M), \left(f_\sigma^{\mathfrak{F}_{\mathfrak{L}}(M)}\right)_{\sigma\in\Sigma}\right)$$

nazýváme *algebrou* $\mathfrak{L}$*-slov,* resp *absolutně volnou* τ*-algebrou.*
Uvažme dále $X = \{x_1, x_2, \dots\}$ množinu tzv. *proměnných.* Prvky $F_{\mathfrak{L}}(X)$ nazýváme *termy* jazyka $\mathfrak{L}$, prvky $F_{\mathfrak{L}}(\{x_1, \dots, x_n\})$ *n-árními termy.*

Uvažme například jazyk 1-unárních algeber s přílušným fukčním symbolem f. Potom n-ární termy budou jednak $x_1, \dots, x_n$ podle 1. a obecně $f_m(x_i)$ pro $m \in \mathbf{N}$ a $i \in \{1, \dots, n\}$ podle 2.

Definice 4.31
Nechť A je množina. Definujme $e_i^{A,n}(a_1, \dots, a_n) := a_i$ pro libvolná $n \in \mathbf{N}$, $a_1, \dots, a_n \in A$ a $i \in \{1, \dots, n\}$ jako *i-tou n-ární projekci* na množinu A.

Definice 4.32
Nechť $f \in A^{A^m}$; $g_1, \dots, g_m \in A^{A^n}$. Definujeme n-ární operaci, tzv. *kompozici* $f(g_1, \dots, g_m) \in A^{A^n}$ takto

$$\left(f(g_1, \dots, g_m)\right)(a_1, \dots, a_n) := f\left(g_1(a_1, \dots, a_n), \dots, g_m(a_1, \dots, a_n)\right)$$

Definice 4.33
Nechť $\mathfrak{A} = \left(A, (f_\sigma^{\mathfrak{A}})_{\sigma\in\Sigma}\right)$ je τ-algebra, $p \in F_{\mathfrak{L}}(\mathbf{N}_n)$. Definujeme $p^{\mathfrak{A},n} \in A^{A^n}$ *polynom na* $\mathfrak{A}$ *indukovaný termem* p jako

$$p^{\mathfrak{A},n} := \begin{cases} e_i^{\mathfrak{A},n} & p = x_i \\ f_\sigma^{\mathfrak{A}}\left(q_1^{\mathfrak{A},n}, \dots, q_{n_\sigma}^{\mathfrak{A},n}\right) & p = f_\sigma(q_1, \dots, q_{n_\sigma}) \end{cases}$$

Definice 4.34

Uspořádanou dvojici termů (p, q) z $F_{\mathfrak{L}}(n)$ nazveme *identitou* (píšeme $p \doteq q$). Řekneme, že algebra $\mathfrak{A}$ splňuje identitu $p \doteq q$ (píšeme $\mathfrak{A} \models p \doteq q$), platí-li $p^{\mathfrak{A},n} = q^{\mathfrak{A},n}$.

Důkaz korektnosti se vede indukcí, znamená ukázat, že pro $m \geq n$ platí $p^{\mathfrak{A},m}(a_1, \ldots, a_m) = p^{\mathfrak{A},n}(a_1, \ldots, a_n)$.

Definice 4.35

Identitu tvaru $f^k(x_i) \doteq f^{k+d}(x^j)$ nazýváme *regulární,* pokud $i = j$.

Definice 4.36

Nechť Π je množina identit. Třídu všech τ-algeber splňujících všechny identity z Π označíme $Mod\,\Pi$. *Varieta* τ-algeber říkáme třídě tvaru $Mod\,\Pi$ pro nějaké Π.

Například

$$Mod\left\{f^{k_i}(x) \doteq f^{k_i+d_i}(x) \mid i \in I\right\} = Mod\left\{f^k(x) \doteq f^{k+d}(x) \mid i \in I\right\}$$

nebo

$$Mod\left\{f^{k_i}(x) \doteq f^{k_i}(y) \mid i \in I\right\} = Mod\left\{f^k(x) \doteq f^k(y) \mid i \in I\right\}$$

kde $k := \min\{k_i \mid i \in I\}$ a $d := GCD\{d_i \mid i \in I\}$.

5 Volné algebry

Tato kapitola je asi to nejzajímavější, co v algebře vůbec bylo. Bohužel nestíhám, ke státnícím to potřeba není, takže to snad doplním v červnu.