6. Okruhy a pole

Definice 6.0.1. Množina P se dvěmi binárními operacemi + a · je *okruh*, jestliže
(1) + a · jsou asociativní a komutativní operace,
(2) + má neutrální prvek, značíme ho 0,
(3) · má neutrální prvek různý od 0, značíme ho 1,
(4) ke každému prvku x existuje inverzní prvek vzhledem k operaci +,
(5) pro libovolné $x, y, z \in P$ platí $x \cdot (y + z) = x \cdot y + x \cdot z$.
Pokud navíc
(6) ke každému prvku $x \neq 0$ existuje inverzní prvek vzhledem k operaci ·,
množina P s operacemi + a · je *pole*.

Inverzní prvek k x vzhledem k operaci + se nazývá *opačný* k x a značí se $-x$. Inverzní prvek k x vzhledem k operaci · se značí x^{-1}.

Podmínka (5) v předchozí definici je *distributivní zákon*.

Příklad. (1) Množiny $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ s operacemi sčítání a násobení jsou pole.

(2) Množina $\mathbb{Z}$ s operacemi sčítání a násobení je okruh, ale není pole.

(3) Množina $\mathbb{N}_0$ s operacemi sčítání a násobení není okruh.

(4) Množina $P[x]$ s operacemi sčítání a násobení polynomů je okruh, ale není pole.

(5) Množina $\mathcal{M}_n(P)$ s operacemi sčítání a násobení matic není okruh.

(6) Nechť $P = \{0, 1\}$ a binární operace + a · na P jsou takové, že

+	0	1
0	0	1
1	1	0

a

·	0	1
0	0	0
1	0	1

Pro operaci + neutrální prvek je 0 a inverzní (opačné) prvky jsou $-0 = 0$ a $-1 = 1$. Pro operaci · neutrální prvek je 1 a inverzní prvek k 1 je 1 ($1^{-1} = 1$), inverzní prvek k 0 neexistuje. Množina $\{0, 1\}$ s těmito operacemi je pole.

(7) Nechť $P = \{0, 1, 2, 3\}$ a binární operace + a · na P jsou takové, že

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

a

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Potom neutrální prvek operace + je 0, neutrální prvek operace · je 1 a

$-0 = 0$ a 0^{-1} neexistuje
$-1 = 3$ a $1^{-1} = 1$
$-2 = 2$ a 2^{-1} neexistuje
$-3 = 1$ a $3^{-1} = 3$

Množina $\{0, 1, 2, 3\}$ s těmito operacemi je okruh, ale není pole. □

Tvrzení 6.0.1. *Buď P okruh. Pak pro libovolné prvky $x, y, z \in P$ platí*

(i) $x \cdot 0 = 0$;
(ii) $x \cdot (-1) = -x$;
(iii) $x \cdot (y - z) = x \cdot y - x \cdot z$.

Důkaz. (i) Platí

$$x \cdot 0 = x \cdot (0 + 0) = \\ = x \cdot 0 + x \cdot 0$$

a po přičtení $-(x \cdot 0)$ k oběma stranám rovnosti dostaneme $0 = x \cdot 0$.
(ii) Platí

$$0 = x \cdot 0 = x \cdot (1 + (-1)) = x \cdot 1 + x \cdot (-1) = \\ = x + x \cdot (-1)$$

a po přičtení $-x$ k oběma stranám rovnosti dostaneme $-x = x \cdot (-1)$.
(iii) Cvičení. □

Cvičení. Dokažte, že v každém okruhu platí:
(1) $(-1) \cdot (-1) = 1$,
(2) $(-x) \cdot y = x \cdot (-y) = -(x \cdot y)$. □

Tvrzení 6.0.2. *Buď P pole a buďte $x, y, z \in P$.*
(1) $x \cdot y = 0$ právě tehdy, když $x = 0$ nebo $y = 0$.
(2) Jestliže $x \cdot y = x \cdot z$ a $x \neq 0$, pak $y = z$.

Důkaz. (1) Jestliže $x = 0$ nebo $y = 0$, pak podle Tvrzení 6.0.1(i) také $x \cdot y = 0$.
Nechť $x \cdot y = 0$. Předpokládejme, že jeden z prvků x, y je nenulový, například $x \neq 0$. Potom s využitím Tvrzení 6.0.1(i) dostaneme

$$y = 1 \cdot y = (x^{-1} \cdot x) \cdot y = x^{-1} \cdot (x \cdot y) = x^{-1} \cdot 0 = 0.$$

(2)

$xy = xz$	k oběma stranám přičteme $-xz$
$xy - xz = 0$	použijeme (iii) z předchozího tvrzení
$x(y - z) = 0$	použijeme první část tvrzení a $x \neq 0$
$y - z = 0$	k oběma stranám přičteme z
$y = z$	

□

Příklad. (1) V příkladu (7) máme okruh, v němž $2 \cdot 2 = 0$ a $2 \cdot 1 = 2 \cdot 3$. To ukazuje, že předchozí tvrzení neplatí pro okruhy.
(2) Pro okruh $P[x]$ ale předchozí tvrzení platí, viz kapitolu o polynomech. □

Obdobně jako v kapitole 5 P^* označuje množinu $P \setminus \{0\}$.

Je-li P okruh, pak P s operací $+$ je komutativní grupa. Pro pole máme navíc následující tvrzení.

Tvrzení 6.0.3. *Je-li P pole, pak P^* s operací $\cdot$ je komutativní grupa.*

Důkaz. Buďte $x, y \in P^*$, tedy $x \neq 0$ a $y \neq 0$. Podle Tvrzení 6.0.2(i) $x \cdot y \neq 0$, tedy $x \cdot y \in P^*$, a množina P^* je uzavřená vzhledem k operaci $\cdot$. Zbytek tvrzení plyne z toho, že operace $\cdot$ je asociativní a komutativní, $1 \in P^*$ je neutrální prvek, každý nenulový prvek je invertibilní a příslušné inverze jsou nenulové. □

Tvrzení 6.0.4. *Množina $\mathbb{Z}_m$ zbytkových tříd je pole právě tehdy, když m je prvočíslo.*

Důkaz. Číslo 1 není prvočíslo a $\mathbb{Z}_1$ není pole (cvičení). Buď $m > 1$. Podle kapitol 5.5 a 5.6 $\mathbb{Z}_m$ splňuje podmínky (1)–(4) z definice okruhu a pole. Ověření, že platí distributivní zákon (5), ponecháme jako cvičení. Zbývá ukázat, že ke každému prvku $[x]_m \neq [0]_m$ existuje inverzní prvek vzhledem k operaci $\cdot$ právě tehdy, když m je prvočíslo.

Předpokládejme, že ke každému prvku $[x]_m \neq [0]_m$ existuje inverze. Podle Tvrzení 5.6.1 každé takové x je nesoudělné s m, tedy m je prvočíslo.

Na druhou stranu, je-li m prvočíslo, pak každé $x \in \mathbb{Z}$ takové, že $[x]_m \neq [0]_m$, je nesoudělné s m. Opět podle Tvrzení 5.6.1 $[x]_m$ má inverzi.

Jiný důkaz tohoto tvrzení lze nalézt v [Marvan, 3. Pole]. □

Takže, například, $\mathbb{Z}_4$ není pole. Čtyřprvkové pole ale existuje.

Příklad. Nechť $X = \{0, 1, a, b\}$ a binární operace + a $\cdot$ na X jsou takové, že

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

a

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Množina X s těmito operacemi + a $\cdot$ je pole. □

Poznámka. Buď n libovolné přirozené číslo. Potom existuje n-prvkové pole právě tehdy, když n je mocnina prvočísla, čili $n = p^k$, kde p je prvočíslo a k je přirozené číslo.

Stejně jako máme podgrupy grup (a podstruktury dalších algebraických struktur), existují podokruhy okruhů a podpole polí. Zmíníme jen podpole.

Definice 6.0.2. Buď P pole. Buď $Q \subseteq P$ podmnožina taková, že
(1) $0, 1 \in Q$;
(2) je-li $x, y \in Q$, pak $x + y \in Q$ a $xy \in Q$;
(3) je-li $x \in Q$, pak $-x \in Q$;
(4) je-li $x \in Q$, $x \neq 0$, pak $x^{-1} \in Q$.
Potom Q je *podpole* pole P.

Aby podmnožina pole byla podpole, musí obsahovat neutrální prvky obou binárních operací, musí být uzavřená vzhledem k oběma binárním operacím a musí být uzavřená vzhledem k inverzím vzhledem k oběma binárním operacím.

Každé podpole je pole.

Příklad. (1) Pole $\mathbb{Q}$ je podpole polí $\mathbb{R}$ a $\mathbb{C}$. Pole $\mathbb{R}$ je podpole pole $\mathbb{C}$.

(2) $\mathbb{Z}$ není podpole pole $\mathbb{Q}$, neboť neobsahuje inverzi k 2 vzhledem k operaci $\cdot$.

(3) Množina $\{0, 1\}$ není podpole pole $\mathbb{Q}$ (a samozřejmě ani $\mathbb{R}$ a $\mathbb{C}$), protože $1 + 1 = 2 \notin \{0, 1\}$. Ačkoliv, jak už víme, na množině $\{0, 1\}$ lze definovat operace sčítání a násobení tak, že to je pole. □

Definice 6.0.3. Podpole pole $\mathbb{C}$ je *číselné pole*.

7. Uspořádání a svazy

7.1. Uspořádané množiny

Definice 7.1.1. Relace ρ na množině X je *uspořádání*, jestliže je
(1) reflexivní, tj. $x \rho x$ pro každé $x \in X$,
(2) antisymetrická, tj. $x \rho y$, $y \rho x$ implikuje $x = y$,
(3) tranzitivní, tj. $x \rho y$, $y \rho z$ implikuje $x \rho z$.
Potom dvojice (X, ρ) je *uspořádaná množina*.

Příklad. (1) Pro libovolnou množinu X relace $=$ je uspořádání.

(2) $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$ $(\mathbb{R}, \leq)$, kde $\leq$ je obvyklé uspořádání podle velikosti, jsou uspořádané množiny.

(3) Buďte X množina a $\mathcal{P}(X)$ množina všech podmnožin množiny X. Inkluze $\subseteq$ je uspořádání na $\mathcal{P}(X)$.

(4) Relace $|$ (dělí) na množině $\mathbb{N}$ (tj. $x \mid y$ právě tehdy, když existuje $n \in \mathbb{N}$ takové, že $x \cdot n = y$) je uspořádání, nazývá se *relace dělitelnosti*. Je zřejmé, že tato relace je reflexivní a tranzitivní.

Ukážeme, že $|$ je i antisymetrická relace. Předpokládejme, že $x \mid y$ a $y \mid x$, tedy existují $m, n \in \mathbb{N}$ taková, že $xm = y$ a $yn = x$. Potom $xmn = x$ a jelikož $x \neq 0$, $mn = 1$. V přirozených číslech to lze jedině tak, že $m = 1$ a $n = 1$. Tedy $x = x \cdot 1 = y$.

Upozorňeme, že obdobně definovaná relace dělitelnosti na $\mathbb{Z}$ není antisymetrická, protože $1 \neq -1$, přestože $1 \mid -1$ a $-1 \mid 1$ (rovnice $mn = 1$ má v celých číslech další řešení $m = -1$ a $n = -1$). □

Buď ρ uspořádání na množině X. Inverzní (opačná) relace ρ^{-1} (tj. relace definovaná předpisem „$x \rho^{-1} y$ právě tehdy, když $y \rho x$“) je také uspořádání. Nazývá se *duální uspořádání*. Máme-li uspořádání $\leq$, potom duální uspořádání $\leq^{-1}$ se označuje symbolem $\geq$. Podobně je to se symboly $\subseteq$ atp.

Definice 7.1.2. Buď $(X, \leq)$ uspořádaná množina, $Y \subseteq X$. Relace $\leq_Y$ na množině Y zadaná předpisem $x \leq_Y y \Leftrightarrow x \leq y$ je uspořádání na množině Y. Nazývá se *indukované uspořádání* a značí se rovněž $\leq$.

Definice 7.1.3. Prvky x, y uspořádané množiny jsou *srovnatelné*, platí-li $x \leq y$ nebo $y \leq x$. Uspořádaná množina je *řetězec*, jsou-li každé dva její prvky srovnatelné.

Příklad. $(\mathbb{R}, \leq)$, $(\mathbb{Z}, \leq)$ $(\mathbb{N}, \leq)$ jsou řetězce. □

Buď $\leq$ uspořádání na X. Označme $x < y$, jestliže $x \leq y$ a zároveň $x \neq y$. Dále zaveďme označení $x \lhd y$, jestliže $x < y$ a neexistuje $z \in X$ takové, že $x < z$, $z < y$. Je-li $x \lhd y$, pak říkáme, že x je *bezprostředním předchůdcem* y, nebo y *pokrývá* x.

Příklad. (1) V množině $\mathbb{N}$ s přirozeným uspořádáním podle velikosti platí $1 < 2$ a $1 \lhd 2$, $1 < 3$, ale neplatí $1 \lhd 3$.

(2) V množině $\mathbb{N}$ s relací dělitelnosti 6 pokrývá 3.

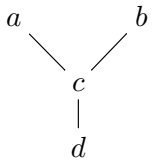
(3) V množině $\mathbb{Q}$ všech racionálních čísel s přirozeným uspořádáním podle velikosti neplatí $x \lhd y$ pro žádnou dvojici $x, y \in \mathbb{Q}$. Pro libovolné $x, y \in \mathbb{Q}$ takové, že $x < y$, platí $z = \frac{1}{2}(x + y) \in \mathbb{Q}$ a $x < z$, $z < y$. □

Konečnou uspořádanou množinu $(X, \leq)$ můžeme znázornit diagramem. Prvky množiny X znázorníme jako body v rovině. Prvky x, y splňující $x \lhd y$ vyznačíme tak, že x leží níže než y a spojíme je úsečkou.

Z diagramu pak můžeme určit uspořádání množiny X: $x \leq y$ právě tehdy, když x leží níže než y a existuje zdola nahoru směřující konečná posloupnost na sebe navazujících úseček z bodu x do bodu y.

Příklad. V uspořádané množině $Y = \{a, b, c, d\}$ s diagramem vpravo platí:

- $d \lhd c$, $c \lhd a$, $c \lhd b$,
- $d < a$, ale nikoliv $d \lhd a$,
- prvky a, b nejsou srovnatelné.



□

Definice 7.1.4. Buď $(X, \leq)$ uspořádaná množina, $Y \subseteq X$. Prvek $x \in X$ je

- *dolní závora* množiny Y, je-li $x \leq y$ pro každé $y \in Y$;
- *horní závora* množiny Y, je-li $y \leq x$ pro každé $y \in Y$.

Příklad. V uspořádané množině Y z předchozího příkladu platí:

- c, d jsou dolní závory podmnožiny $\{a, b\}$,
- podmnožina $\{a, b\}$ nemá žádnou horní závoru. □

Definice 7.1.5. Buď $(X, \leq)$ uspořádaná množina. Prvek $x \in X$ je

- *nejmenší* (*minimální*) prvek množiny X, je-li $x \leq y$ pro každé $y \in X$, v takovém případě píšeme $x = \min X$;
- *největší* (*maximální*) prvek množiny X, je-li $x \geq y$ pro každé $y \in X$, v takovém případě píšeme $x = \max X$.

Příklad. V uspořádané množině Y z předchozího příkladu platí:

- d je její nejmenší prvek,
- její největší prvek neexistuje. □

Cvičení. Každá uspořádaná množina má nejvýše jeden největší prvek a nejvýše jeden nejmenší prvek. □

Definice 7.1.6. Buď $(X, \leq)$ uspořádaná množina, $Y \subseteq X$. Prvek $x \in X$ je

- *infimum* množiny Y, je-li x největší prvek množiny všech dolních závor množiny Y, v takovém případě píšeme $x = \inf Y$,
- *supremum* množiny Y, je-li x nejmenší prvek množiny všech horních závor množiny Y, v takovém případě píšeme $x = \sup Y$.

Příklad. V uspořádané množině Y z předchozího příkladu platí:

- množina dolních závor podmnožiny $\{a, b\}$ je $\{c, d\}$, její největší prvek je c, a proto $\inf\{a, b\} = c$,
- podmnožina $\{a, b\}$ nemá žádnou horní závoru, čili množina horních závor je prázdná, nemá tedy největší prvek, a proto $\sup\{a, b\}$ neexistuje. □

Cvičení. (1) Každá podmnožina má nejvýše jedno supremum a nejvýše jedno infimum.

(2) Jestliže $x \leq y$, pak $\inf\{x, y\} = x$ a $\sup\{x, y\} = y$.

(3) Jestliže $\inf\{x, y\} = x$, pak $x \leq y$.

(4) Jestliže $\sup\{x, y\} = y$, pak $x \leq y$. □

Cvičení. Buď X uspořádaná množina. Supremum prázdné množiny je nejmenší prvek množiny X (pokud existuje) a infimum prázdné množiny je největší prvek množiny X (pokud existuje). □

7.2. Svazově uspořádané množiny a svazy

Definice 7.2.1. Uspořádaná množina je *svazově uspořádaná*, jestliže každá její dvouprvková podmnožina má infimum i supremum.

Každá konečná podmnožina svazově uspořádané množiny má infimum i supremum.

Příklad. (1) Pro libovolnou množinu X je $(\mathcal{P}(X), \subseteq)$ svazově uspořádaná množina, přičemž pro libovolné $Y, Z \in \mathcal{P}(X)$ $\inf\{Y, Z\} = Y \cap Z$ a $\sup\{Y, Z\} = Y \cup Z$.

(2) $(\mathbb{N}, |)$ je svazově uspořádaná množina, přičemž $\inf\{x, y\}$ je největší společný dělitel čísel x, y, $\sup\{x, y\}$ je nejmenší společný násobek čísel x, y.

(3) $(\{1, 3, 5, 6, 9, 10, 12\}, |)$ není svazově uspořádaná množina.

(4) Každý řetězec je svazově uspořádaná množina, přičemž $\inf\{x, y\} = \min\{x, y\}$ je menší z prvků x, y, $\sup\{x, y\} = \max\{x, y\}$ je větší z prvků x, y. □

Definice 7.2.2. Množina X se dvěma binárními operacemi $\wedge$ a $\vee$ je *svaz*, jestliže pro každé $x, y, z \in X$ platí

$x \wedge y = y \wedge x$,	$x \vee y = y \vee x$,	(komutativita $\wedge$ a $\vee$)
$(x \wedge y) \wedge z = x \wedge (y \wedge z)$,	$(x \vee y) \vee z = x \vee (y \vee z)$,	(asociativita $\wedge$ a $\vee$)
$x \wedge (y \vee x) = x$,	$x \vee (y \wedge x) = x$.	(zákon absorpce)

Binární operace $\wedge$ je *průsek*, binární operace $\vee$ je *spojení*.

Příklad. (1) Pro libovolnou množinu X množina $\mathcal{P}(X)$ s operacemi $\cap$ a $\cup$ je svaz.

(2) Množina $\mathbb{N}$ s operacemi D a N, kde $x \,\mathrm{D}\, y$ je největší společný dělitel čísel x, y a $x \,\mathrm{N}\, y$ je nejmenší společný násobek čísel x, y, je svaz.

(3) Množina $\mathbb{R}$ s operacemi min a max je svaz.

(4) Množina $\{0, 1\}$ pravdivostních hodnot s operacemi konjunkce a disjunkce je svaz. □

Tvrzení 7.2.1. *Buď $(X, \wedge, \vee)$ svaz. Pro libovolné $x \in X$ platí*

$$x \wedge x = x, \qquad x \vee x = x. \qquad \textit{(idempotentnost } \wedge \textit{ a } \vee\textit{)}$$

Důkaz.

$$\begin{aligned} x \wedge x &= && \text{(zákon absorpce)} \\ &= x \wedge (x \vee (y \wedge x)) = && \text{(komutativita } \vee\text{)} \\ &= x \wedge ((y \wedge x) \vee x) = && \text{(zákon absorpce)} \\ &= x. \end{aligned}$$

Druhou část tvrzení necháme jako cvičení. □

Ve svazově uspořádané množině X pro každé x, y existují $\inf\{x, y\}$ a $\sup\{x, y\}$ a jsou jednoznačně určena, proto můžeme na X definovat binární operace $\wedge$ a $\vee$:

$$x \wedge y := \inf\{x, y\}, \quad x \vee y := \sup\{x, y\}.$$

Podle následujícího tvrzení každá svazově uspořádaná množina s těmito operacemi je svaz.

Tvrzení 7.2.2. *Svazově uspořádaná množina X s binárními operacemi $\wedge$, $x \wedge y = \inf\{x, y\}$, a $\vee$, $x \vee y = \sup\{x, y\}$, je svaz.*

Důkaz. Cvičení.
Asociativita $\vee$: Návod: Ukažte, že $x \vee (y \vee z) = \sup\{x, y, z\} = (x \vee y) \vee z$. □

Cvičení. Dokažte, že $x_1 \vee x_2 \vee \cdots \vee x_n = \sup\{x_1, x_2, \ldots, x_n\}$. (Vlevo nezáleží na uzávorkování). □

Podle následujícího tvrzení každý svaz je svazově uspořádaná množina.

Tvrzení 7.2.3. *Buď $(X, \wedge, \vee)$ svaz.*

(1) Položme $x \leq_\wedge y$ právě tehdy, když $x \wedge y = x$. Pak $\leq_\wedge$ je uspořádání na X.

(2) Položme $x \leq_\vee y$ právě tehdy, když $x \vee y = y$. Pak $\leq_\vee$ je uspořádání na X.

(3) Uspořádání $\leq_\wedge$ je shodné s uspořádáním $\leq_\vee$ a $(X, \leq_\wedge)$ je svazově uspořádaná množina, přičemž

$$\inf\{x, y\} = x \wedge y, \quad \sup\{x, y\} = x \vee y.$$

Důkaz. Cvičení. □

Svazy i svazově uspořádané množiny tedy můžeme chápat jak jako algebraické struktury tak jako uspořádané množiny. Uspořádání totiž jednoznačně určuje algebraickou strukturu a algebraická struktura zase jednoznačně určuje uspořádání.

Buď $(X, \wedge, \vee)$ svaz. Identity v definici svazu jsou symetrické vzhledem k vzájemné záměně $\wedge$ a $\vee$, proto $(X, \vee, \wedge)$ je také svaz. Nazývá se *duální svaz* a značí se X^*.

Cvičení. Ověřte, že duální svaz má duální uspořádání. □

Tvrzení 7.2.4. *Buď X svaz. Pro každé $x, a, b \in X$ platí*

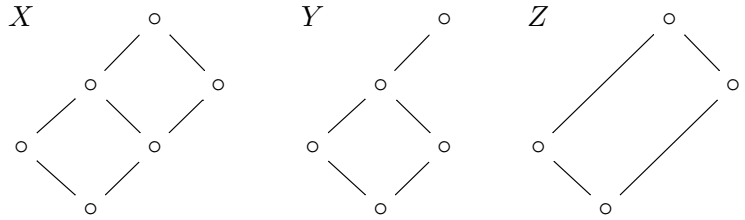
(i) jestliže $a \leq b$, pak $a \wedge x \leq b \wedge x$;
(ii) jestliže $a \leq b$, pak $a \vee x \leq b \vee x$;
(iii) jestliže $x \leq a$, $x \leq b$, pak $x \leq a \wedge b$;
(iv) jestliže $x \geq a$, $x \geq b$, pak $x \geq a \vee b$.

Důkaz. (i) Nechť $a \leq b$, pak $a \wedge b = a$, načež $(a \wedge x) \wedge (b \wedge x) = a \wedge b \wedge x = a \wedge x$; odtud tvrzení. (ii) Cvičení. (iii) a (iv) plynou ihned z definice infima a suprema (cvičení). □

Obsahuje-li podmnožina svazu všechna infima a suprema všech dvojic svých prvků, je to také svaz.

Definice 7.2.3. *Podsvaz* svazu $(X, \wedge, \vee)$ je podmnožina $Y \subseteq X$ taková, že pro každé $x, y \in Y$ platí $x \wedge y \in Y$ a $x \vee y \in Y$.

Příklad. Svaz X a jeho podsvazy Y a Z:



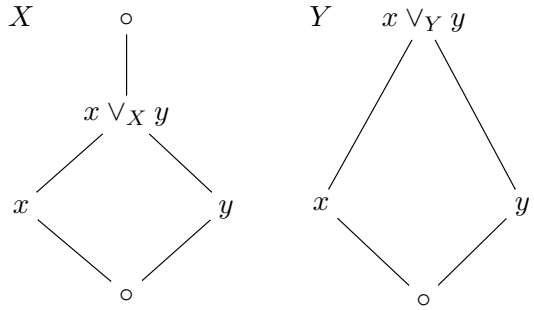
□

Cvičení. (1) Každá podmnožina řetězce je podsvaz.

(2) Každá podmnožina svazu, která je řetězcem, je podsvaz. □

Podmnožina svazu může být svazem vzhledem k indukovanému uspořádání, aniž by byla podsvazem.

Příklad. Svaz X a jeho podmnožina Y, která je svazem, ale není podsvazem.



Supremum $x \vee_Y y$ v Y je různé od suprema $x \vee_X y$ v X. □

7.3. Úplné svazy

Definice 7.3.1. Svaz je *úplný*, má-li každá jeho podmnožina supremum i infimum.

Příklad. (1) Každý konečný svaz je úplný a platí $\inf\{x_1, x_2, \ldots, x_n\} = x_1 \wedge x_2 \wedge \ldots \wedge x_n$, $\sup\{x_1, x_2, \ldots, x_n\} = x_1 \vee x_2 \vee \ldots \vee x_n$.

(2) Svaz $(\mathcal{P}(M), \subseteq)$ je úplný. Infima jsou průniky, suprema jsou sjednocení.

(3) Svaz $(\mathbb{N}, \leq)$ není úplný. Schází například supremum celé množiny $\mathbb{N}$. □

Každý úplný svaz má největší prvek, je to jeho supremum, i nejmenší prvek, je to jeho infimum.

Tvrzení 7.3.1. *Buď X uspořádaná množina, jejíž každá podmnožina má infimum. Pak X je úplný svaz.*

Důkaz. Stačí ukázat, že každá podmnožina má supremum. Buď $Y \subseteq X$. Označme Z množinu všech horních závor množiny Y a položme $s = \inf Z$. Dokažme, že $s = \sup Y$.

Každý prvek množiny Z je horní závora množiny Y, takže každý prvek množiny Y je dolní závora množiny Z. Jelikož s je největší dolní závora množiny Z, tak $y \leq s$ pro každé $y \in Y$, čili s je zároveň horní závora množiny Y. A když $s \in Z$ a současně s je (největší) dolní závora množiny Z, je to nejmenší prvek množiny Z, čili nejmenší horní závora množiny Y. □

Příklad. Předpoklad, že každá (i prázdná) podmnožina množiny X má infimum, znamená, že X má největší prvek. Například $(\mathbb{N}, \leq)$ není úplný svaz, přestože každá *neprázdná* podmnožina má infimum. □

Příklad. Buď G grupa. Označme $P(G)$ množinu všech podgrup grupy G. Pak $(P(G), \subseteq)$ je úplný svaz.

Buď $\{A_\iota \mid \iota \in I\} \subseteq P(G)$, tedy nějaký systém podgrup grupy G. Potom $\bigcap_{\iota \in I} A_\iota$ je také podgrupa (cvičení), která je zároveň $\inf\{A_\iota \mid \iota \in I\}$ (cvičení). Podle předchozího tvrzení je $(P(G), \subseteq)$ úplný svaz. Proto existuje i $\sup\{A_\iota \mid \iota \in I\}$ a je to průnik všech podgrup, které obsahují všechny podgrupy A_ι.

Příklad je zformulován pro grupy, ale jeho analogie platí i pro jiné algebraické struktury. □

Cvičení. Označme $E(X)$ množinu všech relací ekvivalence na množině X. Protože $E(X) \subset \mathcal{P}(X \times X)$, vzniká na $E(X)$ indukované uspořádání. Dokažte, že $E(X)$ je úplný svaz. □