ONDŘEJ LENGÁL

STUDIJNÍ OPORA IDM: SVAZY

FIT VUT V BRNĚ

1

Svazy

Svazy jsou zvláštním typem algeber s dvěmi (či více) operacemi, které charakterizují jistou třídu „hezky se chovajících“ částečně uspořádaných množin. Pod pojmem „hezky se chovající“ chápeme tu vlastnost, že pro každé dva prvky a, b z částečně uspořádané množiny M existuje prvek $c \in M$, který je větší než a i b, tj. $a \leq c$ a $b \leq c$ (a duálně existuje i prvek, který je menší než oba prvky). Tato vlastnost se využívá v mnoha oblastech informatiky, např. při synchronizaci procesů v distribuovaných systémech, práci se sémantikou programovacích jazyků nebo data miningu.

V této kapitole si postupně vybudujeme svazy dvěma způsoby: jako svazově uspořádané množiny a jako algebry s více operacemi.

Konvence: v tomto textu definujeme množinu přirozených čísel jako $\mathbb{N} = \{0, 1, 2, \ldots\}$, tj. $\mathbb{N}$ *obsahuje* nulu. Materiální implikaci a bikondicionál (logické spojky uvnitř formulí) budeme značit symboly $\rightarrow$ a $\leftrightarrow$, logický důsledek a logickou ekvivalenci (vztah mezi formulemi, hlavně v důkazech) symboly $\Rightarrow$ a $\iff$.

Začněme krátkým opakováním pojmu *částečně uspořádané množiny*.

1.1 Částečně uspořádané množiny

Částečně uspořádané množiny zobecňují známé vztahy jako *„číslo 4 je menší než číslo 10“* nebo *„písmeno* ***c*** *je v abecedě před písmenem* ***g****“* a dávají nám obecný rámec pro množiny, jejichž (ne nutně všechny) prvky můžeme mezi sebou *porovnávat*. Nechť M je množina a $\sqsubseteq$ je binární relace na M, tj. $\sqsubseteq\, \subseteq M \times M$, taková, že platí následující:

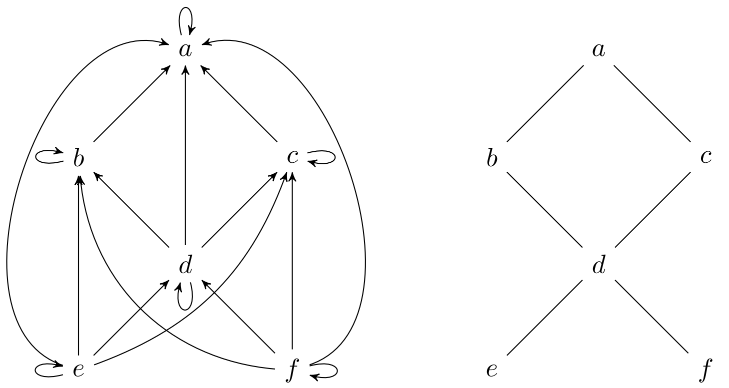
1. **reflexivita**: $\forall x \in M : x \sqsubseteq x$,
2. **antisymetrie**: $\forall x, y \in M : (x \sqsubseteq y \wedge y \sqsubseteq x) \ \rightarrow\ x = y$,
3. **tranzitivita**: $\forall x, y, z \in M : (x \sqsubseteq y \wedge y \sqsubseteq z) \ \rightarrow\ x \sqsubseteq z$.

Množinu M s uspořádáním $\sqsubseteq$ často značíme $(M, \sqsubseteq)$ a nazýváme *částečně uspořádaná množina* (angl. *partially ordered set*, někdy zkráceně jen *poset*). Pokud platí $x \sqsubseteq y$, pak říkáme, že *„x je menší nebo rovno y"* a *„y je větší nebo rovno x"* (a často krátce jen *„x je menší než y"* a *„y je větší než x"*; ostrou nerovnost bychom potom označovali jako *„x je ostře menší než y"*, atd.). Definujme si dále notaci $x \sqsubset y \overset{\text{def}}{\iff} x \sqsubseteq y \land x \neq y$.

Částečně uspořádanou množinu $(M, \sqsubseteq)$ označujeme za *lineárně uspořádanou* (někdy též *úplně* nebo *totálně uspořádanou*), pokud jsou každé dva prvky z M porovnatelné, formálně, $\forall x, y \in M : x \sqsubseteq y \lor y \sqsubseteq x$.

Příklad 1.1

1. Množina přirozených čísel $\mathbb{N}$ a relace *„menší nebo rovno"* $\leq$ mezi nimi je lineárně uspořádaná množina $(\mathbb{N}, \leq)$, protože
   - pro každé přirozené číslo x platí, že $x \leq x$ (*reflexivita*),
   - pokud $x \leq y$ a zároveň $y \leq x$, potom $x = y$ (*antisymetrie*),
   - pokud $x \leq y$ a zároveň $y \leq z$, potom $x \leq y$ (*tranzitivita*) a
   - pro každé dva prvky $x, y \in \mathbb{N}$ buď $x \leq y$ nebo $y \leq x$ (*linearita*).
2. Množina přirozených čísel $\mathbb{N}$ a relace *„ostře menší než"* $<$ *není* částečně uspořádaná množina, protože není reflexivní (existuje přirozené číslo x takové, že neplatí $x < x$, např. $x = 42$).
3. Uvažujme množinu $S = \{a, b, c\}$ a její potenční množinu
   $$2^S = \big\{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{b, c\}, \{a, c\}, S\big\}.$$
   Potom $(2^S, \subseteq)$ je částečně uspořádaná množina. $(2^S, \subseteq)$ *není* lineárně uspořádaná množina, protože obsahuje neporovnatelné prvky, např. $\{a\} \not\subseteq \{b\}$ a zároveň $\{b\} \not\subseteq \{a\}$.
4. Obecněji platí, že máme-li libovolnou množinu S, pak $(2^S, \subseteq)$ je částečně uspořádaná množina. Množina $(2^S, \subseteq)$ obecně není lineárně uspořádaná; půjde o lineární uspořádání jen pokud $|S| \leq 1$.
5. $(\mathbb{N}, |)$, kde $a \mid b$ platí pokud $\exists c \in \mathbb{N} : a \cdot c = b$ (tj. a *„dělí"* b), je částečně uspořádaná množina:
   - (*reflexivita*): Pro všechna čísla $x \in \mathbb{N}$ platí, že pokud $c = 1$, pak $x \cdot 1 = x$, a tedy $x \mid x$.
   - (*antisymetrie*): Pokud platí, že $x \mid y$ a zároveň platí, že $y \mid x$, pak z definice predikátu $\mid$ víme, že existují čísla $c_1, c_2 \in \mathbb{N}$ taková, že $x \cdot c_1 = y$ a zároveň $y \cdot c_2 = x$. Po dosazení první rovnosti do druhé dostaneme $x \cdot c_1 \cdot c_2 = x$, což platí nad přirozenými čísly c_1 a c_2 jen pokud $c_1 = c_2 = 1$, a tedy $x = y$.
   - (*tranzitivita*): Pokud platí, že $x \mid y$ a zároveň platí, že $y \mid z$, pak z definice predikátu $\mid$ víme, že existují čísla $c_1, c_2 \in \mathbb{N}$ taková, že $x \cdot c_1 = y$ a zároveň $y \cdot c_2 = z$. Po dosazení první rovnosti do



(a) Graf relace R (b) Hasseův diagram H_R

Obrázek 1.1: Příklad grafu relace R a odpovídajícího Hasseova diagramu. R je částečné uspořádání na množině $\{a, b, c, d, e, f\}$ definované jako $R = \{(b, a), (c, a), (d, b), (d, c), (e, d), (f, d), (a, a), (b, b), (c, c), (d, d), (e, e), (f, f), (d, a), (e, b), (e, c), (e, a), (f, b), (f, c), (f, a)\}$.

druhé dostaneme $x \cdot c_1 \cdot c_2 = z$, a tedy platí, že existuje $c_3 \in \mathbb{N}$, konkrétně $c_3 = c_1 \cdot c_2$ takové, že $x \cdot c_3 = z$.

6. $(\mathbb{Z}, |_{\mathbb{Z}})$, kde $a |_{\mathbb{Z}} b$ platí pokud $\exists c \in \mathbb{Z} : a \cdot c = b$, *není* částečně uspořádaná množina, protože je porušena vlastnost antisymetrie. Konkrétním příkladem jsou prvky 1 a -1. Platí, že $1 |_{\mathbb{Z}} -1$ (pro $c = -1$), platí i $-1 |_{\mathbb{Z}} 1$ (opět pro $c = -1$), ale $1 \neq -1$.

Cvičení 1.1

1. Dokažte, že částečně uspořádaná množina $(\mathbb{N}, |)$ není *lineárně* uspořádaná.
2. Je $(\mathbb{N}, =)$ částečně uspořádaná množina? Pokud ano, jde o lineární uspořádání?

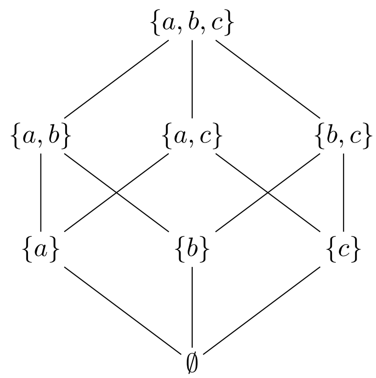
1.1.1 Hasseovy diagramy

Pro přehledné zobrazení *konečných* částečně uspořádaných množin se často používají tzv. Hasseovy diagramy.[1] Nechť R je částečné uspořádání na množině M. Pak *Hasseův diagram* H_R odpovídající R je nejmenší podmnožina R taková, že R je tranzitivně-reflexivní uzávěr relace H_R. Příklad grafu relace a Hasseova diagramu odpovídajícímu relaci je na Obrázku 1.1. Při grafické reprezentaci se používá konvence, že pokud $(x, y) \in H_R$, tedy *x je menší než y*, potom x je v diagramu *pod y* (v diagramu již pak není potřeba zakreslovat u hran šipky).

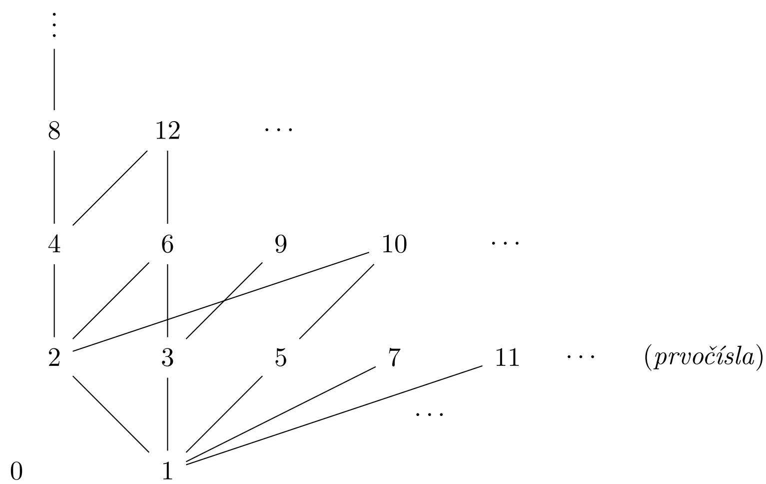
[1] Někdy pomocí Hasseových diagramů budeme naznačovat i *nekonečné* částečně uspořádané množiny.

Příklad 1.2

1. Uvažujme částečně uspořádanou množinu $(2^{\{a,b,c\}}, \subseteq)$. Hasseův diagram odpovídající této množině je uveden níže.



2. Hasseův digram pro částečně uspořádanou množinu $(\mathbb{N}, |)$ je naznačen níže. Všimněte si, že prvek 0 je v relaci pouze sám se sebou.



3. Hasseův diagram pro částečně uspořádanou množinu $(\mathbb{N}, =)$ je naznačen níže. Všimněte si, že *každý* prvek je v relaci pouze sám se sebou.

$$0 \qquad 1 \qquad 2 \qquad 3 \qquad 4 \qquad 5 \qquad \cdots$$

Cvičení 1.2

1. Je $(\mathbb{Z}, |)$ částečně uspořádaná množina, kde $a \mid b$ platí pokud $\exists c \in \mathbb{N} : a \cdot c = b$? Pokud ano, znázorněte její Hasseův diagram.

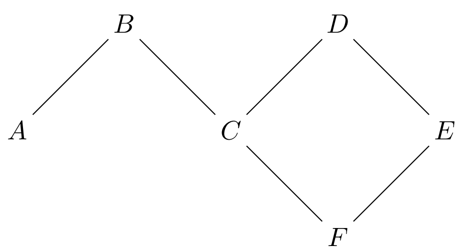
1.1.2 Infimum, supremum

Dále definujeme pojmy dolní a horní závory a taktéž infimum a supremum. Tyto pojmy nám označují prvky, které těsně ohraničují všechny prvky dané podmnožiny částečně uspořádané množiny zespodu a svrchu. Začneme definicí dolní a horní závory.

Nechť $(M, \sqsubseteq)$ je částečně uspořádaná množina a $B \subseteq M$. Prvek $d \in M$ je *dolní závora* množiny B pokud platí, že $\forall x \in B : d \sqsubseteq x$. Jinými slovy, d je dolní závora množiny B pokud je *menší* než všechny prvky z B. Duálně definujeme pojem *horní závora* množiny B jako prvek $h \in M$ takový, že $\forall x \in B : x \sqsubseteq h$, tj., h je *větší* než všechny prvky z B. Je-li jasné, že se pohybujeme ve svazu $(M, \sqsubseteq)$, tak pro množinu $X \subseteq M$ budeme používat $DZ(X)$ pro označení množiny všech jejich dolních závor a $HZ(X)$ pro množinu jejích horních závor.

Příklad 1.3

1. Uvažujme částečně uspořádanou množinu $(M, \sqsubseteq)$ danou následujícím Hasseovým diagramem:



   (a) B je horní závora množiny $\{A, B, C\}$.
   (b) B je též horní závorou množin $\{B\}$, $\{A, B\}$, $\{A\}$ a všech podmnožin $\{B, C, F\}$ (včetně prázdné množiny).
   (c) Množina $\{A, B, C\}$ nemá dolní závoru.
   (d) $\{C, F\}$ je množina dolních závor množiny $\{C, D\}$.
   (e) Množina $\{D\}$ má dolní závory D, C, E, a F.
   (f) M nemá žádnou horní závoru ani žádnou dolní závoru.
   (g) Množina $\emptyset$ má jako dolní i horní závory libovolný prvek z M.

2. Uvažujme lineárně uspořádanou množinu $(\mathbb{N}, \leq)$.

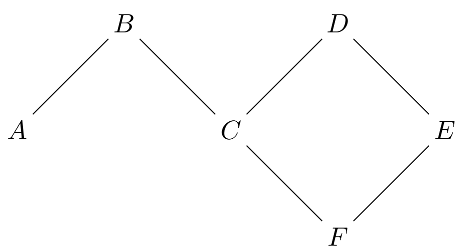
   (a) 142 je příklad horní závory množiny $\{6, 13, 91\}$ a 3 je příklad její dolní závory.
   (b) Množina $\{0, 1, 2, 3, 4, 5, 6\}$ obsahuje přesně všechny dolní závory množiny $\{6, 13, 91\}$ a nekonečná množina $\{91, 92, 93, \ldots\}$ přesně všechny její horní závory.
   (c) Množina $\mathbb{N}$ má (jedinou) dolní závoru 0 a nemá žádnou horní závoru.
   (d) Množina $\emptyset$ má jako dolní i horní závory libovolný prvek z $\mathbb{N}$.

Nyní se již dostáváme k definici infima a suprema. Nechť $(M, \sqsubseteq)$ je částečně uspořádaná množina a $B \subseteq M$. Prvek $i \in M$ je *infimum* množiny B pokud je i dolní závora B a pro všechny dolní závory x množiny B platí, že $x \sqsubseteq i$. Intuitivně, infimum množiny je její *největší* dolní závora. Infimum množiny B značíme jako $\sqcap B$. Pojem *supremum* množiny B je definován duálně jako prvek $s \in M$ takový, že s je horní závora B a pro všechny horní závory x množiny B platí, že $s \sqsubseteq x$. Tedy, supremum množiny je její nejmenší horní závora. Supremum množiny B značíme jako $\sqcup B$. Infimum ani supremum množiny nemusí existovat.

Často budeme pracovat s infimem a supremem dvouprvkových množin, a proto pro prvky $a, b \in M$ zavedeme následující binární operátory: pro infimum $a \sqcap b \stackrel{\text{def}}{=} \sqcap\{a, b\}$ a pro supremum $a \sqcup b \stackrel{\text{def}}{=} \sqcup\{a, b\}$.

Příklad 1.4

1. Uvažujme částečně uspořádanou množinu $(M, \sqsubseteq)$ danou následujícím Hasseovým diagramem (stejný jako v Příkladu 1.3):



   (a) B je supremum množin $\{A, B, C\}$, $\{B\}$, $\{A, B\}$, $\{A, C\}$, $\{B, C\}$, $\{B, C, F\}$ a $\{A, B, C, F\}$.
   (b) D je supremum např. množiny $\{C, E\}$, tj. $D = C \sqcup E$. Množina $\{C, E\}$ má infimum F, tj. $F = C \sqcap E$.
   (c) Dále platí, že $D = D \sqcup F$ a $F = D \sqcap F$.
   (d) M ani $\emptyset$ nemají supremum ani infimum.

2. Uvažujme lineárně uspořádanou množinu $(\mathbb{N}, \leq)$.

   (a) Supremum množiny $\{6, 13, 91\}$ je 91 a její infimum je 6.
   (b) Nekonečná množina $\{8, 10, 12, \ldots\}$ má infimum 8 a nemá supremum.

3. Uvažujme částečně uspořádanou množinu $(M, \leq)$, kde

$$M = \{-\infty\} \cup (-\infty, 0) \cup (0, +\infty) \cup \{+\infty\} .$$

   (a) Interval $\langle 2, 4\rangle$ má v $(M, \leq)$ infimum 2 a supremum 4.
   (b) Interval $(2, 4)$ má v $(M, \leq)$ též infimum 2 a supremum 4.
   (c) Interval $\langle 1, +\infty)$ má v $(M, \leq)$ infimum 1 a supremum $+\infty$.
   (d) Interval $\langle -1, 0)$ má v $(M, \leq)$ infimum -1 a nemá supremum.

Nechť $(M, \sqsubseteq)$ je částečně uspořádaná množina, $N \subseteq M$ její podmnožina a $i = \sqcap N$. Pokud $i \in N$, pak prvku i říkáme *nejmenší prvek* N. Duálně, pokud je $s = \sqcup N$, pak prvku s říkáme *největší prvek* N.

Příklad 1.5

1. Uvažujme částečně uspořádanou množinu $(\mathbb{R}, \leq)$. Číslo 42 je infimum intervalu $(42, 100)$, ale není jeho nejmenší prvek.

Poznámka 1.1

Infimu se někdy také říká *průsek* a supremu *spojení*. V angličtině se dolní a horní závory často označují termíny *lower bound* a *upper bound*. Anglické ekvivalenty pojmu infimum jsou: *infimum*, *meet* nebo *greatest lower bound*. Supremum se anglicky řekne *supremum*, *join* nebo *least upper bound*.

1.2 Svazově uspořádané množiny

Svazově uspořádané množiny jsou, intuitivně, částečně uspořádané množiny, které mají *dobře definované operace infima a suprema*.

Nechť $(M, \sqsubseteq)$ je částečně uspořádaná množina. Říkáme, že $(M, \sqsubseteq)$ je *svazově uspořádaná množina* (většinou jen *svaz*, angl. *lattice*), pokud zároveň platí následující dvě podmínky:

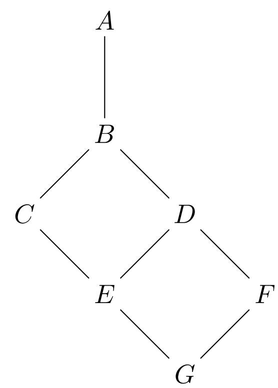
1. Každé dva prvky mají infimum v M, tj. $\forall a, b \in M : a \sqcap b \in M$.
2. Každé dva prvky mají supremum v M, tj. $\forall a, b \in M : a \sqcup b \in M$.

Když v předchozí definici nahradíme „Každé dva prvky“ za „Každá neprázdná konečná podmnožina“, dostaneme ekvivalentní definici. Dále definujme *úplný svaz* jako svaz $(M, \sqsubseteq)$, kde má *každá podmnožina* v M infimum i supremum (tedy i prázdná množina a libovolná nekonečná podmnožina, je-li svaz nekonečný). Formálně můžeme podmínku úplného svazu zapsat následujícím způsobem:

$$\forall A \subseteq M : \sqcap A \in M \qquad \text{a} \qquad \forall A \subseteq M : \sqcup A \in M \ .$$

Příklad 1.6

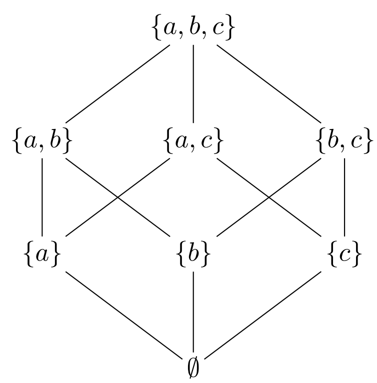
1. Uvažujte částečně uspořádanou množinu danou následujícím Hasseovým diagramem.



Tato množina je svaz, jelikož každé dva prvky v ní mají infimum a supremum. Např.:

- $C \sqcap F = G, \quad C \sqcup F = B,$
- $E \sqcap F = G, \quad E \sqcup F = D,$
- $A \sqcap E = E, \quad A \sqcup E = A.$

2. Uvažujme částečně uspořádanou množinu $(2^{\{a,b,c\}}, \subseteq)$, jejíž Hasseův diagram je uveden níže.



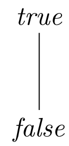
$(2^{\{a,b,c\}}, \subseteq)$ je svaz. Všimněte si, že v tomto svazu infimum dvou množin odpovídá jejich *průniku* a supremum jejich *sjednocení*.

3. Obecněji platí, že máme-li libovolnou množinu S, pak $(2^S, \subseteq)$ je svaz kde infimum odpovídá množinovému průniku a supremum odpovídá množinovému sjednocení. Dokonce se jedná o *úplný* svaz.

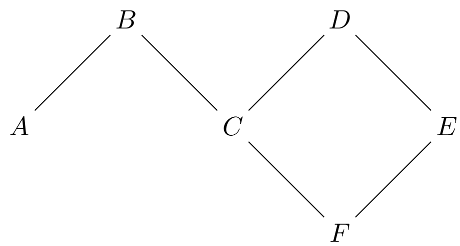
4. Částečně uspořádaná množina $(\{1\}, =)$ je svaz.

5. Částečně uspořádaná množina $(\emptyset, =)$ je svaz.

6. Částečně uspořádaná množina $(\{\mathit{false}, \mathit{true}\}, \Rightarrow)$, kde $\Rightarrow$ značí implikaci, je svaz. Jeho znázornění je na následujícím Hasseově diagramu:



7. Částečně uspořádaná množina vyobrazená Hasseovým diagramem níže není svaz.



Množina např. neobsahuje infimum prvků A a C nebo supremum prvků B a D.

8. Částečně uspořádaná množina $(\mathbb{N}, =)$ není svaz.

Cvičení 1.3

1. Dokažte, že $(\mathbb{N}, |)$ není svaz.
2. Dokažte, že $(\mathbb{N} \setminus \{0\}, |)$ je svaz. Čemu v tomto svazu odpovídá infimum a supremum dvou prvků?

Věta 1.1. *Nechť $(M, \sqsubseteq)$ je svazově uspořádaná množina. Potom pro každé dva prvky $a, b \in M$ platí následující:*

$$a \sqsubseteq b \iff a \sqcap b = a \tag{1.1}$$

$$a \sqsubseteq b \iff a \sqcup b = b \tag{1.2}$$

Důkaz. • $a \sqsubseteq b \iff a \sqcap b = a$:

$(\Rightarrow)$: Sporem. Předpokládejme, že $a \sqsubseteq b$ a $a \sqcap b = c$, kde $c \neq a$. Z definice infima plyne, že c je dolní závora množiny $\{a, b\}$, a tedy platí, že $c \sqsubseteq a$. Protože platí $c \sqsubseteq a \sqsubseteq b$, tak, aby bylo c *největší* dolní závora $\{a, b\}$, musí tedy platit, že $c = a$. Spor.

$(\Leftarrow)$: Plyne triviálně z definice infima.

• $a \sqsubseteq b \iff a \sqcup b = b$: Obdobně jako v předchozím případě. □

Věta 1.2. *Nechť $(M, \sqsubseteq)$ je svazově uspořádaná množina. Pak mají operace $\sqcap$ a $\sqcup$, pro všechna $x, y, z \in M$, následující vlastnosti:*

$$x \sqcap x = x \qquad x \sqcup x = x \qquad \textbf{\textit{(idempotence)}}$$
$$x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z \qquad x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z \qquad \textbf{\textit{(asociativita)}}$$
$$x \sqcap y = y \sqcap x \qquad x \sqcup y = y \sqcup x \qquad \textbf{\textit{(komutativita)}}$$
$$x \sqcap (x \sqcup y) = x \qquad x \sqcup (x \sqcap y) = x \qquad \textbf{\textit{(absorpce)}}$$

Důkaz. • Idempotence: triviální z definice $\sqcap$ a $\sqcup$ (např. $x \sqcap x = \sqcap\{x\}$).

• Asociativita: ukážeme pro infimum $\sqcap$ (pro supremum $\sqcup$ lze dokázat obdobně). Nejdříve dokážeme, že $x \sqcap (y \sqcap z) = \sqcap\{x, y, z\}$. Nechť $u = y \sqcap z$. Jelikož je u infimum y a z, pak platí, že u je největší prvek M pro který platí $u \sqsubseteq y$ a $u \sqsubseteq z$ (z předpokladu, že $(M, \sqsubseteq)$ je svazově uspořádaná množina víme, že právě jeden takový prvek existuje). Pro $x \sqcap (y \sqcap z) = x \sqcap u$ pak musí platit, že jde o největší prvek $i \in M$ takový, že $i \sqsubseteq x$ a $i \sqsubseteq u$. Z tranzitivity $\sqsubseteq$ tedy platí, že i je největší prvek takový, že $i \sqsubseteq x \wedge i \sqsubseteq y \wedge i \sqsubseteq z$, a tedy $i = \sqcap\{x, y, z\}$.

Obdobně lze dokázat i to, že $(x \sqcap y) \sqcap z = \sqcap\{x, y, z\}$. Potom tedy platí $x \sqcap (y \sqcap z) = \sqcap\{x, y, z\} = (x \sqcap y) \sqcap z$.

Důkaz pro $\sqcup$ lze vést obdobně.

• Komutativita: plyne triválně z definice operátorů (např. $x \sqcap y = \sqcap\{x, y\} = y \sqcap x$).

• Absorpce: Aby platilo, že $x \sqcup (x \sqcap y) = x$, musí dle Věty 1.1 platit, že $x \sqsubseteq x \sqcap y$, což platí triviálně z definice infima. Obdobně pro $x \sqcap (x \sqcup y) = x$. □

Z předchozího plyne, že je-li $(M, \sqsubseteq)$ svazově uspořádaná množina, potom je množina M *uzavřena* na operace $\sqcap$ a $\sqcup$. Lze tedy říct, že M s danými operacemi tvoří *algebru*.

1.3 Algebraická definice svazu

Jak jsme viděli v předchozí sekci, svazově uspořádané množiny lze chápat i jako algebry. V této sekci tuto myšlenku rozvedeme.

Pojmem *algebraicky definovaný svaz* označujeme algebru s dvěmi binárními operacemi $(M, \sqcap, \sqcup)$, ve které platí, pro všechna $x, y, z \in M$, následující vlastnosti:

$$
\begin{array}{llr}
x \sqcap x = x & x \sqcup x = x & (\textbf{idempotence}) \\
x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z & x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z & (\textbf{asociativita}) \\
x \sqcap y = y \sqcap x & x \sqcup y = y \sqcup x & (\textbf{komutativita}) \\
x \sqcap (x \sqcup y) = x & x \sqcup (x \sqcap y) = x & (\textbf{absorpce})
\end{array}
$$

Příklad 1.7

1. $(2^{\{a,b,c\}}, \cap, \cup)$ je (algebraicky definovaný) svaz. Zdůvodnění:
   - *idempotence*, *asociativita* a *komutativita* plynou triviálně z odpovídajících vlastností množinových operací $\cap$ a $\cup$.
   - *absorpce*: jelikož pro všechny množiny X, Y platí, že $X \subseteq X \cup Y$, pak bude platit, že $X \cap (X \cup Y) = X$. Obdobně pro $X \cup (X \cap Y) = X$.

Cvičení 1.4

1. Dokažte, že $(\mathbb{N} \setminus \{0\}, nsd, nsn)$, kde nsd značí největšího společného dělitele (např. $nsd(42, 14) = 7$) a nsn nejmenší společný násobek, je svaz.

Všimněme si, že vlastnosti algebraicky definovaného svazu odpovídají vlastnostem svazově uspořádané množiny z Věty 1.2. Jinými slovy, každou svazově uspořádanou množinu lze převést na algebraicky definovaný svaz. Platí to i obráceně? Tedy, lze každý algebraicky definovaný svaz převést na svazově uspořádanou množinu? Na tuto otázku odpovídá kladně Věta 1.4. Při převodu algebraicky definovaného svazu na svazově uspořádnou množinu budeme používat definici uspořádání $x \sqsubseteq y \overset{\text{def}}{\iff} x = x \sqcap y$. Nejdříve si dokažme následující pomocné tvrzení, které říká, že nezáleží, zda toto uspořádání definujeme pomocí infima nebo suprema.

Lemma 1.3. *Platí, že $x = x \sqcap y$ právě když $y = x \sqcup y$.*

Důkaz.

$$
\begin{array}{llr}
 & x = x \sqcap y & \wr\text{předpoklad}\wr \\
\iff & y \sqcup x = y \sqcup (x \sqcap y) & \wr y \sqcup \cdot \text{ na obě strany rovnice}\wr \\
\iff & y \sqcup x = y & \wr\text{absorpce}\wr \\
\iff & x \sqcup y = y & \wr\text{komutativita}\wr
\end{array}
\qquad \square
$$

Z Lemmy 1.3 plyne, že uspořádání $\sqsubseteq$ můžeme definovat i jako $x \sqsubseteq y \iff y = x \sqcup y$. Nyní se již dostáváme k samotné větě, která říká, že každý algebraicky definovaný svaz lze převést na svazově uspořádanou množinu.

Věta 1.4. *Nechť* $(M, \sqcap, \sqcup)$ *je algebraicky definovaný svaz. Pak platí, že* $(M, \sqsubseteq)$, *kde* $x \sqsubseteq y \overset{def}{\iff} x \sqcap y = x$, *je svazově uspořádaná množina.*

Důkaz. 1. Nejdříve ukážeme, že $\sqsubseteq$ je částečné uspořádání na M.

- (*reflexivita*): Máme dokázat, že pro všechna $x \in M$ platí, že $x \sqsubseteq x$. Dle definice $x \sqsubseteq y \overset{\text{def}}{\iff} x \sqcap y = x$ platí, že $x \sqsubseteq x$ právě když $x \sqcap x = x$, což plyne z vlastnosti idempotence.
- (*antisymetrie*): Máme dokázat, pro všechna $x, y \in M$, že pokud $x \sqsubseteq y$ a $y \sqsubseteq x$, pak $x = y$. Z definice $\sqsubseteq$ plyne, že $x \sqsubseteq y$ právě když $x = x \sqcap y$ a $y \sqsubseteq x$ právě když $x \sqcap y = y$. Tedy, platí $x = x \sqcap y = y$, takže $x = y$.
- (*tranzitivita*): Máme dokázat, pro všechna $x, y, z \in M$, že pokud $x \sqsubseteq y$ a $y \sqsubseteq z$, pak $x \sqsubseteq z$. Předpokládejme, že $x \sqsubseteq y$ a $y \sqsubseteq z$ (tj. $x = x \sqcap y$ a $y = y \sqcap z$) a uvažujme následující sekvenci algebraických úprav:

$$
\begin{aligned}
x \sqsubseteq y \iff x &= x \sqcap y && \wr\text{předpoklad a definice } \sqsubseteq\int \\
&= x \sqcap (y \sqcap z) && \wr\text{předpoklad } y = y \sqcap z\int \\
&= (x \sqcap y) \sqcap z && \wr\text{asociativita}\int \\
&= x \sqcap z && \wr\text{předpoklad } x = x \sqcap y\int
\end{aligned}
$$

Dostali jsme, že $x = x \sqcap z$ a tedy (z definice $\sqsubseteq$) platí, že $x \sqsubseteq z$.

2. Aby $(M, \sqsubseteq)$ byla svazově uspořádaná množina, tak nám zbývá dokázat, že každé dva prvky M mají v M unikátní *největší dolní závoru* a *nejmenší horní závoru*. Konkrétně, budeme dokazovat, že pro libovolné $a, b \in M$ platí, že $a \sqcap b$ je největší dolní závora množiny $\{a, b\}$, a že $a \sqcup b$ je její nejmenší horní závora.

Začněme s důkazem největší dolní závory. Nechť $a \sqcap b = c$. Budeme dokazovat, že c je největší dolní závora množiny $\{a, b\}$. Nejdříve dokážeme, že c je dolní závora této množiny.

$$
\begin{aligned}
& & a \sqcap b &= c && \wr\text{předpoklad}\int \\
&\iff & a \sqcup (a \sqcap b) &= a \sqcup c && \wr a \sqcup \cdot \text{ na obě strany rovnice}\int \\
&\iff & a &= a \sqcup c && \wr\text{absorpce}\int \\
&\iff & c &= a \sqcap c && \wr\text{Lemma 1.3}\int \\
&\iff & c &= c \sqcap a && \wr\text{komutativita}\int \\
&\iff & c &\sqsubseteq a && \wr\text{definice } \sqsubseteq\int
\end{aligned}
$$

Dokázali jsme, že $c \sqsubseteq a$. Obdobně dokážeme, že $c \sqsubseteq b$ (v důkazu se v prvním kroce na obě strany rovnice místo $a \sqcup \cdot$ přidá $b \sqcup \cdot$, zbytek postupu je stejný). Z předchozího plyne, že c je dolní závora $\{a, b\}$.

Nyní dokážeme, že c je *největší* dolní závora $\{a, b\}$. Důkaz povedeme sporem. Předpokládejme, že existuje $z \in M$ takové, že platí $z \sqsubseteq a$,

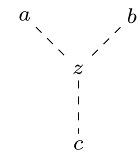
$z \sqsubseteq b$ a $c \sqsubset z$ (tedy $c \sqsubseteq z \wedge c \neq z$).[2] Budeme pokračovat následujícím usuzováním:

$$
\begin{array}{lcr}
 & z \sqsubseteq a & \wr\text{předpoklad}\int \\
\iff & z = z \sqcap a & \wr\text{definice } \sqsubseteq\int \\
\iff & z \sqcap b = (z \sqcap a) \sqcap b & \wr\cdot \sqcap b \text{ na obě strany rovnice}\int \\
\iff & z \sqcap b = z \sqcap (a \sqcap b) & \wr\text{asociativita}\int \\
\iff & z \sqcap b = z \sqcap c & \wr\text{předpoklad } a \sqcap b = c\int \\
\iff & z = z \sqcap c & \wr\text{předpoklad } z \sqsubseteq b\int \\
\iff & z \sqsubseteq c & \wr\text{definice } \sqsubseteq\int
\end{array}
$$

Získali jsme, že $z \sqsubseteq c$, což je ve sporu s předpokladem $c \sqsubset z$.

Důkaz toho, že $a \sqcup b$ je nejmenší horní závora množiny $\{a, b\}$, lze provést obdobně. □

[2] Graficky si můžeme tuto situaci znázornit následujícím výřezem z odpovídajícího Hasseova diagramu.



Dokázali jsme, že svazově uspořádané množiny a algebraicky definované svazy lze mezi sebou převádět. V následujícím textu proto budeme mezi těmito dvěma reprezentacemi volně přecházet a mluvit prostě o *svazech*.

Poznámka 1.2

Ekvivalence svazově uspořádaných množin a algebraicky definovaných svazů je příkladem *dvou různých syntaktických definic, které mají stejnou sémantiku*. Struktura, kterou obě definice vymezují, je *svaz*, a pokud s ním pracujeme, můžeme se svobodně rozhodnout, kterou definici použijeme (zpravidla tu, která je pro nás z nějakeho důvodu výhodnější).

Uvědomění si rozdílu mezi sémantikou a syntaxí (neboli *informací* a její *reprezentací*) je pro informatiky klíčové, jelikož počítače umí pracovat jen s reprezentacemi informací, my však chceme, aby nám poskytovaly informace. Uveďmě si jako příklad reprezentaci konečných množin v paměti počítače. Existuje mnoho způsobů, jak množiny v počítačích reprezentovat, přičemž většina z nich má jiné výhody a hodí se pro jiné účely. Příklady reprezentace množin v počítači (spolu s některými výhodami a nevýhodami) můžou být následující:

- *seřazené pole*: vhodné pro menší množiny, do kterých nevkládáme často nový prvek (vložení prvku má lineární složitost, vyhledávání logaritmickou za použití binárního hledání),
- *binární vyhledávací strom*: logaritmické vkládání i hledání, může však být potřeba strom vyvažovat, což způsobuje dodatečnou režii.
- *hashovací tabulka*: (amortizovaná) konstantní průměrná doba přístupu, nevhodné pro malé množiny, potřeba počítat hashovací funkci.

Pochopení rozdílu mezi syntaxí a sémantikou nám umožní, mimo jiné, navrhování lepších abstrakcí v programech, což vede k udržovatelnějšímu a lépe použitelnému kódu.

1.4 Podsvazy

Uvažujme (algebraicky definovaný) svaz $(M, \sqcap_M, \sqcup_M)$ a podmnožinu $P \subseteq M$. Říkáme, že $(P, \sqcap_P, \sqcup_P)$ je *podsvaz* svazu $(M, \sqcap_M, \sqcup_M)$, pokud platí následující dvě podmínky:

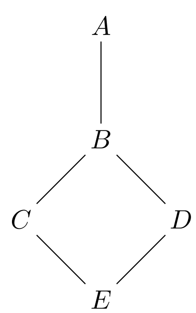
1. $(P, \sqcap_P, \sqcup_P)$ je svaz a
2. pro všechna $x, y \in P$ platí, že

$$x \sqcap_P y = x \sqcap_M y \qquad \text{a} \qquad x \sqcup_P y = x \sqcup_M y \quad .$$

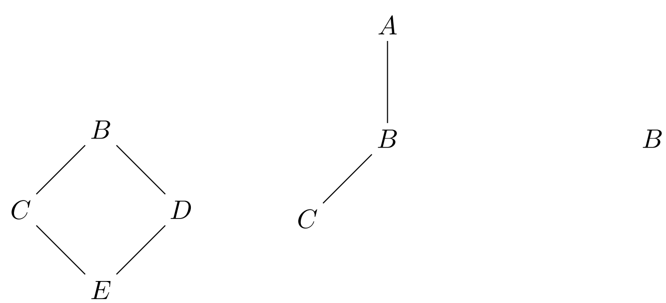
Neformálně bychom mohli říct, že podsvaz je podmnožina původního svazu, kde jsou zachována infima a suprema. Pojem podsvazu budeme spolu s *izomorfismem* svazů definovaným níže používat při klasifikaci svazů v Sekci 1.5.

Příklad 1.8

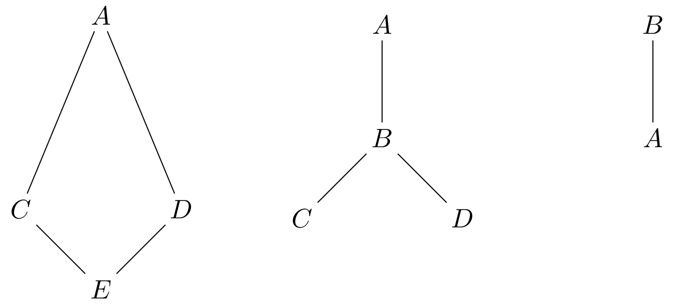
1. Uvažujme svaz $(M, \sqcap_M, \sqcup_M)$ daný následujícím Hasseovým diagramem:



- Následující tři uspořádání *jsou* podsvazy $(M, \sqcap_M, \sqcup_M)$:



- Následující Hasseovy diagramy *nerezprezentují* podsvazy $(M, \sqcap_M, \sqcup_M)$:



(a) (b) (c)

Zdůvodnění:

(a) Není zachováno supremum $C \sqcup_M D = B$.
(b) Nejde o svaz.
(c) Není zachováno infimum $A \sqcap_M B = B$.

Přejděme k vysvětlení pojmu *izomorfismu* svazů. Jsou-li dva svazy izomorfní, jde to chápat tak, že tyto svazy mají stejnou strukturu, tedy, jejich Hasseovy diagramy lze nakreslit tak, že vypadají stejně, až na pojmenovaní uzlů.[3]

[3] U nekonečných svazů samozřejmě nelze Hasseovy diagramy jednoduše nakreslit.

Formálně, mějme svazy $S_M = (M, \sqcap_M, \sqcup_M)$ a $S_N = (N, \sqcap_N, \sqcup_N)$. Pokud existuje bijekce $f : M \longleftrightarrow N$ taková, že pro každé $x, y \in M$ platí

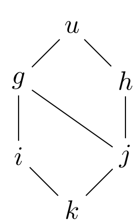
$$f(x \sqcap_M y) = f(x) \sqcap_N f(y) \qquad \text{a} \qquad f(x \sqcup_M y) = f(x) \sqcup_N f(y) \ ,$$

potom jsou svazy S_M a S_N *izomorfní*. Bijekci f nazýváme *izomorfismem* svazů S_M a S_N.[4]

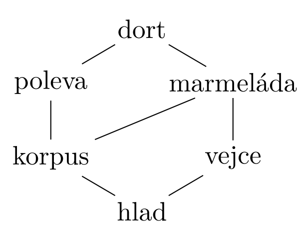
[4] Všimněte si, že izomorfismus svazů je speciální případ izomorfismu algeber.

Příklad 1.9

1. Uvažujme svazy $S_M = (M, \sqcap_M, \sqcup_M)$ a $S_N = (N, \sqcap_N, \sqcup_N)$ dány následujícími Hasseovými diagramy:



$S_M = (M, \sqcap_M, \sqcup_M)$



$S_N = (N, \sqcap_N, \sqcup_N)$

Svazy S_M a S_N jsou izomorfní. Izomorfismem f těchto svazů je funkce

$$\begin{aligned} f = \{&u \mapsto \text{dort}, g \mapsto \text{marmeláda}, h \mapsto \text{poleva}, \\ &i \mapsto \text{vejce}, j \mapsto \text{korpus}, k \mapsto \text{hlad}\} \ . \end{aligned}$$

Všimněte si, že izomorfismus nehledí na to, jestli jsou *neporovnatelné prvky* v Hasseově diagramu vlevo nebo vpravo od sebe. Vskutku, lze říct, že dva svazy jsou izomorfní, pokud jsou *grafy jejich Hasseových diagramů* izomorfní (viz část předmětu zaměřená na *grafy*).

1.5 Klasifikace svazů

Svazy lze klasifikovat mnoha různými způsoby. Již v Sekci 1.2 jsme si řekli o *úplných* svazech. Ve zbytku této sekce si ukážeme další, často se vyskytující podtřídy svazů.

1.5.1 Distributivní svaz

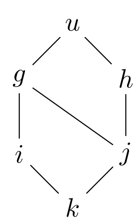
Svaz $(M, \sqcap, \sqcup)$ je *distributivní* pokud pro všechna $x, y, z \in M$ platí následující:

$$x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z) \qquad \text{a} \qquad x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z) \quad .$$

Výše uvedeným vlastnostem se často říká *distributivní zákony*.

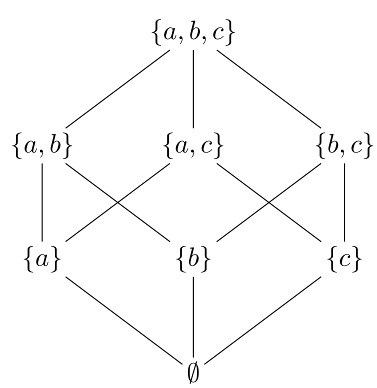
Příklad 1.10

1. Uvažujme svaz daný následujícím Hasseovým diagramem:



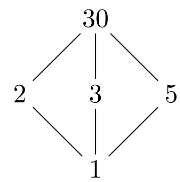
   Tento svaz *je* distributivní (lze ověřit například otestováním distributivních zákonů pro všechny trojice x, y, z).

2. Uvažujme množinový svaz daný následujícím Hasseovým diagramem:



   Tento svaz je též distributivní.

3. Mějme $A = \{1, 2, 3, 5, 30\}$ a uvažujme svazově uspořádanou množinu $M_3 = (A, |)$. (Připomeňme si, že $x \mid y$ právě když x *dělí* y.) Hasseův diagram svazu M_3 je následující:



Tento svaz *není* distributivní, protože

$$(2 \sqcap 3) \sqcup 5 \;=\; 1 \sqcup 5 \;=\; 5 \quad ,$$

ale

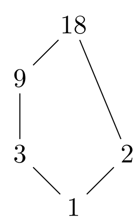
$$(2 \sqcup 5) \sqcap (3 \sqcup 5) \;=\; 30 \sqcap 30 \;=\; 30 \quad .$$

Z předchozího plyne, že

$$(2 \sqcap 3) \sqcup 5 \;\neq\; (2 \sqcup 5) \sqcap (3 \sqcup 5) \quad ,$$

což porušuje distributivní zákon.

4. Mějme $B = \{1, 2, 3, 9, 18\}$ a uvažujme svazově uspořádanou množinu $N_5 = (B, |)$. Hasseův diagram svazu N_5 je následující:



Svaz N_5 *není* distributivní, jelikož

$$(9 \sqcap 2) \sqcup 3 \;=\; 1 \sqcup 3 \;=\; 3 \quad ,$$

ale

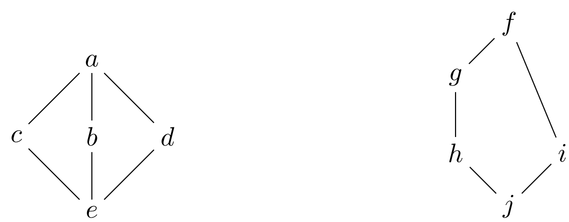
$$(9 \sqcup 3) \sqcap (2 \sqcup 3) \;=\; 9 \sqcap 18 \;=\; 9 \quad .$$

Z předchozího plyne, že

$$(9 \sqcap 2) \sqcup 3 \;\neq\; (9 \sqcup 3) \sqcap (2 \sqcup 3) \quad ,$$

což porušuje distributivní zákon.

Svazy M_3 a N_5 z Příkladu 1.10 jsou významné, jelikož lze pomocí nich určit nezbytná a postačující podmínka pro to, aby byl svaz distributivní (viz Věta 1.5). Když abstrahujeme od konkrétních nosných množin, můžeme si tyto svazy znázornit pomocí následujících Hasseových diagramů:



M_3 N_5

Obrázek 1.2: Základní nedistributivní svazy

Označení M_3 se používá pro libovolný svaz s ním izomorfní a těmto svazům se říká *diamantové svazy.*[5] Podobně i N_5 se používá pro libovolný s ním izomorfní svaz; těmto svazům se říká *pentagonální svazy.*[6]

[5] V literatuře se někdy lze setkat i s označením M_5.

[6] Jako mnemotechnická pomůcka může sloužit zvýraznění ve slovech *dia**M**antový* a *pe**N**tagonální*.

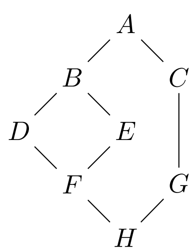
Věta 1.5. *Svaz je distributivní právě tehdy, když neobsahuje žádný podsvaz izomorfní s M_3 nebo N_5.*

Důkaz. Nad rámec tohoto textu, zájemci mohou najít v literatuře. □

Větu 1.5 lze využít pro rychlé rozhodnutí, zda je svaz distributivní.

Příklad 1.11

1. Uvažujme svaz S_M daný následujícím Hasseovým diagramem.



Tento svaz *není* distributivní jelikož obsahuje např. podsvaz $S_P = (\{A, B, F, G, H\}, \sqcap_P, \sqcup_P)$, kde $\sqcap_P$ a $\sqcup_P$ jsou infima a suprema svazu S_M omezena na doménu $\{A, B, F, G, H\}$. Nalezení takového podsvazu pro důkaz nedestributivity stačí, kdybychom ale chtěli být konkrétní, distributivita je porušena např. v následujícím případě:

$$B \sqcap (G \sqcup F) \neq (B \sqcap G) \sqcup (B \sqcap F) \ .$$

Poznámka 1.3

U *úplných* svazů je často požadována silnější podmínka, a to tzv. *úplná distributivita.* Svaz $(M, \sqcap, \sqcup)$ je *úplně distributivní,* pokud v něm pro každou množinu množin $\big\{\{x_{j,k} \in M \mid k \in K_j\} \mid j \in J\big\}$ platí následující vlastnost (J je množina *indexů 1. úrovně* a K_j je, pro každé

$j \in J$, množina *indexů 2. úrovně*):

$$\bigsqcap_{j \in J} \bigsqcup_{k \in K_j} x_{j,k} = \bigsqcup_{f \in F} \bigsqcap_{j \in J} x_{j,f(j)} \ , \tag{1.3}$$

kde F je množina *funkcí výběru* f takových, že pro všechna $j \in J$ bude $f(j)$ vybírat právě jeden prvek z K_j.

1.5.2 Ohraničený svaz

Svaz $(M, \sqcap, \sqcup)$ je *ohraničený* (angl. *bounded*) pokud existují prvky $\bot, \top \in M$ takové, že

$$\forall x \in M : \bot \sqcap x = \bot \qquad \text{a} \qquad \forall x \in M : x \sqcup \top = \top \ .$$

Takový svaz pak někdy značíme jako algebru $(M, \sqcap, \sqcup, \bot, \top)$ kde $\bot$ a $\top$ jsou *nulární* operace[7], tj. funkce $M^0 \to M$. Prvkům $\bot$ a $\top$ se říká infimum a supremum svazu (anglicky někdy také *bottom* a *top*).

[7] Nulárním operacím říkáme *konstanty*. Funkci $M^0 \to M$ si můžeme představit jako funkci, která n-tici „()“ o délce nula přiřazuje jeden vybraný prvek množiny M.

Lemma 1.6. *Je-li* $(M, \sqcap, \sqcup, \bot, \top)$ *ohraničený svaz, potom platí*

$$\bot = \sqcap M = \sqcup \emptyset \qquad a \qquad \top = \sqcup M = \sqcap \emptyset \ .$$

Důkaz. Nechť $(M, \sqcap, \sqcup, \bot, \top)$ je ohraničený svaz.

- Nejprve dokážeme, že $\bot = \sqcap M$.

$$\begin{aligned} & \forall x \in M : \bot = \bot \sqcap x && \wr \text{definice ohraničeného svazu} \int \\ \iff \quad & \forall x \in M : \bot \sqsubseteq x && \wr \text{Věta 1.1} \int \end{aligned}$$

Z předchozího plyne, že $\bot$ je dolní závora množiny M.

Nyní dokažme, že $\bot$ je *jediná*, a tudíž největší dolní závora M, a tedy $\bot = \sqcap M$. Důkaz povedeme sporem. Předpokládejme, že existuje $z \in M$ takové, že z je dolní závora M a $z \neq \bot$. Pak tedy musí platit, že $\forall y \in M : z \sqsubseteq y$. Jelikož $\bot \in M$, pak tedy platí, že $z \sqsubseteq \bot$. Z definice ohraničeného svazu pak platí $\bot \sqsubseteq z$ a z antisymetrie $\sqsubseteq$ plyne, že $z = \bot$. Spor.

- Nyní dokažme, že $\bot = \sqcup \emptyset$. Triviálně platí, že $\bot$ je horní závora prázdné množiny. Jelikož, dle definice ohraničeného svazu a Věty 1.1, je $\bot$ menší než všechny prvky M, pak je $\bot$ nejmenší takováto horní závora.

- Důkazy $\top = \sqcup M$ a $\top = \sqcap \emptyset$ lze provést obdobně jako předešlé. □

Lemma 1.7. *Nechť* $(M, \sqcap, \sqcup)$ *je svaz obsahující prvky* $\bot$ *a* $\top$ *takové, že platí*

$$\bot = \sqcap M = \sqcup \emptyset \qquad a \qquad \top = \sqcup M = \sqcap \emptyset \ .$$

Potom je $(M, \sqcap, \sqcup)$ *ohraničený.*

Důkaz. Ponechán jako cvičení čtenáři. □

Důsledek 1.8. *Svaz* $(M, \sqcap, \sqcup)$ *je ohraničený právě tehdy, když obsahuje prvky* $\perp$ *a* $\top$ *takové, že*

$$\perp = \sqcap M = \sqcup \emptyset \qquad a \qquad \top = \sqcup M = \sqcap \emptyset \ .$$

Důkaz. Směr $\Rightarrow$ plyne z Lemmy 1.6 a směr $\Leftarrow$ plyne z Lemmy 1.7. □

Důsledek 1.9. *Každý úplný svaz je ohraničený.*

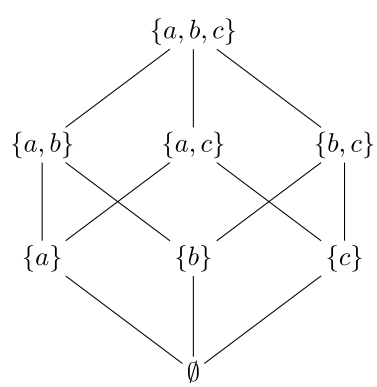
Důkaz. Nechť $(M, \sqsubseteq)$ je úplný svaz, pak z definice úplného svazu platí, že existují prvky $\perp = \sqcap M$ a $\top = \sqcup M$ takové, že $\perp, \top \in M$. Zbývá nám ukázat, že $\perp = \sqcup \emptyset$ a $\top = \sqcap \emptyset$, což plyne z toho, že $\perp$ je nejmenší prvek M a $\top$ je největší prvek M. □

Příklad 1.12

1. Uvažujme svaz $(\mathbb{N} \setminus \{0\}, |)$. Tento svaz není ohraničený (sice má infimum 1, ale nemá supremum).
2. Následující příklad ukazuje, že Věta 1.9 obráceným směrem (tj. „Každý ohraničený svaz je úplný.“) neplatí. Uvažujme svaz $(M, \leq)$, kde

$$M = \{-\infty\} \cup (-\infty, 0) \cup (0, +\infty) \cup \{+\infty\} \ .$$

   Tento svaz je zřejmě ohraničený ($-\infty$ je jeho infimum a $+\infty$ je jeho supremum), ale není úplný, protože např. neobsahuje supremum množiny $(-\infty, 0)$.
3. Uvažujme množinový svaz daný následujícím Hasseovým diagramem:



   Tento svaz je ohraničený (jeho infimum je $\emptyset$ a supremum je $\{a, b, c\}$).

1.5.3 Komplementární svaz

Svaz $(M, \sqcap, \sqcup)$ je *komplementární* (angl. *complemented*) pokud platí následující dvě podmínky:

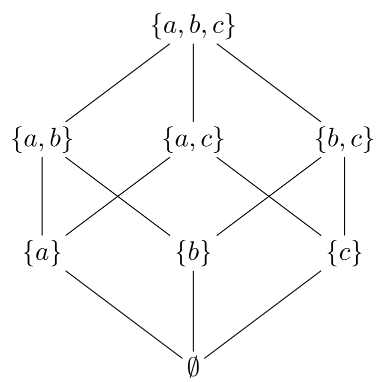
1. je ohraničený, tj. obsahuje infimum $\bot$ a supremum $\top$ a

2. ke každému prvku $x \in M$ existuje *komplement*, tj. prvek $\overline{x}$ takový, že

$$x \sqcap \overline{x} = \bot \quad \text{a} \quad x \sqcup \overline{x} = \top.$$

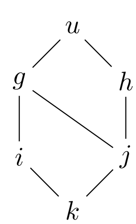
Příklad 1.13

1. Uvažujme množinový svaz daný následujícím Hasseovým diagramem:



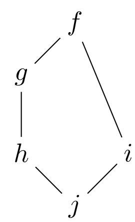
   Tento svaz *je* komplementární. Všimněte si, že komplementem prvku X je prvek $\{a, b, c\} \setminus X$; komplement zde tedy odpovídá množinovému doplňku.

2. Uvažujme svaz daný následujícím Hasseovým diagramem:



   Tento svaz *není* komplementární, jelikož prvky g a j nemají komplement (prvky u, h, i a k komplement mají).

3. Uvažujme svaz daný následujícím Hasseovým diagramem:



Tento svaz komplementární *je*. Všimněte si, že prvek i má dva komplementy (g a h).

Věta 1.10. *Je-li ohraničený svaz zároveň distributivní, pak v něm má každý prvek nejvýše jeden komplement.*

Důkaz. Ponechán jako cvičení čtenáři. □

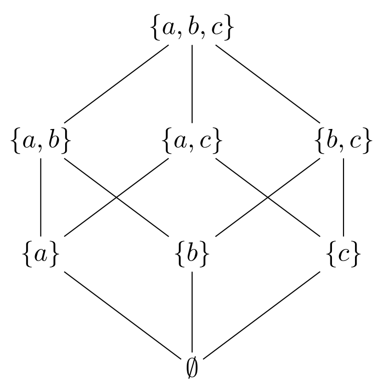
1.5.4 Booleův svaz (Booleova algebra)

Svaz $(M, \sqcap, \sqcup)$ je Booleův svaz, pokud splňuje následující dvě podmínky:

1. je *distributivní* a
2. je *komplementární*.

Příklad 1.14

1. Uvažujme množinový svaz daný následujícím Hasseovým diagramem:



Tento svaz *je* Booleův.

2. Uvažujme následující svaz pravdivostních hodnot výrokové logiky:

Opět jde o Booleův svaz. Infimum odpovídá konjunkci, supremum disjunkci a komplement negaci. Supremum svazu je *true* a infimum svazu je *false*.

Z komplementarity, distributivity a Věty 1.10 plyne, že každý prvek v $(M, \sqcap, \sqcup)$ má právě jeden komplement. Díky tomu lze Booleův svaz chápat též jako tzv. *Booleovu algebru* $(M, \sqcap, \sqcup, \overline{\cdot}, \bot, \top)$, kde

- $\sqcap$ a $\sqcup$ jsou binární operace (např. $x \sqcap y$),
- $\overline{\cdot}$ je unární operace (např. $\overline{x}$) a
- $\bot$, $\top$ jsou nulární operace, tedy konstanty.

Věta 1.11. *Nechť $A_M = (M, \sqcap, \sqcup, \overline{\cdot}, \bot, \top)$ je algebra s binárními operacemi $\sqcap$ a $\sqcup$, unární operací $\overline{\cdot}$ a dvěmi konstantami $\bot$ a $\top$. A_M je Booleova algebra právě tehdy, když pro všechna $x, y, z \in M$ platí následující podmínky:*

$$
\begin{array}{ccr}
x \sqcap (y \sqcap z) = (x \sqcap y) \sqcap z & x \sqcup (y \sqcup z) = (x \sqcup y) \sqcup z & \textbf{\textit{(asociativita)}} \\
x \sqcap y = y \sqcap x & x \sqcup y = y \sqcup x & \textbf{\textit{(komutativita)}} \\
x \sqcap (y \sqcup z) = (x \sqcap y) \sqcup (x \sqcap z) & x \sqcup (y \sqcap z) = (x \sqcup y) \sqcap (x \sqcup z) & \textbf{\textit{(distributivita)}} \\
x \sqcap \overline{x} = \bot & x \sqcup \overline{x} = \top & \textbf{\textit{(komplementarita)}} \\
x \sqcap \top = x & x \sqcup \bot = x & \textbf{\textit{(neutralita)}}
\end{array}
$$

Důkaz. Ponechán jako cvičení čtenáři. □

Věta 1.12. *Nechť $S_M = (M, \sqcap, \sqcup)$ je konečný svaz. S_M je Booleův svaz právě tehdy, když existuje konečná množina P taková, že S_M je izomorfní s Booleovým množinovým svazem $(2^P, \cap, \cup)$.*

Důkaz. Nad rámec tohoto textu, zájemci mohou najít v literatuře. □

Důsledek 1.13. *Je-li $(M, \sqcap, \sqcup)$ Booleova algebra, pak $M = 2^n$ kde $n \in \mathbb{N}$.*

Cvičení 1.5

1. Dokažte, že v Booleově algebře $(M, \sqcap, \sqcup, \overline{\cdot}, \bot, \top)$ platí tzv. *De Morganovy zákony*, tj., pro všechna $x, y \in M$,

$$\overline{x \sqcap y} = \overline{x} \sqcup \overline{y} \qquad \text{a} \qquad \overline{x \sqcup y} = \overline{x} \sqcap \overline{y}\ .$$