1. Teorie svazů

1.1. Svazy

▶ 1.1.1. Definice. Svazem (angl. lattice) rozumíme algebru $S = (M, \wedge, \vee)$ se dvěma binárními operacemi takovou, že pro libovolné $a, b, c \in M$ platí:

(1) $a \wedge b = b \wedge a, \quad a \vee b = b \vee a$ (komutativní zákon);

(2) $(a \wedge b) \wedge c = a \wedge (b \wedge c), \quad (a \vee b) \vee c = a \vee (b \vee c)$ (asociativní zákon);

(3) $a \wedge (b \vee a) = a, \quad a \vee (b \wedge a) = a$ (zákon absorpce).

Operaci $\wedge$ nazýváme průsek a operaci $\vee$ spojení.

▶ 1.1.2. Lemma. Ve svazu $S = (M, \wedge, \vee)$ platí pro libovolný prvek $a \in M$, že $a \wedge a = a$ a $a \vee a = a$ (tzv. idempotentnost)

◦ *Důkaz.* $a \wedge a = a \wedge (a \vee (b \wedge a)) = a$, druhá rovnost symetricky. □

▶ 1.1.3. Věta (princip duality v teorii svazů). Máme-li formuli v teorii svazů, která platí ve všech svazech, pak duální formule vzniklá prohozením operací průseku a spojení opět platí ve všech svazech.

1.2. Svazově uspořádaná množina

▶ 1.2.1. Poznámka. Připomeneme důležité pojmy pro uspořádané množiny $(M, \leq)$.

(1) Horní závora množiny $A \subseteq M$ je každé takové $a \in M$, že $(\forall x \in A)(x \leq a)$.

(2) Má-li množina horních závor první prvek, nazveme jej supremum A. Pro $s = \sup A$ platí:

(a) $(\forall a \in A)(a \leq s)$;
(b) $\big(\forall t \in M\big)\big((\forall a \in A)(a \leq t) \Rightarrow s \leq t\big)$.

(3) $\sup \emptyset$ je první prvek množiny M (pokud existuje).

(4) $\sup M$ je poslední prvek množiny M (pokud existuje).

▶ 1.2.2. Definice. Řekneme, že uspořádaná množina $(M, \leq)$ je svazově uspořádaná, má-li v ní libovolná 2prvková množina infimum a supremum.

▶ 1.2.3. Lemma. Pro libovolné prvky svazu platí, že

$$a \wedge b = a \iff a \vee b = b.$$

◦ *Důkaz.*

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

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

□

► 1.2.4. Věta.

(1) Buď $S = (M, \wedge, \vee)$ svaz. Definujeme-li na M binární relaci $\leq$ jako $a \leq b \Leftrightarrow a \wedge b = a$, pak $(M, \leq)$ je svazově uspořádaná.

(2) Buď $(M, \leq)$ svazově uspořádaná množina. Definujeme-li na M binární operace $\wedge, \vee$ jako $a \wedge b := \inf\{a, b\}$ a $a \vee b := \sup\{a, b\}$, pak $(M, \wedge, \vee)$ je svazem.

◦ *Důkaz.*

(1) **(reflexivita)** $a \leq a \Leftrightarrow a \wedge a = a$.

(antisymetrie) $a \wedge b = a$ a $b \wedge a = b$, a z komutativity plyne $a = b$.

(transitivita) Nechť $a \leq b$ a $b \leq c$, pak $a \wedge c = a \wedge b \wedge c = a \wedge b = a$.

(je svazové) Ukážeme, že $\inf\{a, b\} = a \wedge b$. Obdobně $\sup\{a, b\} = a \vee b$.

(2) **(komutativita)** $a \wedge b = \inf\{a, b\} = \inf\{b, a\} = b \wedge a$.

(asociativita) $(a \wedge b) \wedge c = \inf\{\inf\{a, b\}, c\} = \inf\{a, b, c\} = \inf\{a, \inf\{b, c\}\} = a \wedge (b \wedge c)$ s využitím následujícího lemmatu a faktu, že každá 2prvková má infimum.

(pohlcení) $\inf\{a, \sup\{b, a\}\} = a$ z definice.

Druhý z každé dvojice axiomů dokážeme podobně.

□

► 1.2.5. Lemma. Mějme uspořádanou množinu $(M, \leq)$ a $a, b, c \in M$. Potom pokud existuje $\inf\{\inf\{a, b\}, c\} =: i$, je $i = \inf\{a, b, c\}$. Pokud je navíc $(M, \leq)$ svazově uspořádaná, platí $i = \inf\{a, \inf\{b, c\}\}$.

◦ *Důkaz.*

($i \leq a, b, c$) Je $i \leq c$ a $i \leq \inf\{a, b\}$, tedy $i \leq a, b$.

($d \leq a, b, c \Rightarrow d \leq i$) Neboť $d \leq a$ a $d \leq b$, je $d \leq \inf\{a, b\}$ a současně je $d \leq c$, tedy $d \leq \inf\{c, \inf\{a, b\}\} = i$

Pokud je navíc uspořádaní svazové, pak existuje infimum 2prvkové množiny $\{b, c\}$ a také infimum 2prvkové množiny $\{a, \inf\{b, c\}\}$. A tedy je podle prvního tvzení $\inf\{a, \inf\{b, c\}\} = \inf\{a, b, c\} = i$. □

► 1.2.6. Poznámka. Operace jsou jednoznačně svázané, neboť např. pomocí $\wedge$ definujeme $\leq$ a to nám definuje $\vee$.

► 1.2.7. Lemma. Buď $S = (M, \wedge, \vee)$ svaz a nechť $a, b, c \in M$. Potom platí

$$(a \leq b) \Rightarrow (a \wedge c \leq b \wedge c \text{ et } a \vee c \leq b \vee c).$$

◦ *Důkaz.* Z definice: $a \wedge c \wedge b \wedge c = a \wedge c$, $a \vee c \vee b \vee c = b \vee c$. □

► 1.2.8. Definice. Mějme svaz $S = (M, \wedge, \vee)$. Pak pro $N \subseteq M$ je $T = (N, \wedge, \vee)$ podsvazem svazu S, pokud je T svazem, tj. pokud je N neprázdná a uzavřená vůči oběma operacím.

► 1.2.9. Příklad.

(1) Množinový svaz $S = (M, \cap, \cup)$, kde M je systém množin uzavřený na operace. Speciálním případem je $M = \mathcal{P}(A)$, kde snadno ověříme platnost axiomů svazu. Svazové uspořádání množinového svazu je inkluze $\subseteq$.

Mějme A množinu a $B \subseteq A$ její podmnožinu. Pak $(\mathcal{P}(B), \cap, \cup)$ je podsvazem svazu $(\mathcal{P}(A), \cap, \cup)$.

Dále např. ς-algebry tvoří množinové svazy.

(2) Pro libovolné $a \in S^\bullet$ je $(\{a\}, \wedge, \vee)$ podsvazem S.

Pro libovolné $a, b \in S^\bullet$ je $(\{a, b\}, \wedge, \vee)$ podvazem S, pokud jsou srovnatelné.

(3) Úplně uspořádaná množina je uspořádaná svazově a supremum a infimum přechází v maximum a minimum (vždy to bude jeden z obou prvků). Příkladem jsou číselné množiny $(\mathbb{N}_0, \leq)$ či $(\mathbb{R}, \leq)$.

(4) Mějme uspořádání $(\mathbb{N}_0, |)$ s uspořádáním „dělí“. Pak $k \wedge l$ je největší (podle $|$) takové d, že $d \,|\, k$ a $d \,|\, l$, tj. $k \wedge l = \delta(k, l)$. Obdobně $k \vee l = \nu(k, l)$.

(5) Mějme $G = (M, \cdot)$ grupu a označme M_G systém všech jejích podgrup. Označme $(\wedge) = (\cap)$. Pak umíme definovat $(\leq)$ jako $a \leq b \Leftrightarrow a \cap b = a \Leftrightarrow a \subseteq b$. Tedy průsek i relace jsou stejné jako v množinovém svazu, ale víme, že sjednocení nemůže být spojením. Definujeme ji $a \vee b := \sup\{a, b\}$, to je nejmenší podgrupa G obsahující a i b, což je ab. Tedy platí $(\vee) = (\cdot)$.

(6) $N_G = (N_G^\bullet, \cap, \cdot)$ je svaz všech normálních podgrup grupy G. Pak N_G je podsvazem svazu S_G.

(7) Podobně tvoří svazy systémy podokruhů, ideálů, podtěles, podprostorů vektorového prostoru, doplněné o průnik a součet.

► 1.2.10. Definice. Mějme $a, b \in S^\bullet$, $a < b$. Pak intervalem nazveme množinu $\langle a, b\rangle = \{x \,|\, a \leq x \leq b\}$.

► 1.2.11. Lemma. Interval $\langle a, b\rangle$ je podsvazem S.

◦ *Důkaz.* Mějme $x, y \in \langle a, b\rangle$. Ukážeme, že $x \wedge y \in \langle a, b\rangle$. Platí $x \geq a$ a $y \geq a$, tedy $x \wedge y \geq a \wedge y \geq a \wedge a = a$. Obdobně pro b a pro druhou operaci. □

•

1.3. Ideály

► 1.3.1. Definice. Buď $S = (M, \wedge, \vee)$ svaz. Ideálem rozumíme libovolný jeho podsvaz I takový, že platí

$$(\forall a \in I)(\forall s \in M)(a \wedge s \in I).$$

► 1.3.2. Lemma. Buďte $S = (M, \wedge, \vee)$ svaz a I jeho podsvaz. Následující tvrzení jsou ekvivalentní:

(1) $(\forall a \in I)(\forall s \in M)(a \wedge s \in I)$ (tj. I je ideál);

(2) $(\forall a \in I)(\forall b \in S)(b \leq a \Rightarrow b \in I)$;

(3) $(\forall a, b \in S)(a \vee b \in I \Rightarrow a, b \in I)$.

◦ *Důkaz.*

(1 ⇒ 2) Mějme $a \in I$ a $b \leq a$. Pak podle předpokladu $a \wedge b \in I$, ale současně $a \wedge b = b$, tedy $b \in I$.

(2 ⇒ 3) Buď $a \vee b \in I$. Platí $a \leq a \vee b$ a $b \leq a \vee b$ a podle (2) je $a \vee b \in I$.

(3 ⇒ 1) Mějme $a \in I$ a $s \in M$. Pak $a = a \vee (a \wedge s) \in I$, a tedy $a \wedge s \in I$.

□

► 1.3.3. Důsledek. Ideály ve svazu S jsou takové $I \subseteq M$, $I \neq \emptyset$, že platí $(\forall a, b \in M)(a, b \in I \Leftrightarrow a \vee b \in I)$.

► 1.3.4. Lemma. Buďte S svaz a $a \in M$. Pak množina $I_a := \{x \in M \mid x \leq a\}$ je ideálem.

◦ *Důkaz.* I_a je uzavřená vůči $\vee$ a platí (2) v 1.3.2. □

► 1.3.5. Definice. Ideál $I_a := \{x \in M \mid x \leq a\}$ nazýváme hlavní ideál generovaný prvkem a. Je-li ve svazu každý ideál hlavní, nazveme jej svaz hlavních ideálů.

► 1.3.6. Definice. Buď $S = (M, \wedge, \vee)$ svaz. Filtrem rozumíme libovolný jeho podsvaz F takový, že platí

$$(\forall a \in F)(\forall s \in M)(a \vee s \in F).$$

• 1.4. Izomorfismus svazů

► 1.4.1. Definice. Buďte $S_1 = (M_1, \wedge, \vee)$ a $S_2 = (M_2, \wedge, \vee)$ svazy. Zobrazení $h : M_1 \to M_2$ nazveme homomorfismus, platí-li

$$(\forall x, y \in M_1)(h(x \wedge y) = h(x) \wedge h(y) \text{ et } h(x \vee y) = h(x) \vee h(y)).$$

Izomorfismus je takový homomorfismus, který je bijektivní.

► 1.4.2. Lemma. Homomorfismus svazů je izotonní zobrazení.

◦ *Důkaz.* Mějme $h : S_1 \to S_2$ a $x, y \in S_1^{\bullet}$, $x \leq y$. Potom $h(x) \wedge h(y) = h(x \wedge y) = h(x)$, tedy $h(x) \leq h(y)$. □

► 1.4.3. Věta. Buďte $S_1 = (M_1, \wedge, \vee)$ a $S_2 = (M_2, \wedge, \vee)$ svazy. Zobrazení $h : M_1 \to M_2$ je izomorfismem svazů právě tehdy, je-li izomorfismem svazově uspořádaných množin.

◦ *Důkaz.* Pro obě implikace je předpokladem bijekce, a tedy existence h^{-1}.

(⇒) Podle předchozího lemmatu je $x \leq y \Rightarrow h(x) \leq h(y)$. Zbývá tedy opačná implikace. Předpokládejme $h(x) \wedge h(y) = h(x)$. Potom díky bijekci je $x \wedge y = x$, a tedy $x \leq y$.

(⇐) Platí $x \wedge y \leq x$, tedy $h(x \wedge y) \leq h(x)$ a $h(x \wedge y)$ je dolní závora $h(x)$ a podobně je dolní závorou $h(y)$. Mějme libovolné $d \in S_2^\bullet$ takové, že $d \leq h(x)$ a $d \leq h(y)$. Neboť h je bijekce, existuje $c \in S_1$ takové, že $h(c) = d$. Platí $h(c) \leq h(x)$ a $h(c) \leq h(y)$, čili $c \leq x$ a $c \leq y$, a tedy $c \leq \inf\{x, y\}$ a konečně $d = h(c) \leq h(x \wedge y)$. Tedy každá dolní závora $h(x), h(y)$ je nejvýše rovna $h(x \wedge y)$. Tedy $h(x) \wedge h(y) = h(x \wedge y)$. Obdobně ukážeme, že $h(x) \vee h(y) = h(x \vee y)$.

□

► 1.4.4. Definice. Má-li svaz nejmenší (první), resp. největší (poslední) prvek, nazveme jej nulou, resp. jednotkou a značíme 0, resp. 1.

► 1.4.5. Příklad.

(1) Mějme množinu A a množinový svaz $(\mathcal{P}(A), \cap, \cup)$ s uspořádáním $\subseteq$. Pak jednotkou je A a nulou je $\emptyset$.

(2) Mějme svaz $(\mathbb{N}_0, \delta, \nu)$ s uspořádáním $(|)$. Pak jednotkou je číslo 0 (platí $n \,|\, 0$) a nulou je číslo 1 (platí $1 \,|\, n$).

► 1.4.6. Lemma. Libovolný minimální prvek svazu je nulou. Libovolný maximální prvek svazu je jednotkou.

◦ *Důkaz.* Ukážeme pouze první tvrzení, druhé lze ukázat obdobně. Mějme m minimální a libovolné $x \in S^\bullet$. Pak $x \wedge m \leq m$, ale to je možné jen tehdy, když $x \wedge m = m$, a tedy $m \leq x$. Tedy m je první a je nulou. □

• 1.5. Úplné svazy

► 1.5.1. Definice. Svaz $S = (M, \wedge, \vee)$ nazveme úplným svazem, má-li v něm libovolná podmnožina $N \subseteq M$ infimum i supremum.

► 1.5.2. Poznámka. V každém svazu existuje infimum a supremum konečné podmnožiny. V úplném svazu vyžadujeme existenci infima a suprema pro každou (prázdnou, konečnou, spočetnou, nespočetnou) podmnožinu.

► 1.5.3. Lemma. Úplný svaz má nulu a jednotku.

◦ *Důkaz.*

(1) $1 = \sup M = \inf \emptyset$.

(2) $0 = \inf M = \sup \emptyset$.

□

► 1.5.4. Příklad. V množinovém svazu $S = (\mathcal{P}(M), \cap, \cup)$ je infimem $\mathcal{A} \subseteq \mathcal{P}(M)$ množina $\bigcap \mathcal{A} \subseteq M$ a supremem $\bigcup \mathcal{A} \subseteq M$, tedy S je úplný svaz.

► 1.5.5. Věta (o pevném bodě). Buď $S = (M, \wedge, \vee)$ úplný svaz a buď $f : M \to M$ izotonie. Pak existuje pevný bod izotonie f, tj.

$$(\exists u \in M)(f(u) = u).$$

◦ *Důkaz.* Definujeme $U = \{a \in M \mid f(a) \geq a\}$. Jistě $0 \in U$, tedy U je neprázdná. Označme $u := \sup U$. Mějme libovolné $a \in U$, pak $u \geq a$ a z izotonie je $f(u) \geq f(a) \geq a$, tedy $f(u)$ je horní závora U, a tedy $u \leq f(u)$. Z izotonie dále dostáváme, že $f(u) \leq f(f(u))$, a tedy $f(u) \in U$, tedy $f(u) \leq u$. Celkově máme $f(u) = u$. □

► 1.5.6. Věta. Buď $(M, \leq)$ uspořádaná množina. Má-li každá podmnožina M infimum, pak má každá podmnožina M supremum.

◦ *Důkaz.* Mějme $N \subseteq M$. Nechť Z je množina horních závor N. Dále $Z \neq \emptyset$, neboť v ní je největší prvek M, což je $\inf \emptyset$. Pokud $N = \emptyset$, pak $\sup N$ je $\inf M$.

Nyní máme $(\forall n \in N)(\forall z \in Z)(n \leq z)$. Tedy každý prvek N je dolní závorou Z a platí $n \leq \inf Z$, jehož existenci předpokládáme. A neboť $(\forall n \in N)(n \leq \inf Z)$, tedy $\inf Z$ je horní závora a je nemenší z nich. Tedy $\sup N = \inf Z$. □

► 1.5.7. Důsledek. Buď $(M, \leq)$ uspořádaná množina. Má-li každá podmnožina M supremum, pak má každá podmnožina M infimum.

► 1.5.8. Důsledek. Buď $(M, \leq)$ uspořádaná množina. Má-li každá podmnožina M infimum, nebo má-li každá podmnožina M supremum, pak $(M, \wedge, \vee)$ je úplný svaz.

► 1.5.9. Lemma. Buď $S = (M, \wedge, \vee)$ úplný svaz. Potom průnik libovolného systému ideálů v S je ideál v S.

◦ *Důkaz.* Označme J_α jednotlivé ideály a $I := \bigcap J_\alpha$. Neboť $0 \in M$ a $0 \in J_\alpha$, je $0 \in I$ a $I \neq \emptyset$. Dále platí $a \in I \Leftrightarrow (\forall \alpha)(a \in J_\alpha)$ a pro všechna α je $(\forall a \in J_\alpha)(\forall s \in M)(a \wedge s \in I)$, tedy máme $(\forall a \in I)(\forall s \in M)(a \wedge s \in I)$, což je definiční podmínka ideálu. □

► 1.5.10. Definice. Řekneme, že svaz S_1 lze izomorfně vnořit do svazu S_2, existuje-li monomorfismus $h : S_1 \to S_2$. Potom platí $S_1 \cong h(S_1) \Subset S_2$.

► 1.5.11. Věta. Libovolný svaz lze izomorfně vnořit do úplného svazu.

◦ *Důkaz.* Předpokládejme, že svaz $S_0 = (M_0, \wedge, \vee)$ nemá nulu. Pak definujeme množinu $M := M_0 \cup \{0\}$ a pokládáme $(\forall x \in M_0)(0 < x)$. Tedy $S_0 \Subset S := (M, \wedge, \vee)$.

Označme $\mathfrak{I}_S$ množinu všech ideálů svazu S. Je neprázdná, neboť např. $\{0\}, S \in \mathfrak{I}_S$. Pak $(\mathfrak{I}_S, \subseteq)$ je uspořádaná množina. Pro libovolné $\mathcal{N} \subseteq \mathfrak{I}_S$ je $\inf \mathcal{N} = \bigcap \mathcal{N} \in \mathfrak{I}_S$, a pokud označíme $\mathcal{Z}_\mathcal{N}$ množinu všech horních závor $\mathcal{N}$, platí $\sup \mathcal{N} = \inf \mathcal{Z}_\mathcal{N} = \bigcap \{I \in \mathfrak{I}_S \mid (\forall J \in \mathcal{N})(J \subseteq I)\}$. Tedy pokud položíme $I \wedge J := I \cap J$ a $I \vee J := \bigcap \{K \in \mathfrak{I}_S \mid I, J \subseteq K\}$, je $\mathfrak{U}_S := (\mathfrak{I}_S, \wedge, \vee)$ úplný svaz.

Definujeme zobrazení $h : M \to \mathcal{I}_S$ jako $h(a) = I_a$. Ukážeme, že h je monomorfismus svazů, tj. pokud označíme $\mathcal{H}_S$ množinu všech hlavních ideálů S, máme $h : M \xrightarrow{\text{na.}} \mathcal{H}_S$.

(*h* **je prosté)** Nechť $h(a) = h(b)$. Pak $I_a = I_b$, tedy $a \leq b$ a $b \leq a$, tedy $a = b$.

(*h* **je množinový izomorfismus** $(M, \leq)$ **a** $(\mathcal{H}_S, \subseteq)$**)** Mějme $a, b \in M$. Pak $a \leq b \Leftrightarrow I_a \subseteq I_b \Leftrightarrow h(a) \subseteq h(b)$.

(*h* **je svazový izomorfismus)** Vyplývá z předchozího bodu a předchozího výkladu.

□

► 1.5.12. Příklad. Věta nám umožňuje přechod od $\mathbb{Q}$ k $\mathbb{R}$. Hlavními ideály v $(\mathbb{Q}, \leq)$ jsou $I_a = \{x \in \mathbb{Q} \mid x \leq a\}$. A všemi ideály jsou $\{x \in \mathbb{Q} \mid x \leq r\}$ a $\{x \in \mathbb{Q} \mid x < r\}$ pro všechna $r \in \mathbb{R}$.

• 1.6. Distributivní svazy

► 1.6.1. Věta. Buď $S = (M, \wedge, \vee)$ libovolný svaz. Pak pro libovolné prvky $a, b, c \in M$ platí:

(1) $a \wedge (b \vee c) \geq (a \wedge b) \vee (a \wedge c)$;

(2) $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c)$;

(3) je-li $a \leq c$, platí $a \vee (b \wedge c) \leq (a \vee b) \wedge c$.

◦ *Důkaz.*

(1) Platí $b \leq b \vee c \Rightarrow a \wedge b \leq a \wedge (b \vee c)$ a podobně $a \wedge c \leq a \wedge (b \vee c)$. Tedy $a \wedge (b \vee c)$ je horní závora $\{a \wedge c, a \wedge b\}$, a tedy je větší nebo rovno než $\sup\{a \wedge c, a \wedge b\} = (a \wedge c) \vee (a \wedge b)$.

(2) Symetricky z duality.

(3) Platí $a \vee c = c$, tedy podle (2) je $a \vee (b \wedge c) \leq (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$.

□

► 1.6.2. Definice. Svaz $S = (M, \wedge, \vee)$ nazveme distributivní, pokud pro libovolné $a, b, c \in M$ platí:

(D1) $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$;

(D2) $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.

► 1.6.3. Poznámka. Pro rovnosti máme ve všech svazech zaručeno platnost jedné nerovnosti. Stačí tedy dokázat nerovnosti opačné než v předchozí větě.

► 1.6.4. Lemma. (D1) ⇒ (D2).

◦ *Důkaz.* Vyjdu z pravé strany (D2) a použiji (D1): $(a \vee b) \wedge (a \vee c) = ((a \vee b) \wedge a) \vee ((a \vee b) \wedge c) = a \vee ((a \vee b) \wedge c) = a \vee ((a \wedge c) \vee (b \wedge c)) = (a \vee (a \wedge c)) \vee (b \wedge c) = a \vee (b \wedge c)$. □

► 1.6.5. Příklad. Příklady distributivních svazů:

(1) množinové svazy;

(2) úplně uspořádané množiny;

(3) $(\mathbb{N}_0, |) = (\mathbb{N}_0, \delta, \nu)$.

► 1.6.6. Příklad. Svazy podgrup, normálních podgrup, ... nejsou obecně distributivní.

► 1.6.7. Věta. Libovolný podsvaz i libovolný homomorfní obraz distributivního svazu je distributivní.

◦ *Důkaz.* Distributivita je obecná podmínka, tedy se nemůže po zmenšení nosiče porušit. Homomorfismus zachovává průsek i spojení, tedy zachovává distributivitu. □

► 1.6.8. Definice. Buď $S = (M, \wedge, \vee)$ svaz. Filtr F se nazývá ultrafiltr, je-li $F \neq M$ a platí

$$(\forall a, b \in M)(a \vee b \in F \Rightarrow (a \in F \text{ vel } b \in F)).$$

Množinu všech ultrafiltrů na S označujeme $\mathcal{U}_S$.

► 1.6.9. Poznámka. V definiční podmínce ultrafiltru platí z definice filtru i zpětná implikace.

► 1.6.10. Poznámka. V matematické logice hrají filtry důležitou roli, pokud položíme spojení jako „nebo“ a průsek jako „a zároveň“, pak podmínka ultrafiltru vyjadřuje, kdy je konjunkce pravdivá. Podmínka filtru pak bude $a \wedge b \in F \Leftrightarrow (a \in F \text{ et } b \in F)$.

► 1.6.11. Příklad. Mějme $S = (\mathcal{P}(A), \cap, \cup)$ a $a \in A$, tedy $\{a\} \in \mathcal{P}(A)$. Pak definujeme hlavní filtr $F_{\{a\}} := \{B \in \mathcal{P}(A) \mid \{a\} \subseteq B\} = \{B \subseteq A \mid a \in B\}$. Pak $F_{\{a\}} \not\ni \emptyset$, tedy $F_{\{a\}} \neq \mathcal{P}(A)$.
Mějme $B_1, B_2 \in \mathcal{P}(A)$ a nechť $a \in B_1 \cup B_2$, pak $a \in B_1$ nebo $a \in B_2$, tedy $B_1 \in F_{\{a\}}$ nebo $B_2 \in F_{\{a\}}$. Tedy $F_{\{a\}}$ je ultrafiltr.
Ale $F_{\{a,b\}}$ pro $a \neq b$ není ultrafiltr.

► 1.6.12. Definice. Buď $S = (M, \wedge, \vee)$ a nechť $\emptyset \neq N \subseteq M$. Pak definujeme $\langle N \rangle$ jako nejmenší filtr ve svazu S obsahující N:

$$\langle N \rangle = \bigcap \{F \in \mathcal{F}_S \mid N \subseteq F\}.$$

► 1.6.13. Lemma. Buďte S svaz, F filtr ve svazu S a buď $a_0 \in S^\bullet$, dále označme $H := \{x \in S^\bullet \mid (\exists d \in F)(x \geq d \wedge a_0)\}$ Potom $\langle F \cup \{a_0\} \rangle = H$.

◦ *Důkaz.*

(⊇) Pokud $d \in F$, je $d \wedge a_0 \in \langle F \cup \{a_0\} \rangle$, a tedy $x = x \vee (d \wedge a_0) \in \langle F \cup \{a_0\} \rangle$.

($\subseteq$) Ukážeme, že $F \cup \{a_0\} \subseteq H$. Pro $d \in F$ platí, že $d \geq d \wedge a_0$. Dále mějme libovolné $d \in F$, pak $a_0 \geq d \wedge a_0$. Pokud ukážeme, že H je filtr, bude nutně nejmenší filtr nad $F \cup \{a_0\}$ jeho podmnožinou.

Mějme $x_1 \geq d_1 \wedge a_0$ a $x_2 \geq d_2 \wedge a_0$ pro nějaká $d_{1,2} \in F$, pak $x_1 \wedge x_2 \geq d_1 \wedge a_0 \wedge x_2 \geq d_1 \wedge a_0 \wedge d_2 \wedge a_0$. Položme $d := d_1 \wedge d_2 \in F$, pak $x_1 \wedge x_2 \geq d \wedge a_0$, tedy $x_1 \wedge x_2 \in H$.

□

► 1.6.14. Lemma. Sjednocení řetězce filtrů $\mathcal{R}$ je filtr.

◦ *Důkaz.*

(1) $a \in \bigcup \mathcal{R}, b \in S^\bullet, b \geq a$. $(\exists F)(a \in F \in \mathcal{R})$, tedy $b \in F$, tedy $b \in \bigcup \mathcal{R}$.

(2) $a, b \in \bigcup \mathcal{R}$. Pak $a \in F_1$, $b \in F_2$, bez újmy na obecnosti nechť $F_1 \subseteq F_2$. Potom $a, b \in F_2$, a tedy $a \wedge b \in F_2 \subseteq \bigcup \mathcal{R}$.

□

► 1.6.15. Lemma. Buďte $S = (M, \wedge, \vee)$ distributivní svaz, $a, b \in M$ a nechť neplatí $a \leq b$ (tedy $a > b$ nebo nejsou srovnatelné). Potom existuje ultrafiltr F svazu S tak, že $a \in F$ a současně $b \notin F$.

◦ *Důkaz.* Nechť $\mathcal{F}$ je množina všech filtrů, které obsahují a, ale neobsahují b, tedy platí $\mathcal{F} = \{F \in \mathcal{F}_S \mid a \in F \text{ et } b \notin F\}$. Nutně $F_a = \{x \in S \mid x \geq a\} \not\ni b$, tedy $F_a \in \mathcal{F}$. V $\mathcal{F}$ uspořádané inkluzí má libovolný řetězec $\mathcal{R}$ horní závoru $F = \bigcup \mathcal{F}$, která podle předcházejícího lemmatu je opět filtrem, a tedy triviálně $F \in \mathcal{F}$, neboť $a \in F$ et $b \notin F$. Dle Zornova lemmatu existuje v $\mathcal{F}$ maximální prvek F_0. Ukážeme sporem, že F_0 je ultrafiltr.

Nechť F_0 není ultrafiltr. Tedy existují $a_1, a_2 \in S$ takové, že $a_1 \vee a_2 \in F_0$, ale $a_1 \notin F_0$ ani $a_2 \notin F_0$. Definujme $F_1 := \langle F_0 \cup \{a_1\} \rangle$ a $F_2 := \langle F_0 \cup \{a_2\} \rangle$, přičemž $F_i \supsetneq F_0$ Ukážeme sporem, že $F_1 \in \mathcal{F}$ vel $F_2 \in \mathcal{F}$ a tím vytvoříme spor s maximalitou F_0. Tedy musíme ukázat, že $b \notin F_1$ vel $b \notin F_2$.

Nechť $b \in F_1$ et $b \in F_2$. Platí $F_i = \{x \mid (\exists c_i \in F_0)(x \geq c_i \wedge a_i)\}$, tedy i pro b existují c_i tak, že $b \geq c_1 \wedge a_1$ a $b \geq c_2 \wedge a_2$. Položme $c := c_1 \wedge c_2 \in F_0$, tedy $b \geq c \wedge a_1$ a $b \geq c \wedge a_2$, tedy $b \geq (c \wedge a_1) \vee (c \wedge a_2)$ a díky distributivitě je $b \geq c \wedge (a_1 \vee a_2) \in F_0$, neboť $c \in F_0$, $a_1 \vee a_2 \in F_0$. Ale filtr je uzavřený vůči větším prvkům, tedy $b \in F_0$, což je spor.

Tedy máme $F_1 \in \mathcal{F}$ vel $F_2 \in \mathcal{F}$, což je spor s maximalitou F_0 v $\mathcal{F}$. □

► 1.6.16. Věta (Stone). Libovolný distributivní svaz je izomorfní s nějakým množinovým svazem. Jinými slovy: libovolný distributivní svaz lze izomorfně vnořit do svazu všech podmnožin nějaké množiny.

◦ *Důkaz.* Mějme $S = (M, \wedge, \vee)$ distributivní svaz. Označme $\mathcal{U} = (\mathcal{P}(\mathcal{U}_S), \cap, \cup)$. Definujeme $h : M \to \mathcal{P}(\mathcal{U}_S)$ jako $h(x) := \{F \in \mathcal{U}_S \mid x \in F\}$. Ukážeme, že h je monomorfismus.

(injekce) Mějme $a, b \in M$, $a \neq b$, tj. (non $a \leq b$) vel (non $b \leq a$). Pak $(\exists F_1 \in \mathcal{U}_S)(a \in F_1 \text{ et } b \notin F_1)$ vel $(\exists F_2 \in \mathcal{U}_S)(b \in F_1 \text{ et } a \notin F_2)$, tedy $(\exists F_1 \in h(a) \smallsetminus h(b))$ vel $(\exists F_2 \in h(b) \smallsetminus h(a))$, tedy $h(a) \neq h(b)$.

($h(a \wedge b) = h(a) \cap h(b)$) Mějme libovolné $F \in \mathcal{U}_S$. Pak $F \in h(a \wedge b) \Leftrightarrow a \wedge b \in F \overset{\text{filtr}}{\Leftrightarrow} (a \in F$ et $b \in F) \Leftrightarrow (F \in h(a)$ et $F \in h(b)) \Leftrightarrow F \in h(a) \cap h(b)$.

($h(a \vee b) = h(a) \cup h(b)$) Mějme libovolné $F \in \mathcal{U}_S$. Pak $F \in h(a \vee b) \Leftrightarrow a \vee b \in F \overset{\text{ultrafiltr}}{\Leftrightarrow} (a \in F$ vel $b \in F) \Leftrightarrow (F \in h(a)$ vel $F \in h(b)) \Leftrightarrow F \in h(a) \cup h(b)$.

Celkově tedy máme $S \cong h(S) \overset{\text{svaz}}{\Subset} U$. □

1.7. Modulární svazy

▶ 1.7.1. Definice. Svaz $S = (M, \wedge, \vee)$ nazveme modulární, platí-li pro libovolné $a, b, c \in M$, $a \leq c$ vztah $a \vee (b \wedge c) = (a \vee b) \wedge c$.

▶ 1.7.2. Věta. Libovolný distributivní svaz je modulární.

◦ *Důkaz.* Nechť $a \leq c$, tedy $c = a \vee c$ Pak $a \vee (b \wedge c) \overset{(D2)}{=} (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$. □

▶ 1.7.3. Lemma. Svaz S je modulární právě tehdy, když pro libovolné $a, b, c \in S^\bullet$ platí

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

◦ *Důkaz.*

(⇒) V definičním vztahu položíme místo c spojení $a \vee c \geq a$. Dostaneme přímo dokazovanou rovnost.

(⇐) Pro libovolné $c \geq a$ je $a \vee c = c$, a tedy $a \vee (b \wedge c) = a \vee (b \wedge (a \vee c)) = (a \vee b) \wedge (a \vee c) = (a \vee b) \wedge c$.

□

▶ 1.7.4. Věta. Svaz všech normálních podgrup libovolné grupy G je modulární.

◦ *Důkaz.* Nerovnost $\geq$ v definiční podmínce platí vždy, tedy ukážeme, že

$$(\forall A, B, C \lhd G, A^\bullet \subseteq C^\bullet)(AB \cap C \subseteq A(B \cap C)).$$

Mějme libovolné $x \in (AB \cap C)^\bullet$, tedy $x \in (AB)^\bullet = A^\bullet B^\bullet$ a existují $x = ab$, kde $a \in A^\bullet \subseteq C^\bullet$ a $b \in B^\bullet$, tedy $b = a^{-1}x$, ale a^{-1} i x leží v $C^\bullet$, tedy $b \in C^\bullet$. Tedy $x = ab$, kde $a \in A^\bullet$ a $b \in B^\bullet \cap C^\bullet = (B \cap C)^\bullet$. □

▶ 1.7.5. Věta. Svaz všech ideálů libovolného okruhu je modulární. Svaz všech podprostorů libovolného vektorového prostoru je modulární.

▶ 1.7.6. Definice. Buď $S = (M, \wedge, \vee)$ svaz s nulou a jednotkou. Normální řada ve svazu S je libovolná posloupnost $(a_i)_{i=0}^m$ prvků z M taková, že $1 = a_0 > a_1 > \cdots > a_m = 0$. Číslo m nazveme délkou normální řady.

▶ 1.7.7. Definice. Řekneme, že normální řada $(b_j)_{i=0}^n$ je zjemněním normální řady $(a_i)_{i=0}^m$, pokud $\{a_i\}_{i=0}^m \subseteq \{b_j\}_{i=0}^n$. Zjemnění nazveme vlastní, pokud $n > m$.

► 1.7.8. Definice. Normální řada, která nemá žádné vlastní zjemnění, se nazývá hlavní řada.

► 1.7.9. Věta (Schreier). Libovolné 2 normální řady v modulárním svazu mají zjemnění stejných délek.

► 1.7.10. Věta (Jordan, Hőlder).

(1) Libovolné 2 hlavní řady v modulárním svazu mají stejnou délku.

(2) Existuje-li v modulárním svazu hlavní řada, pak libovolnou normální řadu lze zjemnit na hlavní řadu.

◦ *Důkaz.*

(1) Nechť je (a_i) kratší hlavní řada. Pak ji podle Schreierovy věty lze zjemnit (vlastním zjemněním), což je spor s tím, že je hlavní.

(2) Buď (a_i) hlavní řada a (b_j) libovolná normální řada. Nechť (b_j) nelze zjemnit na hlavní řadu. Pak existuje zjemnění (c_k) delší, než (a_i) a podle Schreierovy věty lze najít jejich zjemnění stejných délek. Protože (c_k) je delší než (a_i), museli bychom (a_i) zjemnit, což je spor s tím, že je hlavní.

□

► 1.7.11. Definice. Buďte $S = (M, \wedge, \vee)$ svaz a $a, b \in M$. Pro interval $\langle a, b\rangle$ použijeme označení b/a, tedy $b/a := \langle a, b\rangle = \{x \in M \mid x \geq a \text{ et } x \leq b\}$.

► 1.7.12. Věta. Buďte $S = (M, \wedge, \vee)$ modulární svaz s nulou a jednotkou a $a, b \in M$, $a < b$. Pak $(a \vee b)/a \cong b/(a \wedge b)$.

◦ *Důkaz.* Definujme 2 zobrazení, $f : \langle a, a \vee b\rangle \to \langle a \wedge b, b\rangle$ jako $f(x) = x \wedge b$ a $g : \langle a \wedge b, b\rangle \to \langle a, a \vee b\rangle$ jako $g(y) = y \vee a$. Ukážeme korektnost definice, tedy mějme $a \leq x \leq a \vee b$, pak $x \wedge b \geq a \wedge b$ a $x \wedge b \leq (a \vee b) \wedge b = b$; korektnost druhé definice ukážeme obdobně.

Zkoumejme zobrazení $g \circ f$, tedy mějme $x \in \langle a, a \vee b\rangle$, pak $g(f(x)) = g(x \wedge b) = (x \wedge b) \vee a$, a neboť $x \geq a$, je $g(f(x)) = x \wedge (b \vee a)$, a neboť $x \leq a \vee b$, je $g(f(x)) = x$. Podobně ukážeme, že $f \circ g = \mathrm{id}$, a tedy f i g jsou bijekce. Ukážeme, že f a g jsou izomorfismy uspořádaných množin, tedy $x \leq y \Leftrightarrow f(x) \leq f(y) \Leftrightarrow g(x) \leq g(y)$. Směr vpravo je snadný, pokud $x \leq y$, je $f(x) = x \wedge b \leq y \wedge b = f(y)$ a podobně pro g. Pro směr vlevo předpokládejme, že $f(x) \leq f(y)$, pak dostáváme $x = g(f(x)) \leq g(f(y)) = y$, a podobně pro g. Tedy jsme našli množinový, a tím i svazový izomorfismus obou intervalů. □

► 1.7.13. Věta. Mějme modulární svaz, ve kterém existují hlavní řady (tedy svaz musí mít nulu a jednotku). Definujeme-li $|a|$ jako délku libovolné hlavní řady hlavního ideálu prvku a, pak platí $|a \vee b| + |a \wedge b| = |a| + |b|$.

◦ *Důkaz.* Dle předchozí věty je $|a \vee b| - |a| = |b| - |a \wedge b|$. □

► 1.7.14. Důsledek. 1. věta o dimenzi.

► 1.7.15. Poznámka. Pokud ve svazu najdeme 2 hlavní řady různé délky, tak víme, že svaz není modulární.

• 1.8. Komplement

► 1.8.1. Definice. Buď $S = (M, \wedge, \vee)$ svaz s nulou a jednotkou. Řekneme, že prvek $a' \in M$ je komplementem prvku $a \in M$, platí-li:

(1) $a \wedge a' = 0$;

(2) $a \vee a' = 1$.

► 1.8.2. Poznámka. Zvláště v množinových svazech používáme často pro komplement prvku A značku $\complement A$.

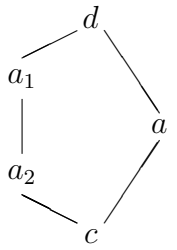
► 1.8.3. Příklad. Ve svazu $S = (\mathcal{P}(A), \cap, \cup)$ platí pro $B \subseteq A$, že $B' = A \setminus B$ a komplement existuje právě jeden.

► 1.8.4. Příklad. $0' = 1$; $1' = 0$.

► 1.8.5. Příklad. Komplement nemusí existovat, ale může jich i existovat více.

(1) Mějme svaz s prvky $\{0, a, 1\}$, pak prvek a nemá komplement.

(2) Mějme svaz $\mathcal{N}_5$ nazývaný pentagon:



Prvek c představuje nulu, prvek d jednotku. K prvku a existují 2 různé srovnatelné komplementy a_1 a a_2. Dále svaz $\mathcal{N}_5$ má 2 hlavní řady různé délky (d, a, c a d, a_1, a_2, c), tedy není modulární, a není ani distributivní.

► 1.8.6. Věta. V modulárním svazu nemá žádný prvek 2 různé srovnatelné komplementy.

◦ *Důkaz.* Nechť a_1 a a_2 jsou komplementy a a nechť $a_1 \leq a_2$. Pak platí $a_1 = a_1 \wedge 1 = a_1 \wedge (a \vee a_2) = (a_1 \wedge a) \vee a_2 = 0 \vee a_2 = a_2$. □

► 1.8.7. Věta. Svaz je modulární právě tehdy, když neobsahuje jako podsvaz $\mathcal{N}_5$.

◦ *Důkaz.*

(⇒) Sporem, tedy nechť obsahuje pentagon. Pak platí $(a_2 \vee a) \wedge a_1 = d \wedge a_1 = a_1 \neq a_2 = a_2 \vee c = a_2 \vee (a \wedge a_1)$, což je protipříklad proti podmínce modularity.

(⇐) Sporem, tedy nechť není modulární. Tedy existují a, b, c takové, že $a \leq c$ ale $a \wedge (b \vee c) < (a \wedge b) \vee c$. Ukážeme, že $a \neq c$ a b je s nimi nesrovnatelný.

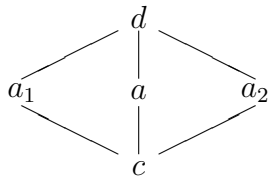
Nechť $a = c$, pak $a \wedge (b \vee a) = a = (a \wedge b) \vee a$, což je spor, tedy $a < c$.

Nechť $b < a$ vel $b < c$, pak jistě $b < c$ a $a \wedge (b \vee c) \leq a < c \leq (a \wedge b) \vee c$.

□

► 1.8.8. Poznámka (algebraický vtip, který nezazněl na přednášce). Víte, proč je Sovětský svaz modulární? Protože nemá Pentagon.

► 1.8.9. Příklad. Definujeme svaz $\mathcal{M}_5$ nazývaný diamant:



Pak $\mathcal{M}_5$ je modulární, ale není distributivní, prvek a má 2 komplementy, které nejsou srovnatelné.

► 1.8.10. Věta. V libovolném distributivním svazu s nulou a jednotkou má každý prvek nejvýše jeden komplement.

◦ *Důkaz.* Mějme a a a_1, a_2 jeho komplementy. Pak $a_1 = a_1 \wedge 1 = a_1 \wedge (a \vee a_2) = (a_1 \wedge a) \vee (a_2 \wedge a_1) = 0 \vee (a_2 \wedge a_1) = a_1 \wedge a_2$, tedy $a_1 \leq a_2$. Ale distributivní svaz je modulární a a_1, a_2 jsou komplementy stejného prvku, tedy $a_1 = a_2$. □

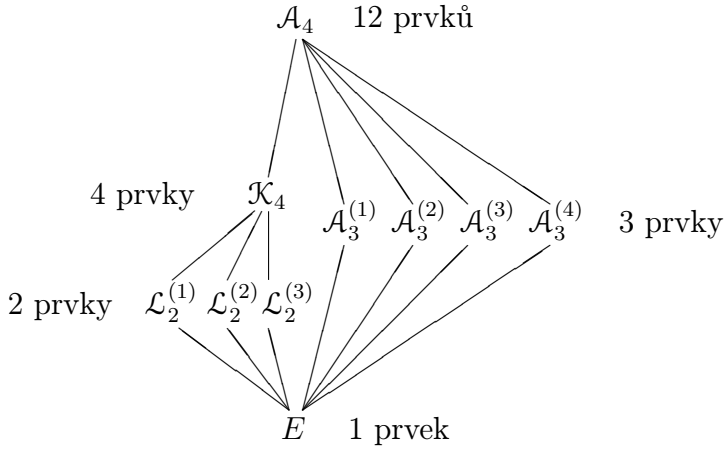
► 1.8.11. Věta. Svaz je distributivní právě tehdy, když neobsahuje jako podsvaz ani $\mathcal{N}_5$, ani $\mathcal{M}_5$.

► 1.8.12. Definice. Řekneme, že svaz s nulou a jednotkou je komplementární, má-li v něm libovolný prvek alespoň jeden komplement.

► 1.8.13. Definice. Řekneme, že svaz s nulou a jednotkou je Booleův, je-li distributivní a komplementární.

► 1.8.14. Příklad. Příkladem Booleových svazů jsou svazy množinové.

► 1.8.15. Příklad. Vraťme se k 12prvkové alternující grupě $\mathcal{A}_4$, která není jednoduchá a nemá žádnou 6prvkovou podgrupu (přestože $6 \mid 12$), a nakresleme schéma svazu jejích podgrup.



Vidíme, že svaz všech podgrup $\mathcal{A}_4$ není modulární, neboť má hlavní řady různé délky. Je to protipříklad, kdyby si někdo myslel, že svaz všech (nejen normálních) podgrup je modulární. Dále svaz podgrup $\mathcal{A}_4$ ani svaz podgrup $\mathcal{K}_4$ není distributivní. Navíc všechny podgrupy $\mathcal{K}_4$ jsou normální, tedy neplatí, že by libovolný svaz normálních podgrup byl distributivní.

• 1.9. Booleova algebra

► 1.9.1. Definice. Mějme Booleův svaz $S = (M, \wedge, \vee)$. Pak algebru $Q = (M, \wedge, \vee, ', 0, 1)$, kde operace $(')$ je komplement a je unární a operace 0 a 1 jsou nulární, tedy konstanty, nazveme Booleova algebra.

► 1.9.2. Věta. Buď A Booleova algebra a nechť $a, b \in A^\bullet$. Pak:

(1) $0' = 1, \quad 1' = 0$;

(2) $(a')' = a$;

(3) $a \wedge b = 0 \Leftrightarrow b \leq a', \quad a \vee b = 1 \Leftrightarrow b \geq a'$;

(4) $(a \wedge b)' = a' \vee b', \quad (a \vee b)' = a' \wedge b'$ (De Morganovy zákony).

◦ *Důkaz.* Ukážeme pouze tvrzení 3 a 4.

(3) $b = b \wedge 1 = b \wedge (a \vee a') = (b \wedge a) \vee (b \wedge a') = 0 \vee (b \wedge a') = b \wedge a' \Leftrightarrow b \leq a'$

(4) $(a \wedge b) \wedge (a' \vee b') = (a \wedge b \wedge a') \vee (a \wedge b \wedge b') = 0 \vee 0 = 0,$
$(a \wedge b) \vee (a' \vee b') = (a \vee a' \vee b') \wedge (b \vee a' \vee b') = 1 \wedge 1 = 1;$

□

► 1.9.3. Lemma. Filtr F ve Booleově svazu je ultrafiltr právě tehdy, platí-li

$$(\forall x \in S^\bullet)(x \in F \Leftrightarrow x' \notin F).$$

◦ *Důkaz.*

(⇒) Mějme libovolné x. Pak $x \vee x' = 1 \in F$, tedy $x \in F$ vel $x' \in F$. Kdyby $x, x' \in F$, pak $0 = x \wedge x' \in F$, což je spor s tím, že $F \neq S^\bullet$.

(⇐) Mějme libovolné prvky a, b. Nechť $a \vee b \in F$, ale $a, b \notin F$. Pak $a', b' \in F$, tedy $a' \wedge b' = (a \vee b)' \in F$, což je spor.

□

► 1.9.4. Věta. Libovolná Booleova algebra je izomorfní s nějakou množinovou Booleovou algebrou.

◦ *Důkaz.* Definujeme zobrazení $f(x) = \{F \in \mathcal{U}_S \mid x \in F\}$. Víme, že f zachovává průsek a spojení.

(′) $f(x') = \{F \in \mathcal{U}_S \mid x \in F\} = \{F \in \mathcal{U}_S \mid x \notin F\} = \complement f(x)$

(0) $f(0) = \{F \in \mathcal{U}_S \mid 0 \in F\}$, ale $0 \in F \Rightarrow F = S^\bullet$, což není filtr. Tedy $f(0) = \emptyset$.

(1) $f(1) = \{F \in \mathcal{U}_S \mid 1 \in F\} = \mathcal{U}_S$.

□

► 1.9.5. Věta. Libovolná konečná Booleova algebra je izomorfní množinové Booleově algebře tvořené všemi podmnožinami vhodné množiny.

► 1.9.6. Věta.

(1) Libovolná konečná Booleova algebra má počet prvků roven číslu 2^n, $n \in \mathbb{N}$.

(2) K libovolnému $n \in \mathbb{N}$ existuje až na izomorfii právě jedna Booleova algebra s 2^n prvky.

► 1.9.7. Příklad. 2-, 4- a 8prvková Booleova algebra.

