1 Uspořádané struktury

1.1 Úvod

Slovo “uspořádání"se v přirozeném jazyce používá pro několik různých věcí. *Teorie uspořádých množin* je matematická oblast spadající do algebry, která zavádí *matematický pojem* “uspořádání na množině". Tento pojem, neformálně řečeno, není v podstatě nic jiného, než že se pro každé dva prvky $a, b \in M$ dané množiny M rozhodneme, že buď a je v nějákem smyslu menší než b, nebo b je menší než a, a nebo jsou prvky a a b neporovnatelné.

Jako příklad si představme třeba množinu lidí, které uspořádáme podle jejich velikosti. V tomto případě bude pro káždé dva prvky (lidi) platit, že buď člověk a je menší než člověk b, a nebo člověk b je menší než člověk a. To je příkladem situace, které se říká lineární uspořádaní. Nezajímá nás při tom *o kolik* je kdo větší, zajímá nás pouze kdo je větší než kdo.

Jako druhý příklad, vezměme množinu M jejíž prvky budou členové vybrané rodiny. Tuto množinu můžeme uspořádat pomocí vztahu “je rodič". U tohoto uspořádání se nám může vyskytnout i třetí situace, ve které jsou dva prvky neporovnatelné, např. u dvou sourozenců. U tohoto příkladu lze navíc uspořádání i názorně namalovat pomocí známého rodinného (genealogického) stromu. Podobné znázornění lze obecně provést u každé uspořádané množiny, v matematice se toto znázornění nazývá tzv. Hasseův diagram. Někteří z čtenářů se s daným příkladem možná již setkali v jiném kontextu a to jako příklad matematického pojmu “stromu"(s vyloučením situace, kdy jsou předkové příbuzní). Tento pojem spádá do tzv. teorie grafů. Na uspořádané množiny se lze dívat i jako na grafy, tento pohled však není příliš přínosný. Grafy obecně nesou více informace, jmenovitě informaci vzdálenosti dvou prvků. To určitým způsobem omezuje možnosti pro jejich zkoumání, resp. používají se k řešení jiného typu úloh, u kterých tato informace hraje roli. Tam kde ne, teorie uspořádání poskytuje výrazně výhodnější algebraické nástroje.

1.2 Základní pojmy

Otázkou je, jakým způsobem lze intuitivní představu pojmu “menší nebo rovno"takového, který umožňuje i neporovnatelné prvky co nejjednodušeji matematicky zachytit. Mějme množinu M. Můžeme vytvořit novou množinu R, která bude obsahovat vybrané dvojce $[a, b]$ prvků $a, b \in M$. Přičemž

$[a, b] \in R$ bude intuitivně znamenat, že a je menší nebo rovno než b. Množina všech dvojic prvků z M u kterých záleží na pořadí se označuje $M \times M$ (tzv. Kartézský součin). Takže, množinu R můžeme formálně zadat jako podmnožinu $M \times M$, tedy jako $R \subseteq M \times M$. Taková množina R se nazývá *relace na množině* M.

Příklad 1.1. Zvolme množinu M jako tříprvkovou množinu $M = \{a, b, c\}$. Potom

$$M \times M = \{[a, a], [b, b], [c, c], [a, b], [b, a], [a, c], [c, b], [b, c], [c, b]\}.$$

Relace na M je libovolná podmnožina v $M \times M$, například

$$R_1 = \{[a, a], [b, b], [c, c], [a, b]\}.$$

Zdůrazněme, že R_1 je pouze příkladem jedné z relací na M. Relací na M existuje tolik kolik existuje různých podmnožin $M \times M$.

Pro zachycení intuitivního pojmu “menší nebo rovno"je však pojem relace příliš obecný. Respektive, má smyl brát v úvahu jen některé relace. Prvně, budeme požadovat, aby pro každé $a \in M$ platilo, že a je větší nebo rovno než a, tj. $[a, a] \in R$ pro všechna $a \in M$. Tato vlastnost se nazývá *reflexivita*. Tedy, relace R se nazývá *reflexivní relace* pokud pro všechna $a \in M$ platí $[a, a] \in R$.

Druhá vlastnost, kterou budeme po relaci R požadovat je, aby platilo, že pokud a je menší nebo rovno než b a zároveň b je menší nebo rovno než a, potom $a = b$. Taková vlastnost se nazývá *symetrie*. Tedy, relace $R \subseteq M \times M$ na množině M se nazývá *symetrická relace*, pokud pro všechna $a, b \in M$ taková, že $[a, b] \in R$ a zároveň $[b, a] \in R$ platí, že $a = b$.

Třetí vlastnost, které se říká *tranzitivita* nám zachycuje představu, že pokud a je menší nebo rovno než b a b je menší nebo rovno než c, potom a je menší nebo rovno než c. Tedy, relace $R \subseteq M \times M$ na množině M se nazývá *tranzitivní relace*, pokud pro všechna $a, b, c \in M$ taková, že $[a, b] \in R$ a $[b, c] \in R$ platí, že $[a, c] \in R$.

Libovolná relace $R \subseteq M \times M$ na množině M taková, která je reflexivní, symetrická a tranzitivní se nazáývá *relace uspořádání*.

Příklad 1.2. Mějme pětiprvkovou množinu $M = \{a, b, c, d, e\}$. Rozhodněte, zda jsou nasledující relace uspořádání.

- $R_1 = \{[a, a], [b, b], [c, c], [e, e], [a, b]\}$,

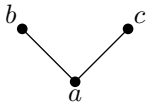
- $R_2 = \{[a,a],[b,b],[c,c],[d,d],[e,e],[c,d],[d,c]\}$,
- $R_3 = \{[a,a],[b,b],[c,c],[d,d],[e,e],[c,d],[d,e]\}$,
- $R_4 = \{[a,a],[b,b],[c,c],[d,d],[e,e]\}$,
- $R_5 = \{[a,a],[b,b],[c,c],[d,d],[e,e],[b,c],[c,d],[b,d]\}$,
- $R_6 = M \times M$.

Řešení 1. Relace R_1 není uspořádání, jelikož není reflexivní (chybí v ní prvek $[d,d]$). Relace R_2 je reflexivní i tranzitivní, ale není symetrická (obsahuje prvky $[c,d]$ a $[d,c]$, přičemž $c \neq d$), tedy není uspořádáním. Relace R_3 je reflexivní, symetrická, ale není tranzitivní (obsahuje $[c,d]$ a $[d,e]$, ale neobsahuje $[c,e]$), takže není uspořádání. Relace R_4 je reflexivní, symetrická i tranzitivní, tudíž to je relace uspořádání. Stejně tak R_5 i R_6.

V teorii uspořádání je běžné, že se relace uspořádání značí symbolem $\leq$ namísto R, tj. $\leq \subseteq M \times M$. Pro prvky $a, b \in M$ namísto $[a,b] \in \leq$ pak píšeme $a \leq b$. Množina M spolu s relací uspořádání $\leq$ na množině M se nazývá *uspořádáná množina* a značí se $(M, \leq)$ (místo slov "relace uspořádání"budeme říkat krátce "uspořádání", resp. "uspořádání na množině M").

Pro grafické znázornění uspořádané množiny $(M, \leq)$ se používá takzvaný *Hasseův diagram* uspořádané množiny $(M, \leq)$. Jde o obrázek obsahující všechny prvky množiny M namalovaný tak, že pokud $a \leq b$, potom b je nakresleno výše než a a jsou spojeny čarou.

Příklad 1.3. Nechť M je tříprvková množina $M = \{a, b, c\}$ a uspořádání $\leq$ je zadáno pomocí $a \leq b$, $a \leq c$ (jinak řečeno $\leq = \{[a,a],[b,b],[c,c],[a,b],[a,c]\}$). Potom Hasseův diagram uspořádané množiny $(M, \leq)$ je



V případě, že $a \leq b$ a $b \leq c$, potom z vlastnosti tranzitivity víme, že i $a \leq c$. Obrázek pak namalujeme následovně, prvek a s prvkem c již nespojujeme, jelikož a je spojen s b a b je již spojeno s c, takže z tranzitivity víme, že i $a \leq c$.

Tento příklad taktéž ilustruje, jak budeme uspořádané množiny zadávat. Vzali jsme v něm nejmenší uspořádání na množině $M = \{a, b, c\}$ ve kterém $a \leq b$ a $b \leq c$. Není potřeba vypisovat, že $a \leq c$, jelikož to plyne z tranzitivity a není potřeba vypisovat $a \leq a$, $b \leq b$, $c \leq c$, jelikož to plyne z reflexivity. Tímto způsobem budem uspořádané množiny zadávat i nadále, bude to vždy nejmenší uspořádání, které splňuje zadné podmínky.

Příklad 1.4. Popište celou relaci a namalujte Hasseovy diagramy následujících uspořádání $(M, \leq_1), (M, \leq_2), (M, \leq_3)$ a $(M, \leq_4)$ na množině $M = \{a, b, c, d\}$.

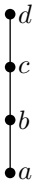
1. $a \leq_1 b$, $b \leq_1 c$, $c \leq_1 d$.
2. $b \leq_2 c$.
3. $a \leq_3 c$, $a \leq_3 d$, $b \leq_3 c$, $b \leq_3 d$.
4. $a \leq_4 b$, $b \leq_4 c$, $a \leq_4 d$, $d \leq_4 c$.

Řešení 2. První relaci uspořádání $\leq_1$ lze explicitně rozepsat jako

$$\leq_1 = \{[a, a], [b, b], [c, c], [d, d], [a, b], [a, c], [a, d][b, c], [b, d], [c, d]\}.$$

Její Hasseův diagram je:

Obrázek 1: $(M, \leq_1)$



Druhou relaci uspořádání $\leq_2$ lze explicitně rozepsat jako

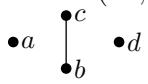
$$\leq_2 = \{[a, a], [b, b], [c, c], [d, d], [b, c]\}.$$

Její Hasseův diagram je:

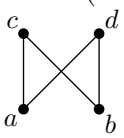
Třetí relaci uspořádání $\leq_3$ lze rozepsat jako

$$\leq_3 = \{[a, a], [b, b], [c, c], [d, d], [a, c], [a, d], [b, c], [b, d]\}.$$

Obrázek 2: $(M, \leq_2)$



Obrázek 3: $(M, \leq_3)$



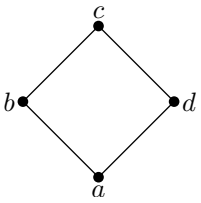
Její Hasseův diagram je:

Čtvrtou relaci uspořádání $\leq_4$ lze rozepsat jako

$$\leq_4 = \{[a,a],[b,b],[c,c],[d,d],[a,b],[a,c],[b,c],[a,d],[d,c]\}.$$

Její Hasseův diagram je:

Obrázek 4: $(M, \leq_4)$



Uspořádaná množina $(M, \leq)$ se nazývá *lineárně uspořádaná množina* pokud pro každé dva prvky $a, b \in M$ platí $a \leq b$, nebo $b \leq a$. Tedy, libovolné dva prvky jsou porovnatelné. Hasseův diagram lineárně uspořádané množiny je vždy svislá čára. Příkladem jsou třeba přirozené $(\mathbb{N}, \leq)$, celé $(\mathbb{Z}, \leq)$, racionální $(\mathbb{Q}, \leq)$, či reálné čísla $(\mathbb{R}, \leq)$ uspořádané podle velikosti.

Poznámka 1.5. Jelikož je podstatně jednodušší dohledávat informace v angličtině, zmiňme se o anglické terminologii (pokud ji čtenář momentálně nepotřebuje, může poznámku přeskočit). Překlad termínu “relace na množině"je bezproblémový, tj. “a relation on a set". Komplikace nastává u pojmu “uspořádáná množina". Přímý překlad “an ordered set"znamená v různých anglických textech různé věci. Někdy se používá pro “uspořádáná množina",

někdy pro “lineárně uspořádaná množina". V angličtině se proto pojmu “an ordered set"vyhýbají a pro uspořádánou množinu standardně používájí “a partially ordered set"(doslovně přeloženo “částečně uspořádaná množina") a pro lineárně uspořádánou “a lineary ordered set".

1.3 Význačné prvky

Mějme zadanou uspořádanou množinu $(M, \leq)$. Zvolme podmožinu $N \subseteq M$ množiny M. Řekneme, že $a \in N$ je *nejmenší prvek* podmnožiny N pokud pro všechna $x \in N$ platí, že $a \leq x$. Podobně, řekneme, že $b \in N$ je *největší prvek* podmnožiny N pokud pro všechna $x \in N$ platí, že $x \leq b$. Pro zadanou podmnožinu N obecně největší (resp. nejmenší) prvek nemusí existovat (vezměmě třeba relaci R_4 a $N = M$ v příkladu 1.2). Pokud ale existuje, je vždy jedinný.

Podobný, nicméně odlišný je pojem minimálního, resp. maximálního prvku podmnožiny N. Zatím co nejmenší prvek $a \in N$ podmnožiny N popisoval vlastnost “a z podmnožiny N je menší než všichni ostatní z N", pojem minimálního prvku $m \in N$ popisuje situaci, kdy “v N není žádný menší prvek než $m \in N$". Pokud je uspořádání na M lineární, tj. všechny prvky jsou porovnatelné, pak pojem nejmenšího a minimálního prvku splývají. Pokud jsou v M i vzájemně neporovnatelné prvky, pak se tyto pojmy mohou lišit, viz příklad 1.4, relace $(M, \leq_3)$, kde $a, b \in M$ jsou minimální prvky množiny M, ale ani jeden z nich není nejmenší. Podobný, nicméně odlišný je pojem minimálního, resp. maximálního prvku podmnožiny N. Zatím co nejmenší prvek $a \in N$ podmnožiny N popisoval vlastnost “a z podmnožiny N je menší než všichni ostatní z N", pojem minimálního prvku $m \in N$ popisuje situaci, kdy “v N není žádný menší prvek než $m \in N$". Pokud je uspořádání na M lineární, tj. všechny prvky jsou porovnatelné, pak pojem nejmenšího a minimálního prvku splývají. Pokud jsou v M i vzájemně neporovnatelné prvky, pak se tyto pojmy mohou lišit, viz příklad 1.4, relace $(M, \leq_3)$, kde $a, b \in M$ jsou minimální prvky množiny M, ale ani jeden z nich není nejmenší. Formálně řečeno, prvek $m \in N$ se nazývá *minimální* v podmožině N pokud pro libovolné $x \in N$ takové, že $x \leq m$ platí, že $x = m$. Podobně, prvek $n \in N$ se nazývá *maximální* v podmnožině N pokud pro libovolné $x \in N$ takové, že $n \leq x$ platí, že $x = n$.

Do třetice, řekneme, že $k \in M$ se nazývá *dolní závora* podmnožiny N pokud pro všechna $x \in N$ platí, že $k \leq x$. Pojem dolní závory se od pojmu nejmenšího prvku liší v tom, že k nemusí ležet v podmnožině N, ale v množině M. Dolní závory pro zadanou podmnožinu N nemusí existovat, ale narozdíl od

nejmenších prvků jich pro N může existovat více. Podobně, $l \in M$ se nazývá *horní závora* podmnožiny N pokud pro všechna $x \in N$ platí, že $x \leq l$.

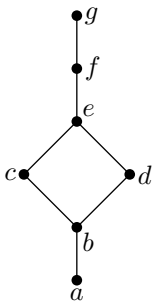
1.4 Svazy

V následující podkapitole probereme klíčový matematický pojem, a to pojem svazu.

Uvažujme uspořádanou množinu $(M, \leq)$ a nějakou její podmnožinu $N \subseteq M$. Prvek $a \in M$ se nazývá *infimum* množiny N pokud je a největším prvkem v množině dolních závor podmnožiny N. Infimum množiny N značíme jej $\bigwedge N$. Analogicky, prvek $b \in M$ se nazývá *supremum* množiny N, pokud je b nejmenší dolní závora množiny N, značíme $\bigvee N$. Pojem infima i suprema podmnožiny N je velmi intuitivní, jedná se o největší prvek, který je pod všemi prvky z N, resp. nejmenší prvek, který je nad všemi prvky podmnožiny N.

Příklad 1.6. Nechť $(M, \leq)$ je svaz na sedmiprvkové množině $M = \{a, b, c, d, e, f, g\}$ s uspořádáním $a \leq b$, $b \leq c$, $b \leq d$, $c \leq e$, $d \leq e$, $e \leq f$, $f \leq h$,tj. s Hasseovým diagramem

Obrázek 5: $(M, \leq)$



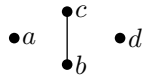
Vezměme podmnožinu $N_1 = \{a, b\}$. Její horní závory jsou prvky b, c, d, e, f, g. Nejmenší z těchto prvků je b, tedy supremum podmnožiny N_1 je b, značíme $\bigvee N_1 = b$. Dolní závory N_1 jsou pouze a, tedy infimum $\bigwedge N_1 = a$.

Vezměme podmnožinu $N_2 = \{c, d\}$. Horní závory N_2 jsou e, f, g, nejmenší z nich je e, tedy $\bigvee N_2 = e$. Dolní závory N_2 jsou a, b přičemž největší z nich je b, tedy $\bigwedge N_2 = b$.

Infimum podmnožiny N v obecném případě nemusí existovat. Důvody mnohou být dva. Pro zvolenou podmnožinu N se může stát, že množina dol-

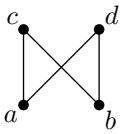
ních závor je prázdná, viz podmnožina $N_1 = \{a, b\}$ v uspořádané množině $(M_1, \leq_1)$ zadané diagramem

Obrázek 6: $(M_1, \leq_1)$



Druhý případ, kdy infimum neexistuje je, pokud množina dolních závor je sice neprázdná, nicméně nemá největší prvek, vezměme podmnožinu $N_2 = \{c, d\}$ v $(M_2, \leq_2)$ zadané diagramem

Obrázek 7: $(M_2, \leq_2)$



Uspořádaná množina $(M, \leq)$ se nazývá *svaz*, pokud pro libovolnou **konečnou** podmnožinu N existuje suprémum i infimum. Svazy jsou klíčové matematické objekty a vyskytují se ve všech oblastech matematiky. Teorie svazů je jednou ze základních částí moderní algebry.

Příklad 1.7. Příklady svazů:

(i) $(M, \leq_1)$ a $(M, \leq_4)$ z příkladu 1.2,

(ii) $(M, \leq)$ z příkladu 1.4,

(iii) přirozená čísla $\mathbb{N}$ spolu s obvyklým uspořádáním podle velikosti $\leq$, tj. $(\mathbb{N}, \leq)$,

(iv) podobně celá, racionální, reálná čísla s obvyklým uspořádáním, tj. $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$ a $(\mathbb{R}, \leq)$.

Příklad 1.8.

Věta 1.9. *Nechť $(M, \leq)$ je uspořádaná množina ve které pro libovolné $a, b \in M$ existuje $\bigwedge\{a, b\}$ i $\bigvee\{a, b\}$ (tj. pro libovolou dvouprvkovou podmnožinu existuje infimum a supremum). Potom $(M, \leq)$ je svaz.*

Důkaz. Pro ověření definice svazu je potřeba ukázat, že z existence suprema a infima dvouprvkových podmnožin množiny M už nutně plyne i existence suprema a infima všech konečných podmnožin množiny M.

Předpokládejme tedy, že existují infima a suprema všech dvouprkových podmnožin. Vezměme libovolnou konečnou podmnožinu $N \subseteq M$ množiny M a zkusíme ukázat, že existuje její suprémum. Jelikož je N konečná, můžeme si její prvky označit pomocí $a_1, a_2, dots, a_n$ pro nějaké $n \in \mathbb{N}$ tj. $N = \{a_1, dots, a_n\}$. Jelikož předpokládáme, že existují suprema dvouprvkových podmnožin, víme, že existuje prvek $\bigvee\{a_1, a_2\}$. Stejně tak existuje prvek $\bigvee\{\bigvee\{a_1, a_2\}, a_3\}$. Takto můžeme postupně přidat všechny prvky N, tj. existuje prvek $a = \bigvee\{\bigvee\{\cdots\bigvee\{\bigvee\{a_1, a_2\}, a_3\}\ldots, a_{n-1}\}, a_n\}$.

Jelikož je a supremum a tedy horní závora prvků a_n a $\bigvee\{\cdots\bigvee\{\bigvee\{a_1, a_2\}, a_3\}\ldots, a_{n-1}\}$, víme, že $a_n \leq a$ a $\bigvee\{\cdots\bigvee\{\bigvee\{a_1, a_2\}, a_3\}\ldots, a_{n-1}\} \leq a$. Podobně, z definice $a_{n-1} \leq \bigvee\{\cdots\bigvee\{\bigvee\{a_1, a_2\}, a_3\}\ldots, a_{n-1}\}$. Složením s předchozí nerovností a použitím tranzitivity získáme $a_{n-1} \leq a$. Opakováním úvahy dostaneme, že $a_i \leq a$ pro libovolný index $i \in 1, \ldots, n$. Tedy a je horní závorou podmnožiny N.

Abysme ukázali, že a supremum, tj. nejmenší horní závora, je potřeba ukázat, že pro libovolnou jinou horní závoru $b \in M$ podmnožiny N platí $a \leq b$. Předpokládejme tedy, že b je horní závora podmnožiny N. Potom z definice b je i horní závorou podmnožiny $a_1, a_2 \subseteq N$, tj. $(a_1 \vee a_2) \leq b$. Jelikož $a_3 \leq b$, potom i $(a_1 \vee a_2) \vee a_3 \leq b$. Tímto způsobem můžeme postupovat dále a dostaneme, že $(\ldots((a_1 \vee a_2) \vee a_3) \vee a_4)\cdots \vee a_{n-1}) \vee a_n) \leq b$. To ale není nic jiného, než že $a \leq b$.

Existence infim se ukáže analogicky. □

Předcházející věta nám říká, že pro ověření zda-li je uspořádaná množina $(M, \leq)$ svaz stačí ověřit, že existují suprema a infima dvouprvkových podmnožin.

Pro označení infima (suprema) dvouprvkové podmnožiny $\{a, b\} \subseteq M$, $a, b \in M$ budeme namísto symbolu $\bigwedge\{a, b\}$ ($\bigvee\{a, b\}$) používat symbol $a \wedge b$ ($a \vee b$), tedy $a \wedge b = \bigwedge\{a, b\}$ ($a \vee b = \bigvee\{a, b\}$).

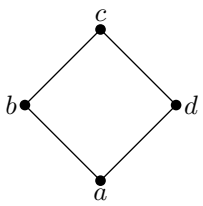
V tento okamžik čtenáři doporučuje připomenutí si základních definic z algebry resp. definici grupy, se kterou bude následující úzce souviset. Připomeňme, že *operace $*$ na množině M* je definována jako zobrazení $* : M \times M \to M$. Tedy, jedná se o předpis, který dvoum prvkům přiřadí třetí. Jako příklad můžeme za množinu M vzít přirozená čísla, tj. $M = \mathbb{N}$, s operací

sčítání, tedy $* = +$.

Vezměme nyní libovolný svaz $(M, \leq)$. Pro libovolné dva prvky $a, b \in M$ jsme schopni z definice svazu najít $a \vee b$, tj. dvěma prvkům a, b přiřadíme třetí $a \vee b$. Tedy, $\vee$ nám zadává operaci na množině M. Stejně tak nám $\wedge$ zadává operaci na množině.

Příklad 1.10. Mějme svaz $(M, \leq)$, zadaný pomocí $M = \{a, b, c, d\}$ jako $a \leq b$, $b \leq c$, $a \leq d$, $d \leq c$.

Obrázek 8: $(M, \leq_4)$



Sestrojme nyní, stejně jako se to dělalo u grup, tabulky operací $\vee$ a $\wedge$. Výsledek operace lze vyčíst z tabulky na příslušné pozici, např. $b \vee d = c$.

$\vee$	a	b	c	d
a	a	b	c	d
b	b	b	c	c
c	c	c	c	c
d	d	c	c	d

$\wedge$	a	b	c	d
a	a	a	a	a
b	a	b	b	a
c	a	b	c	d
d	a	a	d	d

K tabulkám operací z předchozího příkladu se vrátíme později, nyní mějme jen na paměti, že na $\vee$ a $\wedge$ lze pohlížet jako na operace. Stejně jaku grup se lze bavit o vlastnostech těchto operací $\vee$ a $\wedge$. Ideálně, zkusíme najít takové, které budou pro $\vee$ a $\wedge$ platit v libovolném svazu $(M, \leq)$. První taková důležitá vlastnost je komutativita. Symbolem $*$ nyní budeme značit libovolnou operaci na množině M. Operace $* : M \times M \to M$ na množině M se nazývá *komutativní* pokud pro všechna $a, b \in M$ platí

$$a * b = b * a.$$

Druhá důležitá vlastnost operace je, zda-li, pokud operaci provedeme s více prvky po sobě, záleží na pořadí. Jinak řečeno zda nám záleží na uzávorkování. Formálně zapsáno, zda pro libovolné $a, b, c \in M$ platí

$$(a * b) * c = a * (b * c).$$

Pokud je to splněno, říkáme, že operace $*$ je *asociativitivní*. Pro jednoduchou představu operace, která je komutativní a asociativní si lze představit přirozené čísla $\mathbb{N}$ s operací sčítání, tj. $(\mathbb{N}, +)$. Případně přirozená čísla s násobením $(\mathbb{N}, \cdot)$.

Další vlastnosti se říká *idempotence*. Operace $*$ na množině M se nazývá *idempotentní* pokud pro všechna $a \in M$ platí

$$a * a = a.$$

Přirozená čísla se sčítáním $(\mathbb{N}, +)$ ani s násobením $(\mathbb{N}, \cdot)$ již idempotetní nejsou. $(\mathbb{N}, \cdot)$ má jedný idempotetní prvek a to 1, jelikož $1 \cdot 1 = 1$.

Věta 1.11. *Nechť $(M, \leq)$ je svaz. Potom pro libovolné $a, b \in M$ platí*

$$a \vee b = b \vee a,$$

$$a \wedge b = b \wedge a.$$

Tedy, operace $\vee$ a $\wedge$ jsou komutativní.

Důkaz. □

Věta 1.12. *Nechť $(M, \leq)$ je svaz. Potom pro libovolné $a, b, c \in M$ platí*

$$(a \vee b) \vee c = a \vee (b \vee c),$$

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

Tedy, operace $\vee$ a $\wedge$ jsou asociativní.

Důkaz. □

Tedy, pro libovolný svaz $(M, \leq)$, $(M, \vee)$ a $(M, \wedge)$ jsou komutativní pologrupy.

Věta 1.13. *Nechť $(M, \leq)$ je svaz. Potom pro libovolné $a \in M$ platí*

$$a \vee a = a,$$

$$a \wedge a = a.$$

Tedy, operace $\vee$ a $\wedge$ jsou idempotetní.

Důkaz. □

Poslední vlastnost se váže k takové množině M, na ktere jsou definované dvě operace, označme si je $*$ a $\circ$. Řekneme, že na M platí *absorbční zákony* pokud pro libovolné $a, b \in M$ platí

$$a * (a \circ b) = a,$$

$$a \circ (a * b) = a.$$

Absorbční zákony již nejsou jednoduše představitelné tak, jako vlastnosti předchozí, což momentálně nevadí. Důležité je si uvědomit, že nám říkají, že zmíněné dvě operace $*$ a $\circ$ jsou nějakým způsobem provázány, jsou na sobě závislé. Pokud zvolíme jednu $*$, potom $\circ$ nelze zvolit libovolně, ale musí nějak s $*$ "spolupracovat".

Věta 1.14. *Nechť $(M, \leq)$ je svaz. Potom pro libovolné $a, b \in M$ platí*

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

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

Tedy, pro operace $\vee$ a $\wedge$ platí absorbční zákony.

Důkaz. □

Tedy, shrneme-li předcházející sérii tvrzení, v kazdém svazu $(M, \leq)$ platí pro operaci $\vee$ a $\wedge$ komutativita, asociativita, idempotence a absorbční zákony.

Vraťme se nyní k příkladu 1.10. Tam jsme ze znalostí uspořádání $\leq$ na svazu $(M, \leq)$ odvodili výsledky operací $\vee$ a $\wedge$, a byli schopni napsat jejich tabulky. Nabízí se otázka, pokud by nám někdo zadal pouze množinu M a dvě uvedené

tabulky operací $\vee$ a $\wedge$, ovšem neřekl nám nic o tom, jak vypadá uspořádání $\leq$, jestli ze zmíněných tabulek operací můžeme jednoznačně uspořádání $\leq$ odvodit. Odpověď zní - ano. K tomu, jak to provést nám pomůže následující věta.

Věta 1.15. *Nechť $(M, \leq)$ je svaz. Pro libovolné $a, b \in M$ platí*

$$a \leq b \text{ právě tehdy když } a \vee b = b$$

a

$$a \leq b \text{ právě tehdy když } a \wedge b = a.$$

Důkaz. □

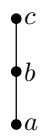
Příklad 1.16. Mějme tříprvkovou množinu $M = \{a, b, c\}$. Mějme zadné tabulky operací $\vee$ a $\wedge$ jako

$\vee$	a	b	c
a	a	b	c
b	b	b	c
c	c	c	c

$\wedge$	a	b	c
a	a	a	a
b	a	b	b
c	a	b	c

Odvoďte uspořádání $\leq$ na M a namalujte Hasseův diagram.

Řešení 3. Pomocí věty 1.15 zjistíme z $a \vee b = b$, že $a \leq b$. Podobně, z $b \vee c = c$, že $b \leq c$. Což nám stačí, jelikož uspořádání již nemůže vypadat jinak než:



Přejděme nyní k další úvaze. V předchozím příkladě se nám pomocí věty 1.15 podařilo zjistit uspořádání $\leq$ na množině M z tabulky operací $\vee$ a $\wedge$. Tedy, známe-li operace $\vee$ a $\wedge$ na konkrétním svazu $(M, \leq)$, jednoznačně z nich odvodíme uspořádání $\leq$. Nicméně, u tabulek v předchozím příkladě nám bylo dopředu řečeno, že jde o tabulky svazových operací $\vee$ a $\wedge$. Otázka zní, jestli je možné svazové uspořádání tímto způsobem odvodit z jakýchkoliv dvou zadaných tabulek, tj. z libovolných dvou zadaných operací na množině M. Není těžké ukázat, že to nelze. Stačí si vzít dvouprvkovou množinu $M = \{a, b\}$ s tabulkou operace

$\vee$	a	b
a	a	a
b	a	a

Problém zde je, že $b \vee b = a$, což není možné, protože podle věty 1.13 operace suprema $\vee$ ve svazu M musí být idempotentní, tedy musí platit $b \vee b = b$. Svaz s výše zmíněnou tabulkou operace suprema tedy neexistuje. Naši otázku tedy modifikujeme a zeptáme se, jestli pro zadanou množinu M a dvojci operací $*$ a $\circ$ na M neexistují nějaké vlastnosti těchto operací které nám zajistí, že bude existovat svaz $(M, \leq)$ takový, že $* = \vee$ a $\circ = \wedge$. Na tuto otázku odpoví následující věta.

Věta 1.17. *Nechť M je množina a $*$ a $\circ$ operace na M. Pokud jsou obě tyto operace komutativní, asociativní, idempotentní a splňují absorbční zákony, potom existuje jednoznačně určený svaz $(M, \leq)$ takový, že $* = \vee$ a $\circ = \wedge$.*

Důkaz. □

Spolu s poznámkou za větou 1.14 dostáváme, že dvě operace $*$ a $\circ$ na množině M jednoznačně zadávají svaz pomocí $* = \vee$ a $\circ = \wedge$ právě tehdy když jsou komutativní, asociativní, idempotetní a splňují absorbční zákony.

Tento poznatek je důležitý, protože nám umožňuje svaz zadefinovat jiným způsobem. Konkrétně, svaz lze definovat jako množinu M se dvěma operacemi $\vee$ a $\wedge$, které jsou komutativní, asociativní, idempotentní a splňují absorbční zákony. Tento fakt zdůrazňujeme tím, že svaz zapisujeme jako $(M, \vee, \wedge)$. Pomocí věty 1.17 a věty 1.15 pak z $(M, \vee, \wedge)$ můžeme odvodit svaz jako uspořádanou množinu $(M, \leq)$.

Důvodů proč nás tohle zajímá je vícero. Obě vyjádření svazu $(M, \vee, \wedge)$ a $(M, \leq)$ mají svou užitečnost. Výhodou $(M, \leq)$ je, že skutečne vidíme, jak uspořádání vypadá, např. můžeme nakreslit jeho Hasseuv diagram. Naproti

tomu vyjádření $(M, \vee, \wedge)$ je vhodnější z algebraického hlediska. Moderní algebra se zabývá množinami s operacemi. Pokud čtenář prošel základním kurzem algebry, setkal s grupami - což jsou množiny s operací se specifickými vlastnostmi, jejich homomorfismy, jejich faktorizacemi a podobně. Stejně tak v předmětu pracujícím s lineární algebrou narazil na vektorové prostory - což jsou opět množiny s operacemi, jejich lineární zobrazení (což je jen jiný název pro homomorfismy), báze, dimenze a podobně. Vyjádření svazu jako množiny s operacemi $(M, \vee, \wedge)$ nám umožňuje tyto pojmy fomulovat i pro svazy, tj. bavit se o homomorfismech svazů, faktorizaci svazů, bazích atd.

2 Podsvazy, homomorfismy

V této krátké kapitole zavedeme dva základní algebraické pojmy týkající se svazů. Prvním bude pojem podsvazu.

Definice 2.1. Podmnožina $N \subseteq M$ svazu $(M, \leq)$ se nazývá *podsvaz* svazu $(M, \leq)$ pokud pro všechna $a, b \in N$ platí $(a \wedge b) \in N$, $(a \vee b) \in N$.

Jinak řečeno, podsvaz N svazu $(M, \leq)$ je podmnožina uzavřená na operace. Čtenáři doporučujeme tuto definici srovnat s definicí podgrupy H grupy $(G, *)$, či podprostoru vektorového prostoru, jelikož jde o úplně stejnou úvahu.

Nechť $(M, \leq)$. Uvažujme libovolné $a, b \in M$. Symbolem $[a, b]$ označíme podmnožinu $[a, b] \subseteq M, [a, b] = \{x \in M \mid a \leq x \leq b\}$. Symbol $[a, b]$ tedy označuje množinu všech prvků ležících mezi prvky a, $b \in M$. Všiměme si, že $[a, b]$ je podsvaz. To není těžké ukázat, zřejmě pro libovolné $x, y \in [a, b]$ dostaneme $(x \vee y) \in [a, b]$ i $(x \wedge y) \in [a, b]$. Takovému podsvazu budeme říkat *intervalový podsvaz* $[a, b]$ svazu $(M, \leq)$.

Druhým důležitým pojmem je izomorfismus dvou svazů.

Definice 2.2. Zobrazení $f : M \to L$ se nazývá izomorfismus ze svazu $(M, \vee_M, \wedge_M)$ do svazu $(L, \vee_L, \wedge_L)$ pokud je f bijekce a zároveň platí

$$f(a \vee_M b) = f(a) \vee_L f(b),$$
$$f(a \wedge_M b) = f(a) \wedge_L f(b).$$

Opět, odkazujeme čtenáře na pojem izomorfismu grup, případně vektorových prostorů, kde jde o analogický pojem bijektivního zobrazení, které zachovává

operace. Pokud bychom vynechali podmínku bijekce, dostaneme homomorfismus svazů, nicméně ten v tomto textu nebudeme potřebovat.

Pokud mezi dvěma svazy existuje $(M, \vee_M, \wedge_M)$ a $(L, \vee_L, \wedge_L)$ existuje izomorfismus $f : M \to L$, znamená to (podobně jako u grup), že jsou tyto svazy "stejné"(z algebraického hlediska), mají stejnou strukturu. Pokud bysme namalovali jejich Hasseovy diagramy, půjde o stejné obrázky.

3 Modulární svazy

Jeden z pohledů na algebraické struktury, tj. množiny s operacemi, je, že vznikly z konkrétních matematických objektů tím, že "zapomeneme"všechny ostaní vlastnosti které nesouvisí s operací na daném objektu. Například, u celých čísel $\mathbb{Z}$ se můžeme bavit o grupě $(\mathbb{Z}, +)$. Samořejmě, konkrétní grupa $(\mathbb{Z}, +)$ má víc vlastností než úplně libolná obecná grupa $(G, *)$. V té máme zajištěnou platnost pouze axiomů grupy. Pointa je, že bysme chtěli nikoliv nejprve zadefinovat $\mathbb{Z}$ a pak z něj abstrahovat grupu $(\mathbb{Z}, +)$, ale naopak vzít si obecnou grupu $(G, *)$ a najít nějakou (algebraickou) vlastnost, která nám zajistí, že $(G, *)$ bude izomorfní (stejná jako) $(\mathbb{Z}, +)$. V tomto konkrétním případě $(\mathbb{Z}, +)$ to lze udělat. Libovolná gurupa $(G, *)$ je izomorfní se $(\mathbb{Z}, +)$ právě tehdy když $(G, *)$ je generovaná jedním prvkem a je nekonečná.

Pro zadanou grupu $(G, *)$ můžeme uvažovat množinu $S(G)$, která obsahuje všechny její normální podgrupy. Tuto množinu můžeme uspořádat množinovou inkluzí $\subseteq$. Není těžké dokázat (viz třeba ...), že $(S(G), \subseteq)$ je svaz. Modulární svazy, o kterých se budeme bavit v této kapitole, vznikly abstrakcí svazu všech normálových podgrup $(S(G), \subseteq)$, resp. obecněji faktoralgeber. Tedy, i poprostory vektorového prostoru, či ideály okruhu uspořádané množinovou inkluzí $\subseteq$ tvoří modulární svaz (pokud čtenář pojmy z tohoto odstavce nezná, tak to ničemu nevadí).

Přejděme nyní k definici modularity. Svaz $(L, \leq)$ se nazývá *modulární svaz* pokud pro libovolné $a, b, c \in L$ takové, že $a \leq b$ platí

$$a \vee (c \wedge b) = (a \vee c) \wedge b.$$

Z této definice samozřejmě není hned viditelné, co by tahle podmínka měla znamenat a proč by svazy, které ji splňují měli někoho zajímat. Než ovšem uvádět příklady svazů které podmínku splňují, pro pochopení jejího vznamu je lepší pokusit se najít nějaký svaz, který ji nesplňuje. Půjdeme postupně od nejmenších svazů, které známe.

0.) Svaz na prázdné množině $(\emptyset, \leq)$ triviálně splňuje vše.

1.) Pro jednoprvkový svaz $(L_1, \leq)$, $L = \{x\}$ není těžké ověřit, že podmínka je splněna, jelikož jediný případ, co může nastat je

$$x \vee (x \wedge x) = x = (x \vee x) \wedge x.$$

2.) Dvouprvkový svaz existuje (až na izomorfismus) pouze jeden, a to $(L_2, \leq)$, kde $L_2 = \{x, y\}$ a $x \leq y$. Dosazováním prvků do definice modularity:

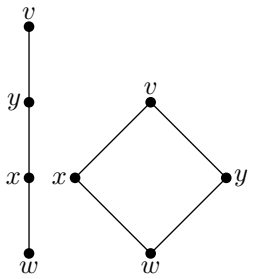
$$\begin{aligned}
x \vee (x \wedge x) &= x = (x \vee x) \wedge x, \\
x \vee (y \wedge x) &= x = (x \vee y) \wedge x, \\
x \vee (x \wedge y) &= x = (x \vee x) \wedge y, \\
x \vee (y \wedge y) &= y = (x \vee y) \wedge y, \\
y \vee (x \wedge y) &= y = (y \vee x) \wedge y, \\
y \vee (y \wedge y) &= y = (y \vee y) \wedge y.
\end{aligned}$$

Tedy $(L_2, \leq)$ je modulární.

3.) Tříprvkový svaz existuje (až na izomorfismus) také pouze jeden, a to $(L_3, \leq)$, kde $L_3 = \{x, y, z\}$ a $x \leq y \leq z$. Zde je pořeba ověřit více kombinací, nicméně prozradíme čtenáři, že i $(L_3, \leq)$ je modulární svaz.

4.) Čtyřprovkové svazy existují dva neizomorfní, jmenovitě $(L_4, \leq_L)$ a $(S_4, \leq_S$).

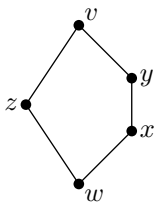
Obrázek 9: $(L_4, \leq_L), (S_4, \leq_S)$



Opět, postupným dosazováním prvků od rovnosti z definice modularity lze dojít k závěru, že oba tyto svazy jsou modulární.

5.) Až pětiprvkové svazy přinesou změnu. Existuje pět neizomorfních pětiprvkových svazů. Jejich nalezení je pro čtenáře jednoduché, ale důležité cvičení. Čtyři z nich opět budou modulární. Zaměřme se nyní na svaz který označíme jako $(M_5, \leq)$. Tento svaz bude definován pomocí $M_5 = \{x, y, z, v, w\}$ a vyztahů $w \leq x \leq y \leq v$ a $w \leq z \leq v$viz obrázek.

Obrázek 10: $(M_5, \leq)$



Postupným dosazováním do rovnosti z definice modularity se dostaneme k případu

$$x \vee (z \wedge y) = x \neq y = (x \vee z) \wedge y,$$

tedy $(M_5, \leq)$ není modulární. Tento svaz je klíčovým příkladem díky následující větě.

Věta 3.1. *Nechť $(L, \leq)$ je svaz. Potom $(L, \leq)$ je modulární právě tehdy když neobsahuje podsvaz izomorfní svazu $(M_5, \leq)$.*

Důkaz. □

Předešlá věta nám dává způsob, jak (z obrázku) rozhodnout, zda zadaný svaz $(L, \leq)$ je či není modulární. Pokud se nám v $(L, \leq)$ podaří najít podsvaz který vypadá jako $(M_5, \leq)$, potom víme, že $(L, \leq)$ není modulární. Pokud se nám to naopak nepodaří, potom $(L, \leq)$ modulární je.

Pro pochopení smyslu modulárních svazů nám poslouží nasledující věta.

Věta 3.2. *Nechť $(L, \leq)$ je svaz. Potom $(L, \leq)$ je modulární právě tehdy když pro každé dva prvky $a, b \in L$ platí, že intervalové podsvazy $[a \wedge b, a]$ a $[b, a \vee b]$ jsou izomorfní.*

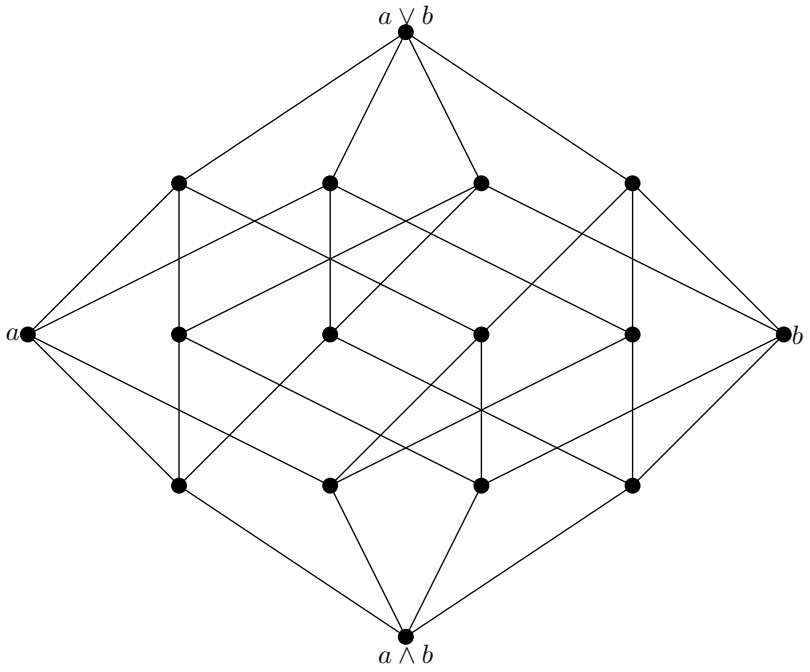
Pro dané prvky $a, b \in L$ je zmíněný izomorfismus $f : [a \wedge b, a] \to [b, a \vee b]$ určen předpisem $f(x) = x \vee b$.

...obrazek (viz `https://en.wikipedia.org/wiki/Modular_lattice#Diamond_isomorphism_theorem` *)*

Důkaz. □

Pro ilustraci významu předchozí věty uvažujme modulární svaz $(L, \leq)$ zadáný následujícím obrázkem

Obrázek 11: $(L, \leq)$



Zvolme si dva prvky, např. $a, b \in L$ vyznačené na obrázku. Z něj pak dobře vydíme, že prvky které se nachází mezi $a \wedge b$ a a (tj. z intervalu $[a \wedge b, a]$) mají stejnou strukturu (zadávají stejný obrázek) jako prvky, které leží mezi b a $a \vee b$.

Čtenář si může vybrat libovolné dva jiné prvky a vyzkoušet si, že tato vlastnost opět bude platit.

Zdůrazněme, že díky slovům "právě tehdy"ve větě 3.2 platí i obrácený směr. Tj. pokud libovolný svaz $(L, \leq)$ splňuje výše popsanou vlastnost pro každé dva své prvky, potom je modulární. Modulární svazy si tedy můžeme představovat jako přesně ty svazy, které mají výše popsanou vlastnost.

4 Distributivní svazy

Další důležitou skupinou svazů jsou takzvané distributivní svazy. Distributivita je vlastnost, se kterou se každý čtenář již setkal již na základní škole a to v pojmu "vytýkání před závorku"při počítání s reálnými čísly. Jinak řečeno, víme, že $(5 \cdot 3) + (5 \cdot 4)$ je to samé jako $5(3 + 4)$. Obecně zapsáno, pro libovolné $x, y, z \in \mathbb{R}$ platí $x(y + z) = (x \cdot y) + (x \cdot z)$. Této vlastnosti se v algebře říka *distributivita*. Obecně, nemusíme se omezovat na reálná čísla s operací sčítání a součinu $(\mathbb{R}, +, \cdot)$, ale tuto vlastnost můžeme uvažovat u libovolné množiny se dvěma operacemi $(M, *, \circ)$. Tedy, dává smysl ji uvažovat také u svazu $(L, \vee, \wedge)$.

Svaz $(L, \leq)$ se nazývá *distributivní svaz* pokud pro libovolné $a, b, c \in L$ platí

$$a \vee (b \wedge c) = (a \vee b) \wedge (a \vee b).$$

Nyní ukážeme, jak budou distributivní svazy vypadat. Analogicky jako v předchozí kapitole zkusíme najít co nejmenší svaz, který naopak distributivní není. Pro stručnost ovšem prozradíme čtenáři, že všechny svazy které mají 4 či méně prvků distributivní jsou (což lze opět ověřit dosazováním jejich prvků do definice distributivity).

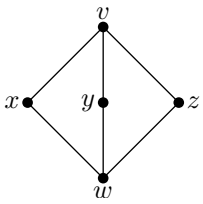
Nyní se vraťme k nejmenšímu svazu, který nesplnil podmínku modularity, tj. k pětiprvkovému svazu $(M_5, \leq)$ zadaného pomocí $M_5 = \{x, y, z, v, w\}$ a vyztahů $w \leq x \leq y \leq v$ a $w \leq z \leq v$. Postupným dosazováním prvů se dostaneme k případu

$$y \vee (x \wedge z) = y \neq x = (y \vee x) \wedge (y \vee z).$$

tedy, $(M_5, \leq)$ není distributivní svaz.

Podívejme se nyní na další příklad pětiprvkového svazu, a to svazu $(N_5, \leq)$ zadaného pomocí $N_5 = \{x, y, z, v, w\}$ a vyztahů $w \leq x \leq v$, $w \leq y \leq v$ a $w \leq z \leq v$ (viz obrázek).

Obrázek 12: $(N_5, \leq)$



Opět, ověřujeme-li postupně podmínku distributivity pro jednotlivé prvky, dostaneme se k případu

$$x \vee (y \wedge z) = x \neq v = (x \vee y) \wedge (x \vee z).$$

Tedy ani $(N_5, \leq)$ není distributivní. Není těžké (nicméně zdlouhavé) ukázat, že pětiprvkové svazy jiné než $(M_5, \leq)$ a $(N_5, \leq)$ distributivní jsou. Svazy $(M_5, \leq)$ a $(N_5, \leq)$ jsou duležitými příklady, jak ukazuje následující věta.

Věta 4.1. *Nechť $(L, \leq)$ je svaz. Potom $(L, \leq)$ je distributivní právě tehdy když neobsahuje podsvaz izomorfní svazu $(M_5, \leq)$, nebo $(N_5, \leq)$.*

Důkaz. □

S trochou zamyšlení nad předchozí větou a větou 3.1 vidíme, že každý distributivní svaz je modulární. Z nich dále plyne následující důsledek

Corollary 4.2. *Svaz $(M, \leq)$ je distributivní právě tehdy, pokud je modulární a neobsahuje podsvaz izomorfní s $(N_5, \leq)$.*

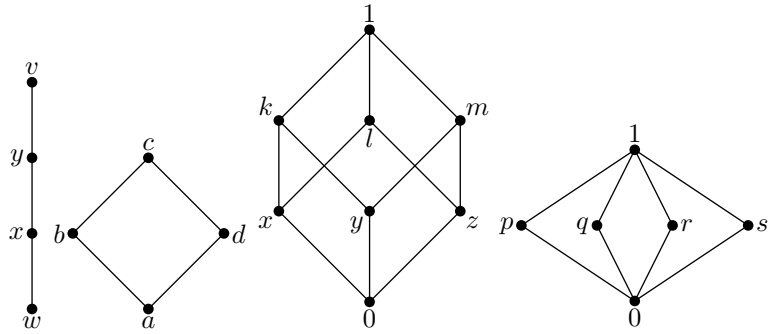
Tedy, množina distributivních svazů je podmnožinou modulárních svazů přesně takových, které neobsahují $(N_5, \leq)$ jako podsvaz. Proč nás tento fakt zajímá a k čemu se hodí, když modulární svaz neobsahuje podsvaz $(N_5, \leq)$ si nenechte ujít v následující kapitole.

5 Komplementární svazy

Nyní představíme ještě jeden důležitý pojem a to je pojem komplementu. Nechť $(L, \leq)$ je svaz obsahující největší prvek $1 \in L$ a nejmenší prvek $0 \in L$. Nechť $a \in L$. Prvek $a' \in L$ se nazývá *komplement* prvku $a \in L$ pokud platí $a \vee a' = 1$ a zároveň $a \wedge a' = 0$.

Příklad 5.1. Najděte komplementy jednotlivých prvků u svazů zadaných následujícími diagramy:

Obrázek 13: $(C, \leq_C), (D, \leq_D), (B, \leq_B), (U, \leq)$



Řešení 4. První svaz $(C, \leq_C)$ je řetězec. Vidíme, že pro prvky $x, y \in C$komplementy neexistují. Je jasné, že třeba pro x zde není žádný prvek t takový, pro který by platilo $x \vee t = v$ a $x \wedge t = w$. Stejně tak pro y. Komplement v' prvku v je w, tedy $w = v'$. Komplement w' prvku w je prvek $v = w'$.

V druhém svazu $(D, \leq_D)$ mají všechny prvky komplementy. Komplement a' prvku a je c, komplement b' prvku b je d, komplement c' prvku c je a a komplement d' prvku d je b.

Ve třetím svazu $(B, \leq_B)$ mají opět všechny prvky komplement. Jsou to:
$0' = 1$,
$x' = m$,
$y' = l$,
$z' = k$,
$k' = z$,
$l' = y$,
$m' = x$,
$1' = 0$.

Ve čtvrtém svazu $(U, \leq)$ mají opět všechny prvky komplement, nicméně komplementy nejsou jednoznačné. Komplementy prvku p jsou prvky q, r, s, protože vidíme, že platí $p \vee q = 1$, $p \wedge q = 0$, ale taky $p \vee r = 1$, $p \wedge r = 0$ a zároveň $p \vee s = 1$, $p \wedge s = 0$. Komplementy prvku q jsou prvky p, r, s atd.

Jak je vidno z předchozích příkladů, svaz může obsahovat prvky, pro které

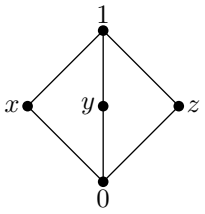
komplement neexistuje (viz svaz $(C, \leq_C)$) a stejně tak prvky, které mají komplementů více (viz svaz $(U, \leq)$).

Svaz $(L, \leq)$, ve kterém pro každý prvek $a \in L$ existuje alespoň jeden komplement $a' \in L$ se nazývá *komplementární*. Zamysleme se nyní, jakou podmínkou v komplementárním svaze zajistit, aby pro každý prvek $a \in L$ existoval *přesně* jeden komplement $a' \in L$. Pokud požadujeme, aby v komplementárním svazu existoval pro každý prvek $a \in L$ právě jeden komplement $a' \in L$, tak vlastně požadujeme, aby v L neexistovali tři prvky $x, y, z \in L$ takové, že

$$x \vee y = 1, x \vee z = 1, y \vee z = 1,$$
$$x \wedge y = 0, x \wedge z = 0, y \wedge z = 0.$$

Jinak řečeno, aby byly komplementy jednoznačné, komplementární svaz L nesmí obsahovat podsvaz

Obrázek 14: $(N, \leq)$



Věta 4.1 nám říká, že pokud je svaz distributivní, neobsahuje podsvaz $(N_5, \leq$), tedy neobsahuje ani podsvaz výše uvedený podsvaz. Dostáváme tedy:

Věta 5.2. *Nechť $(L, \leq)$ je komplementární svaz. Pokud je $(L, \leq)$ distributivní, potom pro každé $a \in L$ existuje právě jedno $a' \in L$, takové, že $a \vee a' = 1$ a $a \wedge a' = 0$. Jinak řečeno, pro každé $a \in L$ existuje právě jeden komplement $a' \in L$. .*

Důkaz. □

Distribitvita nám tedy v komplementárním svazu zajišťuje jednoznačnost komplementů. Nabízí se i obrácená otázka, tedy jestli svaz, ve kterém má každý prvek jednoznačný komplement musí být distributivní. To obecně neplatí, nicméně ve spoustě důležitých skupin svazů jako jsou třeba modulární ano. Na distributivitu se tedy můžeme dívat jako na vlastnost, která nám

v komplementárních svazech zajišťuje jednoznačnost komplementů. Zdůrazněmě, že pouze v komplementárních svazech, existují distributivní svazy, které nejsou komplementární, tj. existují v nich prvky, které nemají žádný komplement, viz příklad ...

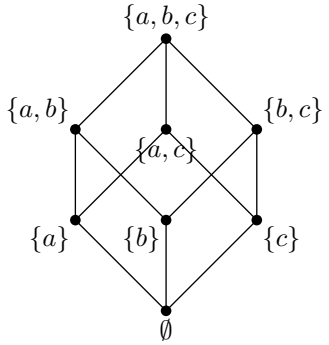
6 Booleovy algebry

Komplementární distributivní svaz $(L, \leq)$ se nazývá *Booleův svaz*, nebo též *Booleova algebra*. Dvě názvy téže věci souvisí s pohledem na svazy jako na množiny s uspořádáním $(L, \leq)$ a jako na množiny s dvěma operacem $(L, \vee, \wedge)$, tedy jako na algebry.

Většina studentů pravděpodobně již slova Booleova algebra, případně Booleova logika zaslechla, a to v logice na střední škole, případně v aplikovaných předmětech. To úzce souvisí s významem a použitím Booleových algeber. K tomu se dostaneme v druhé části kapitoly, nyní ještě chvíli zůstanem v matemtice a zaměříme se na jednu z důležitých vlastností Booleových algeber.

Příklad 6.1. Vraťme se k příkladu tříprvkové množiny $X = \{a, b, c\}$ a množiny všech jejích podmnožin $P(X)$. Tedy $P(X) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$. Jako uspořádání na $P(X)$ množinovou inkluzi $\subseteq$, tj. například $\{a\} \subseteq \{a, b\}$. Potom $(P(X), \subseteq)$ je svaz.

Obrázek 15: $(P(X), \subseteq)$



Porozkoumáním obrázku a použítím věty ... zjistíme, že jde o distributivní svaz. Dále, pro každý prvek lze nalézt jeho komplement, konkrétně $\emptyset' = \{a, b, c\}, \{a\}' = \{b, c\}, \{b\}' = \{a, c\}, \{c\}' = \{a, b\}, \{a, b\}' = \{c\}, \{a, c\}' = \{b\}, \{b, c\}' = \{a\}, \{a, b, c\}' = \emptyset$. Jde tedy o distributivní komplementární svaz, $(P(X), \subseteq)$ je tedy Booleova algebra.

Vidíme taky, že pro libovolné podmnožiny $A, B \in P(X)$, suprémum $A \vee B$ je rovno sjednocení množin $A \cup B$, tj. $A \vee B = A \cup B$. Podobně $A \wedge B = A \cap B$.

Výše uvedený příklad jde zobecnit. Nemusíme brát X pouze tříprvkouvou, ale můžeme vzít libovolnou množinu. Tedy, pro libovolnou množinu X, množina všech podmnožin $P(X)$ uspořádaná množinovou inkluzí $\subseteq$ je Booleova algebra $(P(X), \subseteq)$. Pro konkrétní podmnožinu $A \in P(X)$, komplement A' bude její množinový doplňek, tedy $A' = X - A$. Množiny všech podmnožin jsou důležitým příkladem Booleových algeber.

Zkusme si nyní vyřešit trochu jiný úkol, a to, pokusme se najít všechny možné Booleovy algebry, které mají 8 prvků. Tedy, čtenář se může pokusit malovat si různé osmiprvkové svazy tak, aby byly zároveň distributivní a komplementární. Po krátké snaze mu ale stejně prozradíme, že jedinný takový obrázek, který se mu podaří najít bude stejný jako obrázek v příkladu 6.1. Jinak řečeno, každá osmiprvková Booleova algebra je izomorfní svazu podmnožin $P(X)$ tříprvkové množiny X.

Naše otázka zní, platí-li něco podobného i obecněji. Odpověď je možná překvapivě, že ano.

Věta 6.2. *Každá* **konečná** *Booleova algbera B je izomorfní svazu všech podmnožin $P(X)$ nějaké množiny X.*

Důkaz výše uvedené věty není náročný a zvídavý čtenář mu se základními znalostmi může porozumět (lze nalézt třeba v ...), nicméně přesahuje potřeby tohoto textu jehož smysl je v předání základních úvah teorie svazů. Dodojeme, že důležitým předpokladem diskutované věty je konečný počet prvků Booleovy algebry B. Pro nekonečné Booleovy algebry platí obecnější věta, která říká, že libovolná Booleova algebra B je izomorfní **podsvazu** svazu všech podmnožin $P(X)$ nějaké množiny X.

Ačkoliv to čtenáři možná tak nepříjde, věta 6.2 je důležitá na několika úrovních. První z důsledků je, že pro zadaný počet prvků existuje pouze jedinná Booleova algebra. Za druhé nám říka, že každá konečná Booleova algebra má 2^n prvků, pro nějaké $n \in \mathbb{N}$ (jelikož každá množina podmnožin má 2^n prvků). Věta nám dává dobrou představu o tom, jak Booleovy algebry vypadají. Hlavním důvodem, kvůli kterému se o ni ale bavíme je, že je příkladem situace, které v matematice říká *konkrétní reprezentace*.

Booleovu algebru $(L, \leq)$ jsme definovali jako libovolnou množinu L s relací uspořádání $\leq$, která je svaz, je distributivní a komplementární. To je v jistém smyslu abstraktní způsob, je to jakákoliv množina L s relací $\leq$, která

má určité vlastnosti. Na druhé straně máme jendotlivé příklady Booleových algeber, tj. množiny všech podmnožin $P(X)$ pro zadané množiny X. O těch víme jak konkrétně vypadají, když nám někdo zadá množinu X, není težké si představit, jak bude $P(X)$ vypadat. Zmíněná věta nám říká, že ve skupině abstraktně definovaných (konečných) Booleových algeber žádné jiné Booleovy algebry, než zmíněné příklady $P(X)$ nejsou.

Čtenáře pravděpodobně napadne, proč se tedy vůbec abstraktní popis Booleových algeber zavádí, když jsou vlastně všechny mají stejnou strukturu jako $P(X)$ pro nějaké X. Důvodem je povaha matematické práce, kdy při dokazování je často výhodnější pracovat s abstraktním popisem, než s konkrétním $P(X)$. Například, pokud dostaneme zadaný svaz $(L, \leq)$ a máme ověřit, že jde o Booleovu algebru. Díky abstraktnímu popisu víme, že stačí ověřit distributivitu a komplementaritu. V případě, že bysme jej neznali, museli bysme ukázat, že L je izomorfní nějakému $P(X)$, což je mnohem více práce.

Analogii zmíněné situace lze nalézt v algebře i na jiných místech. Např. pro studenty se znalostí pojmu vektorového prostoru $(V, +)$ nad tělesem T. Vektorový prostor $(V, +)$ nad tělesem T je definován taktéž abstraktně jako libovolná množina V s operací $+$ a pronásobováním prvky z tělsa T, splňující určité vlastnosti (uzavřenost, komutativitu, asociativitu, existenci inverzních prvků, axiomy pronásobování z tělesa T). Později se však ukáže, že libovolný (konečněrozměrný) vektorový prostor na tělesem T je izomorfní kartézkému součinu T^n, tedy, že není níc jiného, než n-tice prvků z T. Taktéž by šlo namítnout, proč se trápíme s axiomy vektorového prostoru když by jej šlo definovat jako n-tice prvků. Nicméně abstraktní popis je nepoměrně výhodnější při dokazování.

Podobná situce je u grup, v případě **konečných** komutativních grup. Opět, konečná komutativní grupa $(G, +)$ je definována "abstraktně"jako množina G s operací $+$, která je uzavřená, komutativní, asociativní, pro každý prvek existuje inverze a má konečný počet prvků. Později se ukáže, že každá taková grupa G je izomorfní kartézkému součinu $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times \cdots \times \mathbb{Z}_{n_k}$, kde $\mathbb{Z}_{n_1}, \ldots, \mathbb{Z}_{n_k}$ jsou grupy zbytkových tříd po dělení $n_1, \ldots, n_k$.

6.1 Booleovy algebry v logice

Pravděpodobně každý čtenář tohoto textu se se symboly $\vee$ a $\wedge$ setkal již dříve a to v logice. Konkrétně symbol $\vee$ zastupuje spojku "a", případně "a zároveň"(konjunkci) a symbol $\wedge$ zastupuje spojku "nebo"(disjunkci). Připo-

meňmě ještě, že v logice se mluvilo o negaci výroků, která se značila ¬. Nyní budeme chvíli používat symboly ∨ a ∧ v jejich výše zmíněném logickém smyslu.

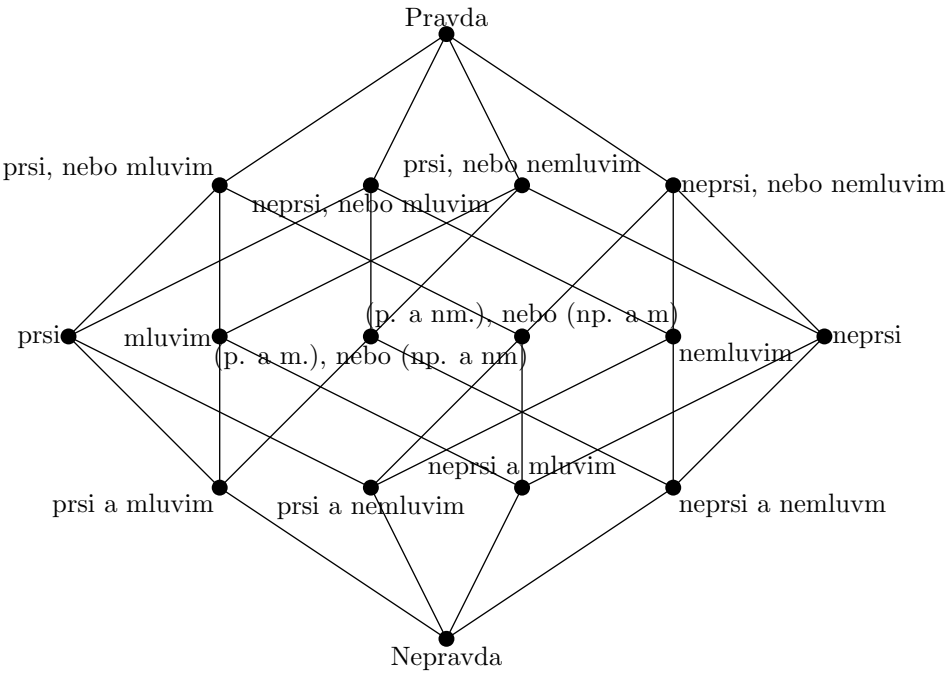
Vezměme si nyní dva výroky, jeden bude “prší"a druhý “mluvím". Úkol následujích stránek bude z těchto dvou výroků utvořit všechny možné nové výroky které vzniknou použitím výše zmíněných spojek “a", “nebo"či negace. Pusťme se do toho. První dostaneme výrok “Prší a mluvím". Podobně výrok “Prší, nebo mluvím". Mohli bychom výrok “prší"přidat dvakrát a dostali bysme “Prší a prší a mluvím", což je zjevně to samé (platí to právě tehdy když) jako “Prší a mluvím", takže tyto výroky vyloučíme. Mluvili jsme také o negaci, takže je potřeba přidat výroky “neprší"a “nemluvím". Výroky typu “Prší a neprší"jsou vždy nepravdivé, tak ty též nebudeme zmiňovat a označíme je jako “Nepravda". Naopak výrok “Prší, nebo neprší"je vždy pravdivý, tak ten označíme jako “Pravda". Určité výroky si budou odpovídat z hlediska pravdivosti, výrok “(Prší, nebo neprší) a mluvím"platí právě tehdy když platí “mluvím", takže ten taky nebudeme uvádět. Závorky, které v přirozeném jazyce samozřejmě neexistují, jsou tu potřeba, protože nám říkájí, v jakém pořadí logické spojky aplikujeme. Se značnou dávkou přemýšlení bysme se dostali k tomu, že lze vytvořit přesně 16 různých výroků, a to:

“prší"
“mluvím"
“neprší"
“nemluvím"
“prší a mluvím"
“prší a nemluvím"
“neprší a mluvím"
“neprší a nemluvím"
“prší, nebo mluvím"
“prší, nebo nemluvím"
“neprší, nebo mluvím"
“neprší, nebo nemluvím"
“(prší a mluvím), nebo (neprší a nemluvím)"
“(neprší a mluvím), nebo (prší a nemluvím)"
“Pravda"
“Nepravda"

Ověření toho, že jsou výroky všechny zahrnuje práci s pravdivostníma tabulkama, což je momentálně zbytečná technikalita, a tedy poprosíme čtenáře

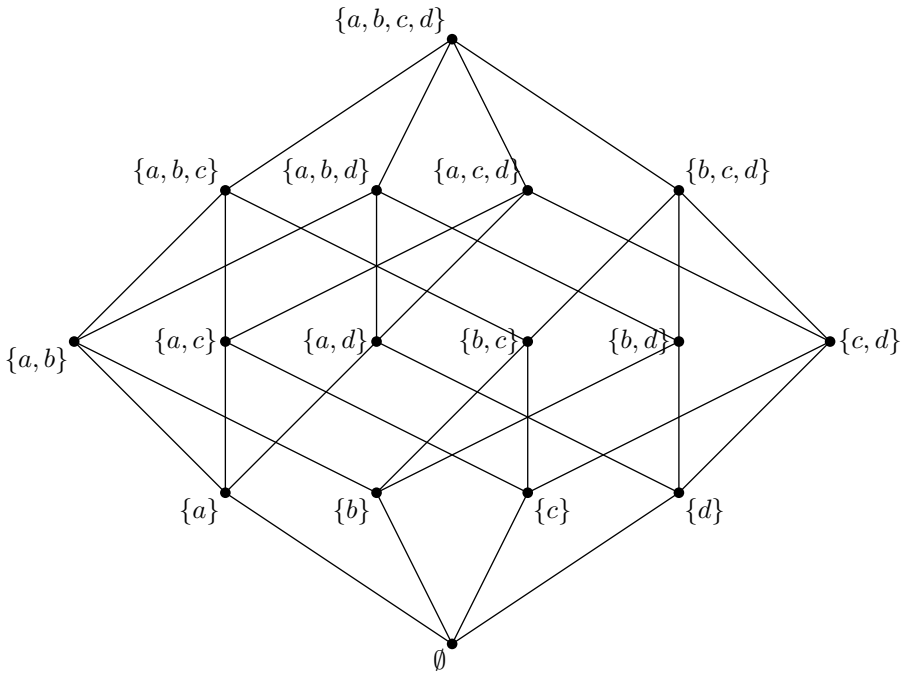
o důvěru. Je dále zjevné, že mezi výroky platí nějaké vztahy. Pokud platí výrok “prší", potom platí i výrok “prší, nebo mluvím". Říkáme, že výrok “prší"implikuje výrok “prší, nebo mluvím". Namalujme si nyní výroky jako obrázek a to tak, že pokud nějaký výrok implikuje jiný, bude níže a budou spojeny čarou. V obrázku nahradíme spojku “a", “nebo"jejich logickými symboly $\vee$ a $\wedge$.

Obrázek 16: $(M, \rightarrow)$



Srovnejme výše uvedený obrázek s obrázkem Booleovy algebry množiny všech podmnožin $P(X)$ na čtyřprvkové množině $X = \{a, b, c, d\}$.

Obrázek 17: $(P(X), \subseteq)$



Tedy pokud se na logické spojky “a"a “nebo", resp. $\vee$ a $\wedge$, díváme jako na operace na množině všech výše uvedených výroků, dostaneme Booleovu algebru. Konjunkce dvou výroků p a q (spojka “a") odpovídá jejich infimu $p \wedge q$, disjunkce dvou výroků p a q (spojka “nebo") odpovídá jejich suprému $p \vee q$. Všiměme si dále, že negace výroku p odpovídá jeho svazovému komplementu p' (např. pokud výrok “prší"odpovídá podmnožině $\{a, b\}$, potom výrok “neprší"odpovídá podmnožině $\{c, d\}$ v našem příkladě $P(X)$ na čtyřprvkové množině X, tj. komplementu $\{a, b\}$). Uspořádání $\leq$ pak odpovídá implikaci, tj. $p \leq q$ právě tehdy když p implikuje q.

Tohle platí i obecně, pokud vezmeme množinu výroků, která bude uzavřená na logické operace “a"a “nebo"a negaci, dostaneme Booleovu algebru. Booleovy algebry tedy z matematického hlediska popisují strukturu množiny výroků z pohledu výrokové logiky. Tento fakt se označuje tvrzením, že Booleovy algebry jsou *modely* výrokových logik. Booleových algebry nám umožňují používat matematický aparát na zkoumání výrokové logiky.

Nyní zmiňme příklad Booleovy algebry, která je základem mnoha technických disciplín, mj. logických obvodů, či programování, a to dvouprvková Booleova algebra $B = \{0, 1\}$, kde $0 \leq 1$.

...

Pravdivostní tabulky vypadají následovně:

Prvek 0 je standardně interpretován jako logická nepravda, přičemž 1 jako pravda.

Klíčovým pojmem výrokové logiky je *pravdivostní ohodnocení* výroku p. V praxi jde o to, že každému výroku z dané množiny přiřadíme buďto 0, což znamená, že výrok je nepravdivý, či 1, znamenající, že výrok je pravda. Tohle přiřazení není úplně libovolné, např. pokud je výrok p pravda, tj. 1, a výrok q také pravda, tj. přiřadíme mu taktéž 1, potom pravdivostní ohodnocení vyžaduje, aby ohodnocení výroku "p a zároveň q", tj. $p \wedge q$, bylo taktéž pravda. Z hlediska matematiky je prvadivostní ohodnocení množiny výroků L homomorfismem z Booleovy lagebry L do dvouprvkové Booleovy algebry $B = \{0, 1\}$.