ZÁKLADY TEORIE SVAZŮ

Radan Kučera, říjen 2003

Literatura

- **Doporučená:**
  - L. Procházka a kol., Algebra, Academia, Praha 1990 (kap. IX).
- **Další:**
  - G. Birkhoff, T. C. Bartee: Aplikovaná algebra, Alfa, Bratislava 1981 (kap. 9).
  - G. Birkhoff, S. Mac Lane: Prehľad modernej algebry, Alfa, Bratislava 1979 (kap. 11).
  - A. G. Kuroš: Kapitoly z obecné algebry, Academia, Praha 1977 (kap. IV).
  - S. Mac Lane, G. Birkhoff: Algebra, Alfa, Bratislava 1974 (kap. XIV).
- **Hlubší:**
  - R. Faure, E. Heurgonová: Uspořádání a Booleovy algebry, Academia, Praha 1984 (kap. II-V). Při studiu z této knihy se však nedejte zmást ani definicí zobrazení uvedenou v kapitole I ani tiskovými chybami, třeba opačně napsanými nerovnosti v Lemma 2 na str. 88.

Úvodní zamyšlení o volbě definic. Většina pojmů, se kterými se setkáváte na matematických přednáškách, jsou pojmy, na jejichž definici se matematikové v průběhu doby jednoznačně shodli. Často to bývá ta evidentně nejvhodnější ze všech variant, které se nabízely. V některých případech však volba není tak zřejmá: nabízí se najednou více vhodných variant. Příkladem může být definice množiny přirozených čísel: máme považovat nulu za přirozené číslo nebo ne? Je jasné, že příliš se obě varianty neliší, liší se jen ve znění některých vět, u nichž se v předpokladech nebo v tvrzeních musí ubrat či přidat požadavek nenulovosti, a ve znění některých navazujících definic, kde je třeba udělat totéž. V tomto případě jsme se přidali na stranu těch, kteří množinou přirozených čísel $\mathbb{N}$ nazývají množinu kladných celých čísel, tj. nulu za přirozené číslo nepovažujeme.

Druhý podobný případ je případ okruhů, kdy někdo (tak jako my na přednášce) v definici vyžaduje, aby každý okruh měl jedničku (a pak tedy také požaduje, aby tuto jedničku obsahoval i každý podokruh okruhu a aby homomorfismus okruhů zobrazil jedničku jednoho okruhu na jedničku druhého okruhu). V jiném přístupu se definují okruhy bez požadavku jedničky a o předchozím speciálním případě se mluví jako o okruhu s jedničkou. Je asi každému jasné, že se nedá říci, která z obou variant je ta správná. Správné jsou obě, jen je nezbytné se zvolené definice držet, tj. ve všech následujících úvahách užívat zvolenou definici. Je na tom dobře vidět i tvořivost v matematice: matematik si volí definice do značné míry svobodně a ze zvolených definic pak odvozuje řadu tvrzení o popisovaných objektech. Přitom definice volí s ohledem na to, aby popisované objekty odpovídaly jeho představám o nich a aby v odvozované teorii vycházela tvrzení co možná nejelegantněji. Zde je asi měřítkem elegance to, zda tvrzení lze snadno formulovat bez nutnosti probírat různé speciální případy zvlášť.

Podobnou situací, kdy není zcela jasné, jak definici formulovat, je případ prázdné struktury. Máme připustit, aby například grupoid mohl mít za nosnou množinu množinu prázdnou? Ti, kteří zastávají názor, že grupoid má mít neprázdnou nosnou množinu, zdůvodňují svůj postoj tím, že grupoid na prázdné nosné množině je těžké si představit. A že konec konců tím, že tento případ připustíme, získáme jen velmi nezajímavý objekt, o kterém je ihned všechno známo. Jak si vlastně představit grupoid na prázdné množině? Operace na množině G je zobrazení $G \times G \to G$. Jestliže $G = \emptyset$, pak $G \times G$, jakožto množina uspořádaných dvojic prvků z G, je též prázdná. Připomeňme, co je zobrazení množiny A do množiny B. Je to uspořádaná trojice (A, B, f), kde f je podmnožina kartézského součinu $A \times B$, v níž pro každé $a \in A$ existuje právě jedna uspořádaná dvojice s první složkou a. Je-li tedy $A = \emptyset$, pak pro libovolnou množinu B takové zobrazení je jediné: f je také prázdná množina. Je-li naopak $A \neq \emptyset$ a současně $B = \emptyset$, pak takové zobrazení neexistuje. Proto tedy na nosné množině $G = \emptyset$ máme jediný grupoid, jehož (jedinou možnou) operací na G je prázdné zobrazení, tj. trojice $(\emptyset, \emptyset, \emptyset)$.

A v čem spočívá výhoda toho považovat prázdnou množinu spolu s prázdným zobrazením za grupoid? Jisté výhody se začnou objevovat až v okamžiku, kdy definujeme podgrupoid grupoidu, tj. podmnožinu nosné množiny grupoidu uzavřenou vůči operaci grupoidu. Protože je rozumné chtít, aby (po zúžení operace) byl podgrupoid sám grupoidem, v případě, kdy grupoid definujeme jen na neprázdné nosné množině, je třeba v definici podgrupoidu přidat požadavek neprázdnosti podmnožiny (tedy podgrupoidem rozumět jen takovou neprázdnou podmnožinu, že součin libovolných dvou jejích prvků do ní patří). Ale pak neplatí, že průnikem dvou podgrupoidů daného grupoidu je opět podgrupoid, neboť tímto průnikem může být i prázdná množina. Připuštěním prázdného grupoidu tedy zjednodušíme definici podgrupoidu i větu o průniku podgrupoidů. A toto formální zjednodušování celé teorie, které jsme viděli na předchozím příkladě, obzvláště vynikne při studiu univerzálních algeber. Právě pod vlivem univerzální algebry jsem se rozhodl opustit svůj předchozí předpoklad neprázdnosti nosné množiny. Myslím si, že určité nepříjemnosti spojené s představou podivného prázdného grupoidu (později též prázdného svazu či prázdné univerzální algebry) jsou čtenáři vyváženy výhodami snadnějších formulací vět a definic.

A když se už zabýváme prázdnou množinou, uvědomme si, jaké relace na prázdné množině máme: relací na množině M je libovolná podmnožina kartézského součinu $M \times M$, pro $M = \emptyset$ máme tedy jedinou relaci: prázdnou množinu. A protože pro všechny prvky prázdné množiny platí naprosto cokoli (uvědomte si, že implikace $x \in \emptyset \Longrightarrow V$ je pravdivá pro všechna x a pro každé tvrzení V, neboť je nepravdivý předpoklad implikace $x \in \emptyset$), je tato prázdná relace ekvivalencí, ale i uspořádáním na M, které je dokonce dobré: každá neprázdná podmnožina (taková neexistuje) má nejmenší prvek. Promysleme si, jak vypadá rozklad na prázdné množině. Rozkladem na množině M rozumíme množinu neprázdných podmnožin množiny M (těmto podmnožinám říkáme třídy rozkladu) takovou, že každý prvek množiny M patří do právě jedné třídy rozkladu. Rozklad na prázdné množině $M = \emptyset$ tedy nemůže mít žádnou třídu rozkladu, neboť neexistuje žádná neprázdná podmnožina prázdné množiny M. Na druhou stranu prázdná množina je rozkladem na $M = \emptyset$, neboť pro každý prvek prázdné množiny platí zcela cokoli, například i to, že pro něj existuje třída rozkladu, do níž patří. Na prázdné množině tedy existuje jediný rozklad: prázdná množina.

1. Polosvazy

Definice. *Prvek x grupoidu $(G, \cdot)$ se nazývá idempotentní, jestliže $x \cdot x = x$.*

Definice. *Komutativní pologrupa, jejíž každý prvek je idempotentní, se nazývá polosvaz.*

Poznámka. Podle předchozí definice tedy budeme i prázdný grupoid, který je samozřejmě komutativní i asociativní, považovat za polosvaz.

Příklad. Pro libovolnou množinu X budeme (i v dalším textu) symbolem 2^X označovat množinu všech podmnožin množiny X. Pak $(2^X, \cap)$ a $(2^X, \cup)$ jsou polosvazy.

Příklad. Množina všech přirozených čísel $\mathbb{N}$ spolu s operací největší společný dělitel (resp. nejmenší společný násobek) tvoří polosvaz.

Poznámka. V následující větě použijeme právě učiněnou změnu definice grupoidu: grupoidem rozumíme i grupoid na prázdné množině, proto prázdná množina je podgrupoidem libovolného grupoidu. Protože existují komutativní pologrupy, v nichž žádný prvek není idempotentní (například $(\mathbb{N}, +)$), museli bychom bez této změny následující větu formulovat takto: „Nechť $(G, \cdot)$ je komutativní pologrupa. Pak množina všech idempotentních prvků, je-li neprázdná, tvoří podgrupoid pologrupy $(G, \cdot)$, který je polosvazem.“

Věta 1.1. *Nechť $(G, \cdot)$ je komutativní pologrupa. Pak množina všech idempotentních prvků tvoří podgrupoid pologrupy $(G, \cdot)$, který je polosvazem.*

Důkaz. Jsou-li x a y idempotentní, pak $x \cdot x = x$ a $y \cdot y = y$, odkud plyne $(x \cdot y) \cdot (x \cdot y) = x \cdot x \cdot y \cdot y = x \cdot y$. Jde tedy skutečně o podgrupoid, zbytek tvrzení je zřejmý.

Věta 1.2. *Nechť $(G, \leq)$ je uspořádaná množina, v níž k libovolným dvěma prvkům $a, b \in G$ existuje supremum $a \vee b$. Pak $(G, \vee)$ je polosvaz. Navíc pro každé $a, b \in G$ platí*

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

Důkaz. Komutativita i idempotentnost je zřejmá, ekvivalence obou podmínek též. Pro libovolné $a, b, c \in G$ jistě platí $(a \vee b) \vee c \geq c$, $(a \vee b) \vee c \geq a \vee b \geq a$, podobně $(a \vee b) \vee c \geq b$. Je tedy $(a \vee b) \vee c$ horní závora množiny $\{b, c\}$, proto $(a \vee b) \vee c \geq b \vee c$. Je tudíž $(a \vee b) \vee c$ horní závora množiny $\{a, b \vee c\}$, proto $(a \vee b) \vee c \geq a \vee (b \vee c)$. Analogicky opačná nerovnost, z antisymetrie asociativita.

Věta 1.3. *Nechť $(G, \cdot)$ je polosvaz. Potom relace $\leq$, daná vztahem*

$$a \leq b \iff a \cdot b = b$$

pro každé $a, b \in G$, je uspořádání na G, ve kterém pro každé $a, b \in G$ je $a \cdot b$ supremum množiny $\{a, b\}$ v $(G, \leq)$.

Důkaz. Pro každé $a, b, c \in G$ platí

$$\begin{aligned} a \cdot a = a \quad &\Longrightarrow \quad a \leq a, \\ a \leq b,\ b \leq a \quad &\Longrightarrow \quad a = b \cdot a = a \cdot b = b, \end{aligned}$$

a tedy je $\leq$ reflexivní a antisymetrická relace. Rovněž platí

$$\begin{aligned} a \leq b,\ b \leq c \quad &\Longrightarrow \quad a \cdot b = b,\ b \cdot c = c \\ &\Longrightarrow \quad a \cdot c = a \cdot (b \cdot c) = (a \cdot b) \cdot c = b \cdot c = c \\ &\Longrightarrow \quad a \leq c, \end{aligned}$$

čímž jsme dokázali tranzitivitu. Je tedy $\leq$ uspořádání na G. Protože

$$\begin{aligned} a\cdot(a\cdot b) &= (a\cdot a)\cdot b = a\cdot b,\\ b\cdot(a\cdot b) &= (b\cdot a)\cdot b = (a\cdot b)\cdot b = a\cdot(b\cdot b) = a\cdot b, \end{aligned}$$

platí $a \leq a\cdot b$, $b \leq a\cdot b$. Nechť c je libovolná horní závora množiny $\{a,b\}$ v $(G,\leq)$, tedy $a\leq c$, $b\leq c$. Pak platí $a\cdot c = c$, $b\cdot c = c$, odkud

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

tedy $a\cdot b\leq c$, je tedy $a\cdot b$ supremum množiny $\{a,b\}$ v $(G,\leq)$.

Poznámka. Z dokázaných vět vyplývá následující

Důsledek. *Polosvazy jsou totéž co uspořádané množiny, kde ke každým dvěma prvkům existuje supremum.*

Poznámka. Princip duality: Nechť $(G,\leq)$ je uspořádaná množina. Definujeme-li na G novou relaci $\preceq$ takto: pro libovolné prvky $a,b\in G$ klademe

$$a\preceq b \iff b\leq a,$$

pak je $(G,\preceq)$ opět uspořádaná množina, přičemž supremum v $(G,\leq)$ se stane infimem v $(G,\preceq)$ a naopak.

Důsledek. *Polosvazy jsou totéž co uspořádané množiny, kde ke každým dvěma prvkům existuje infimum.*

2. Svazy

Definice. *Uspořádaná množina, v níž ke každým dvěma prvkům existuje supremum i infimum, se nazývá svaz.*

Příklad. Každý řetězec (neboli lineárně uspořádaná množina, tj. uspořádaná množina, v níž jsou každé dva prvky srovnatelné) je svaz.

Příklad. Pro libovolnou množinu X je $(2^X,\subseteq)$ svaz.

Věta 2.1. *Nechť $(G,\leq)$ je svaz. Pro libovolné prvky $a,b\in G$ označme jejich supremum symbolem $a\vee b$ a jejich infimum symbolem $a\wedge b$. Pak $(G,\vee)$ a $(G,\wedge)$ jsou polosvazy a obě operace jsou spolu svázány tzv. absorpčními zákony: pro každé prvky $a,b\in G$ platí*

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

Kromě toho pro každé prvky $a,b\in G$ platí

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

Důkaz. To, že $(G, \vee)$ a $(G, \wedge)$ jsou polosvazy, plyne z věty 1.2 a principu duality; rovněž tak ekvivalentnost uvedených podmínek. Absorpční zákony jsou zřejmé.

Věta 2.2. *Nechť $(G, \vee, \wedge)$ je množina se dvěma idempotentními, asociativními a komutativními operacemi, které jsou spolu svázány absorpčními zákony. Pak platí*

1. *pro každé prvky $a, b \in G$ platí $a \wedge b = a \Longleftrightarrow a \vee b = b$,*
2. *definujeme-li na G relaci $\leq$ takto: pro libovolné prvky $a, b \in G$ klademe*

   $$a \leq b \Longleftrightarrow a \vee b = b,$$

   pak je $\leq$ uspořádání na G takové, že $(G, \leq)$ je svaz, v němž pro libovolné prvky $a, b \in G$ je prvek $a \vee b$ jejich supremum a prvek $a \wedge b$ jejich infimum.

Důkaz. Nechť pro prvky $a, b \in G$ platí $a \wedge b = a$. Pak $a \vee b = (a \wedge b) \vee b = b \vee (a \wedge b) = b$ dle absorpčního zákona. Opačná implikace analogicky. Ostatní plyne z věty 1.3.

Poznámka. Z dokázaných vět vyplývá, že svazy jsou totéž co algebraické struktury $(G, \vee, \wedge)$ se dvěma idempotentními, asociativními a komutativními operacemi, svázanými spolu absorpčními zákony. Proto i tyto struktury $(G, \vee, \wedge)$ budeme také nazývat svazy.

Poznámka. Princip duality: Je-li $(G, \vee, \wedge)$ svaz, pak i $(G, \wedge, \vee)$ je svaz. Obecně, jestliže v nějakém platném tvrzení o svazech systematicky zaměníme supremum $\leftrightarrow$ infimum, $\vee \leftrightarrow \wedge$, $\leq \leftrightarrow \geq$, dostaneme opět platné tvrzení o svazech.

Poznámka. Protože není nutné zdůrazňovat, zda máme na mysli svaz jako uspořádanou množinu nebo jako algebraickou strukturu se dvěma operacemi, nebudeme v dalším textu, nebude-li to z nějakých důvodů vhodné nebo dokonce nevyhnutelné, uspořádání či operace vyznačovat. Budeme tedy místo o svazu $(G, \leq)$ či svazu $(G, \vee, \wedge)$ jednoduše psát o svazu G.

Věta 2.3. *V libovolném svazu G pro každou trojici prvků $a, b, c \in G$ platí tzv. distributivní nerovnosti*

$$(a \vee b) \wedge (a \vee c) \geq a \vee (b \wedge c),$$
$$(a \wedge b) \vee (a \wedge c) \leq a \wedge (b \vee c).$$

Je-li navíc $c \leq a$, platí tzv. modulární nerovnost

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

Důkaz. Jistě platí $a \vee b \geq a$, $a \vee c \geq a$, a tedy i $(a \vee b) \wedge (a \vee c) \geq a$. Podobně $a \vee b \geq b \geq b \wedge c$, $a \vee c \geq c \geq b \wedge c$, odkud $(a \vee b) \wedge (a \vee c) \geq b \wedge c$. Dohromady dostáváme první distributivní nerovnost. Druhou dokážeme analogicky, nebo lze užít principu duality a odvodit ji z první. Je-li navíc $c \leq a$, platí $a \wedge c = c$, proto modulární nerovnost plyne z druhé distributivní nerovnosti.

Věta 2.4. *Nechť G je svaz, $n \in \mathbb{N}$. Pro libovolné prvky $a_1, \dots, a_n \in G$ platí, že $a_1 \vee \cdots \vee a_n$ je supremum množiny $\{a_1, \dots, a_n\}$ a $a_1 \wedge \cdots \wedge a_n$ je infimum množiny $\{a_1, \dots, a_n\}$.*

Důkaz. Indukcí vzhledem k n.

3. Podsvazy, ideály, filtry, homomorfismy

Definice. *Nechť $(G, \vee, \wedge)$ je svaz, A podmnožina jeho nosné množiny G. Řekneme, že A je podsvaz svazu $(G, \vee, \wedge)$, jestliže je A podgrupoidem grupoidu $(G, \wedge)$ a současně podgrupoidem grupoidu $(G, \vee)$.*

Poznámka. Je tedy $A \subseteq G$ podsvazem svazu G, právě když pro každé $a, b \in A$ platí $a \vee b \in A$ a $a \wedge b \in A$.

Příklady. Každá jednoprvková podmnožina svazu je jeho podsvazem, prázdná množina je podsvazem libovolného svazu, každý svaz je svým podsvazem.

Definice. *Nechť G je svaz, $A \subseteq G$ podmnožina. Řekneme, že A je ideál svazu G, jestliže je A podsvazem svazu G, který navíc splňuje podmínku: pro každé $a \in A$ a každé $x \in G$ platí*

$$x \leq a \Longrightarrow x \in A.$$

Duálně, řekneme, že A je filtr svazu G, jestliže je A podsvazem svazu G, který navíc splňuje podmínku: pro každé $a \in A$ a každé $x \in G$ platí

$$x \geq a \Longrightarrow x \in A.$$

Poznámka. Ideál svazu je tedy podsvaz, který s každým svým prvkem a obsahuje i všechny prvky svazu menší než a, filtr svazu je podsvaz, který s každým svým prvkem a obsahuje i všechny prvky svazu větší než a.

Příklady. Každý svaz je svým ideálem i filtrem. Prázdná množina je ideálem i filtrem libovolného svazu.

Věta 3.1. *Průnik libovolného neprázdného systému podsvazů (resp. ideálů, resp. filtrů) daného svazu je opět podsvaz (resp. ideál, resp. filtr) tohoto svazu.*

Důkaz. Nechť $I \neq \emptyset$ a pro každé $i \in I$ je A_i podsvaz svazu G. Označme $A = \bigcap_{i \in I} A_i$ jejich průnik. Pak pro každé $a, b \in A$ platí $a, b \in A_i$ pro všechna $i \in I$, a tedy $a \vee b \in A_i$ a $a \wedge b \in A_i$. Odtud $a \vee b \in A$ a $a \wedge b \in A$, a proto je A podsvaz svazu G. Předpokládejme navíc, že pro každé $i \in I$ je A_i dokonce ideál svazu G. Mějme $a \in A$, $x \in G$, $x \leq a$. Pak pro každé $i \in I$ je $a \in A_i$, tedy i $x \in A_i$, tudíž $x \in A$. Tvrzení o filtrech nyní plyne z duality.

Poznámka. Zde nám opět to, že jsme připustili i prázdný podsvaz, zjednodušilo formulaci. Jinak by věta 3.1 musela být formulována takto: „Průnik libovolného neprázdného systému podsvazů (resp. ideálů, resp. filtrů) daného svazu je opět podsvaz (resp. ideál, resp. filtr) tohoto svazu nebo prázdná množina.“

Důsledek. *Průnik libovolného neprázdného konečného systému neprázdných ideálů (resp. filtrů) daného svazu je opět neprázdný ideál (resp. filtr) tohoto svazu.*

Důkaz. Jsou-li $A_1, \ldots, A_n$ neprázdné ideály a zvolíme-li $a_i \in A_i$, pak $a = a_1 \wedge \cdots \wedge a_n \leq a_i$, a tedy $a \in A_i$. Průnik tedy není prázdná množina. Duálně pro filtry.

Příklad. Ukažme, že průnikem neprázdných ideálů v předchozí větě může být opravdu prázdná množina. Uvažme svaz celých čísel s obvyklým uspořádáním podle velikosti $(\mathbb{Z}, \leq)$. Pro libovolné $n \in \mathbb{Z}$ je $A_n = \{x \in \mathbb{Z};\ x \leq n\}$ ideál tohoto svazu. Ale $\bigcap_{n \in \mathbb{Z}} A_n$ je prázdná množina, neboť pro každé celé číslo m najdeme celé číslo $n < m$, pak ovšem $m \notin A_n$, a tedy m nepatří do průniku všech ideálů A_n.

Definice. *Nechť G je svaz, $A \subseteq G$ podmnožina. Díky předchozí větě můžeme nyní definovat ideál $A{\downarrow}$ svazu G generovaný množinou A jako průnik všech ideálů tohoto svazu obsahujících množinu A. (Uvědomte si, že alespoň jeden ideál tohoto svazu obsahující množinu A existuje, totiž celý svaz G.) Duálně, filtr $A{\uparrow}$ svazu G generovaný množinou A je průnik všech filtrů tohoto svazu obsahujících množinu A. Je-li $A = \{a\}$, píšeme stručně $a{\downarrow}$ místo $\{a\}{\downarrow}$, resp. $a{\uparrow}$ místo $\{a\}{\uparrow}$, a hovoříme o hlavním ideálu, resp. o hlavním filtru, generovaném prvkem a.*

Poznámka. Pro svaz G a podmnožinu $A \subseteq G$ je ideál $A{\downarrow}$ generovaný množinou A tím nejmenším (vzhledem k množinové inkluzi) ideálem svazu G ze všech ideálů obsahujících množinu A. Duálně filtr $A{\uparrow}$ generovaný množinou A je tím nejmenším (vzhledem k množinové inkluzi) filtrem svazu G ze všech filtrů obsahujících množinu A.

Poznámka. Je zřejmé, že podmnožina $A \subseteq G$ je ideálem svazu G, právě když $A{\downarrow} = A$, a je filtrem svazu G, právě když $A{\uparrow} = A$.

Věta 3.2. *Nechť G je svaz, $A \subseteq G$ podmnožina. Pro ideál $A{\downarrow}$ generovaný* *množinou A platí*

$$A{\downarrow} = \{x \in G; \exists n \in \mathbb{N} \exists a_1, \ldots, a_n \in A : x \leq a_1 \vee \cdots \vee a_n\}.$$

Duálně, pro filtr $A{\uparrow}$ generovaný množinou A platí

$$A{\uparrow} = \{x \in G; \exists n \in \mathbb{N} \exists a_1, \ldots, a_n \in A : x \geq a_1 \wedge \cdots \wedge a_n\}.$$

Důkaz. Každý ideál svazu G obsahující množinu A musí pro každé $a_1, \ldots, a_n \in A$ obsahovat i $a_1 \vee \cdots \vee a_n$. Proto obsahuje i množinu

$$B = \{x \in G; \exists n \in \mathbb{N} \exists a_1, \ldots, a_n \in A : x \leq a_1 \vee \cdots \vee a_n\}.$$

Je tedy $A{\downarrow} \supseteq B$. Stačí ověřit, že B je ideál obsahující A. Inkluze $A \subseteq B$ je zřejmá, neboť pro $a \in A$ lze volit $n = 1$ a $a_1 = a$. Jistě B obsahuje s každým svým prvkem i všechny prvky svazu ještě menší, stačí tedy ověřit, že je B podsvaz. Nechť $x, y \in B$. Potom existují $a_1, \ldots, a_n \in A$ tak, že $x \leq a_1 \vee \cdots \vee a_n$, a existují $b_1, \ldots, b_m \in A$ tak, že $y \leq b_1 \vee \cdots \vee b_m$. Pak $x \wedge y \leq x \leq a_1 \vee \cdots \vee a_n$, a tedy $x \wedge y \in B$. Na druhou stranu $x \leq a_1 \vee \cdots \vee a_n \leq (a_1 \vee \cdots \vee a_n) \vee (b_1 \vee \cdots \vee b_m)$, podobně $y \leq b_1 \vee \cdots \vee b_m \leq (a_1 \vee \cdots \vee a_n) \vee (b_1 \vee \cdots \vee b_m)$, odkud $x \vee y \leq (a_1 \vee \cdots \vee a_n) \vee (b_1 \vee \cdots \vee b_m)$, proto $x \vee y \in B$. Je tedy B podsvaz, což se právě mělo dokázat. Tvrzení o filtrech plyne z duality.

Definice. *Nechť $(G, \leq)$, $(H, \preceq)$ jsou uspořádané množiny, $f : G \to H$ zobrazení. Řekneme, že je f izotonní zobrazení, jestliže pro každé $a, b \in G$ platí implikace*

$$a \leq b \Longrightarrow f(a) \preceq f(b).$$

Řekneme, že f je izomorfismus uspořádaných množin, je-li f bijekce a obě zobrazení f i f^{-1} jsou izotonní.

Definice. *Nechť G a H jsou svazy, $f : G \to H$ zobrazení. Řekneme, že je f svazový homomorfismus, jestliže pro každé $a, b \in G$ platí*

$$f(a \wedge b) = f(a) \wedge f(b), \qquad f(a \vee b) = f(a) \vee f(b).$$

Řekneme, že f je svazový izomorfismus (neboli izomorfismus svazů), je-li f bijektivní homomorfismus.

Poznámka. Protože každý svaz je také uspořádaná množina, má smysl se ptát, zda svazový homomorfismus je též izotonní zobrazení.

Věta 3.3. *Nechť G a H jsou svazy, $f : G \to H$ zobrazení.*

1. *Je-li f svazový homomorfismus, pak f je izotonní zobrazení a homomorfní obraz*
$$f(G) = \{f(a);\ a \in G\}$$
je podsvaz svazu H.

2. *Zobrazení f je svazový izomorfismus, právě když f je izomorfismus uspořádaných množin.*

Důkaz. Dokažme nejprve první část věty. Je-li f svazový homomorfismus, pak pro každé $a, b \in G$ z $a \leq b$ plyne $a = a \wedge b$, proto $f(a) = f(a \wedge b) = f(a) \wedge f(b)$, a tedy $f(a) \leq f(b)$. Je tedy f izotonní. To, že $f(G)$ je podsvaz svazu H, plyne přímo z definic.

Dokažme nyní druhou část věty. Nechť je f nejdříve svazový izomorfismus, ukážeme, že pak f^{-1} je svazový homomorfismus. Zvolme libovolně $c, d \in H$ a označme $a = f^{-1}(c)$, $b = f^{-1}(d)$. Pak platí

$$f^{-1}(c \vee d) = f^{-1}(f(a) \vee f(b)) = f^{-1}(f(a \vee b)) = a \vee b = f^{-1}(c) \vee f^{-1}(d),$$
$$f^{-1}(c \wedge d) = f^{-1}(f(a) \wedge f(b)) = f^{-1}(f(a \wedge b)) = a \wedge b = f^{-1}(c) \wedge f^{-1}(d).$$

Odvodili jsme, že f^{-1} je svazový homomorfismus. Aplikací první části věty na zobrazení f i f^{-1} dostaneme, že f je izomorfismus uspořádaných množin. Nechť nyní naopak f je izomorfismus uspořádaných množin, $a, b \in G$. Protože $a \leq a \vee b$, $b \leq a \vee b$ a f je izotonní zobrazení, dostáváme $f(a) \leq f(a \vee b)$, $f(b) \leq f(a \vee b)$, je tedy $f(a \vee b)$ horní závora prvků $f(a)$, $f(b)$. Nechť $c \in H$ je libovolný takový, že $f(a) \leq c$, $f(b) \leq c$. Protože f^{-1} je izotonní zobrazení, platí $a \leq f^{-1}(c)$, $b \leq f^{-1}(c)$, proto i $a \vee b \leq f^{-1}(c)$, a protože f je izotonní zobrazení, dostáváme $f(a \vee b) \leq c$. To ale znamená, že $f(a \vee b)$ je supremum prvků $f(a)$, $f(b)$, tj. $f(a) \vee f(b) = f(a \vee b)$. Analogicky (nebo z duality) pro infima.

4. Úplné svazy

Poznámka. Podle věty 2.4 v libovolném svazu má každá neprázdná konečná podmnožina $\{a_1, \ldots, a_n\}$ supremum $a_1 \vee \cdots \vee a_n$ a infimum $a_1 \wedge \cdots \wedge a_n$. Nekonečná podmnožina však supremum či infimum obecně mít nemusí.

Definice. *Uspořádaná množina, v níž pro každou podmnožinu existuje supremum i infimum, se nazývá úplný svaz.*

Poznámka. Každý úplný svaz G má nejmenší prvek (infimum množiny G ve svazu G) a největší prvek (supremum množiny G ve svazu G).

Poznámka. Promysleme si, co znamená infimum, resp. supremum, prázdné podmnožiny svazu G. Je-li $A \subseteq G$, pak infimum množiny A ve svazu G je největší dolní závora množiny A ve svazu G. Dolní závora množiny A ve svazu G je prvek $x \in G$ takový, že pro každé $a \in A$ platí $x \leq a$. V případě $A = \emptyset$ je tato podmínka splněna pro každé $x \in G$, a tedy odtud plyne, že každý prvek svazu G je v G dolní závorou prázdné množiny. Proto infimem prázdné množiny ve svazu G je největší prvek svazu G. Duálně: supremem prázdné množiny ve svazu G je nejmenší prvek svazu G.

Příklady. Zřejmě platí, že každý úplný svaz je svazem a podle věty 2.4 je každý neprázdný konečný svaz úplným svazem.

Příklad. Prázdný svaz není úplný, neboť pro jeho (jedinou) prázdnou podmnožinu neexistuje infimum ani supremum. Jinými slovy: prázdný svaz nemá nejmenší prvek ani největší prvek, protože nemá žádný prvek.

Příklad. Pro libovolnou množinu X je $(2^X, \subseteq)$ úplný svaz.

Příklad. Pro libovolnou nekonečnou množinu X tvoří množina všech konečných podmnožin množiny X spolu s inkluzí $\subseteq$ svaz, který není úplným svazem.

Příklad. Nekonečný řetězec nemusí být úplný svaz (například $(\mathbb{N}, \leq)$ není úplný svaz, neboť neexistuje supremum celé množiny $\mathbb{N}$).

Věta 4.1. *Nechť $(G, \leq)$ je uspořádaná množina. Následující podmínky jsou ekvivalentní:*

1. *$(G, \leq)$ je úplný svaz.*
2. *$(G, \leq)$ má nejmenší prvek a každá neprázdná podmnožina množiny G má v uspořádané množině $(G, \leq)$ supremum.*
3. *$(G, \leq)$ má největší prvek a každá neprázdná podmnožina množiny G má v uspořádané množině $(G, \leq)$ infimum.*

Poznámka. Vzhledem k předchozí poznámce víme, že podmínku 2 lze formulovat stručněji takto: každá podmnožina množiny G má v uspořádané množině $(G, \leq)$ supremum. Analogicky pro podmínku 3: každá podmnožina množiny G má v uspořádané množině $(G, \leq)$ infimum.

Důkaz. Snadno se vidí, že druhá a třetí podmínka jsou navzájem duální, zatímco první podmínka je duální sama k sobě. Stačí tedy ukázat, že první je ekvivalentní s druhou, ekvivalenci první s třetí pak dostaneme z duality.

Ihned z definice úplného svazu je vidět, že z první podmínky plyne druhá.

Předpokládejme tedy, že uspořádaná množina $(G, \leq)$ má nejmenší prvek a každá neprázdná podmnožina množiny G má v $(G, \leq)$ supremum, a ukažme, že $(G, \leq)$ je úplný svaz. Pak tedy i celá množina G má v $(G, \leq)$ supremum, což musí být největší prvek uspořádané množiny $(G, \leq)$. Proto prázdná množina má v $(G, \leq)$ infimum. Nechť A je neprázdná podmnožina množiny G a ukažme, že má v $(G, \leq)$ infimum. Označme B množinu všech dolních závor množiny A, tj.

$$B = \{x \in S; \forall a \in A : x \leq a\}.$$

Množina B je neprázdná, neboť jistě obsahuje nejmenší prvek uspořádané množiny $(G, \leq)$. Proto podle předpokladů má B supremum, které označíme m. Ukážeme-li, že $m \in B$, bude pak m největší ze všech dolních závor množiny A, tedy její infimum, a budeme hotovi. Pro libovolné $a \in A$ platí $x \leq a$ pro všechna $x \in B$, proto a je horní závora množiny B. Ovšem m je její supremum, tedy $m \leq a$. To však platí pro všechny $a \in A$, a proto $m \in B$, což jsme chtěli dokázat.

Příklad. Svaz všech podgrup dané grupy G je dle předchozí věty úplný svaz, neboť má největší prvek (celou grupu G) a každá neprázdná množina podgrup má v tomto svazu infimum, kterým je průnik těchto podgrup (to, že jejich průnikem je opět podgrupa, jsme dokazovali kvůli definici podgrupy generované podmnožinou grupy). Rovněž svaz všech podsvazů (popřípadě svaz ideálů nebo svaz filtrů) daného svazu je úplný svaz (viz větu 3.1). Díky analogickým větám o průnicích neprázdných systémů nějakých podstruktur lze totéž říci i o svazu všech podokruhů daného okruhu nebo o svazu jeho ideálů, o svazu všech podtěles daného tělesa nebo o svazu všech podprostorů daného vektorového prostoru.

Příklad. $(\mathbb{N} \cup \{\infty\}, \leq)$ je dle předchozí věty úplný svaz, neboť má největší prvek ∞ a každá neprázdná podmnožina množiny $\mathbb{N} \cup \{\infty\}$ má v $(\mathbb{N} \cup \{\infty\}, \leq)$ infimum (plyne z dobré uspořádanosti).

Příklad. Ze svazu $(\mathbb{N}, |)$, který není úplný, lze doplněním nuly (která se stane jeho největším prvkem) utvořit úplný svaz $(\mathbb{N} \cup \{0\}, |)$.

Poznámka. Jak ukazuje následující věta, předchozí případy nebyly nijak výjimečné: vždy existuje způsob, jak doplnit svaz tak, aby se stal úplným.

Věta 4.2. *Nechť G je svaz. Pak existuje úplný svaz U, který obsahuje podsvaz H, který je izomorfní se svazem G.*

Důkaz. Je jasné, že stačí najít vhodný úplný svaz U a injektivní svazový homomorfismus $f : G \to U$. Pak je totiž $f(G)$ podsvaz svazu U a zúžením oboru hodnot dostaneme svazový izomorfismus $f : G \to f(G)$.

Nechť U značí množinu všech ideálů svazu G. Ve větě 3.1 jsme ukázali, že průnik libovolného neprázdného systému prvků z U je opět prvkem U. Protože uspořádaná množina $(U, \subseteq)$ má největší prvek G, je to dle předchozí věty úplný svaz. Přitom pro libovolné dva prvky $A, B \in U$ je jejich infimem $A \wedge B = A \cap B$ množinový průnik, jejich supremem $A \vee B = (A \cup B)\!\downarrow$ je ideál generovaný množinovým sjednocením.

Uvažme zobrazení $f : G \to U$, které každý prvek svazu G zobrazí na ideál jím generovaný: pro každé $a \in G$ klademe $f(a) = a\!\downarrow$. Podle věty 3.2 je tedy $f(a) = \{x \in G;\, x \leq a\}$. Odtud plyne, že f je injekce: jsou-li totiž $a, b \in G$ takové, že $f(a) = f(b)$, pak $a \in b\!\downarrow$, odkud $a \leq b$, analogicky $b \leq a$, dohromady $a = b$.

Budeme hotovi, ukážeme-li, že f je svazový homomorfismus. Nechť $a, b \in G$ jsou libovolné. Máme ukázat, že

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

což znamená

$$(a \wedge b)\!\downarrow = a\!\downarrow \cap\, b\!\downarrow, \qquad (a \vee b)\!\downarrow = (a\!\downarrow \cup\, b\!\downarrow)\!\downarrow.$$

Nejprve ukážeme obě inkluze dokazující první rovnost. Protože $a \wedge b \leq a$, $a \wedge b \leq b$, platí $a \wedge b \in a\!\downarrow \cap\, b\!\downarrow$, odkud $(a \wedge b)\!\downarrow \subseteq a\!\downarrow \cap\, b\!\downarrow$. Naopak, je-li $x \in a\!\downarrow \cap\, b\!\downarrow$, je $x \leq a$, $x \leq b$, tedy $x \leq a \wedge b$, neboli $x \in (a \wedge b)\!\downarrow$. Nyní se zaměřme na druhou rovnost. Z nerovností $a \leq a \vee b$, $b \leq a \vee b$, plynou inkluze $a\!\downarrow \subseteq (a \vee b)\!\downarrow$, $b\!\downarrow \subseteq (a \vee b)\!\downarrow$, odkud $a\!\downarrow \cup\, b\!\downarrow \subseteq (a \vee b)\!\downarrow$ a proto i $(a\!\downarrow \cup\, b\!\downarrow)\!\downarrow \subseteq a \vee b\!\downarrow$. Na druhou stranu platí $a, b \in (a\!\downarrow \cup\, b\!\downarrow)\!\downarrow$, proto i $a \vee b \in (a\!\downarrow \cup\, b\!\downarrow)\!\downarrow$, odkud $(a \vee b)\!\downarrow \subseteq (a\!\downarrow \cup\, b\!\downarrow)\!\downarrow$.

Věta 4.3 (Tarski). *Nechť G je úplný svaz, $\varphi : G \to G$ izotonní zobrazení. Pak existuje prvek $a \in G$ tak, že $\varphi(a) = a$ (tj. a je pevný bod zobrazení φ).*

Důkaz. V úplném svazu existuje nejmenší prvek (infimum celého svazu); označme jej 0. Pak jistě $0 \leq \varphi(0)$, a proto množina

$$A = \{x \in G;\, x \leq \varphi(x)\}$$

je neprázdná. Označme a supremum množiny A (to existuje, neboť svaz je úplný). Pro každé $x \in A$ tedy platí $x \leq a$, a proto z izotonie $\varphi(x) \leq \varphi(a)$, což spolu s $x \leq \varphi(x)$ (vždyť $x \in A$) dává $x \leq \varphi(a)$. Je tedy $\varphi(a)$ horní závora množiny A, tedy její supremum $a \leq \varphi(a)$. Z izotonie $\varphi(a) \leq \varphi(\varphi(a))$, ale to znamená $\varphi(a) \in A$. Ovšem a je supremum množiny A, proto $\varphi(a) \leq a$. Celkem tedy $a = \varphi(a)$.

5. Součin svazů

Poznámka. Podobně jako jsme součinem grup $(G, \cdot)$, $(H, \cdot)$ získali grupu $(G \times H, \cdot)$ na kartézském součinu nosičů obou grup, můžeme součinem svazů získat nový svaz. Konstrukce bude naprosto stejná: operace na uspořádaných dvojicích se provedou nezávisle v každé složce.

Definice. *Nechť $(G, \vee, \wedge)$, $(H, \vee, \wedge)$ jsou svazy. Na kartézském součinu $G \times H$ definujme nové operace $\vee$ a $\wedge$ takto: pro každé $g_1, g_2 \in G$, $h_1, h_2 \in H$ klademe*

$$(g_1, h_1) \vee (g_2, h_2) = (g_1 \vee g_2, h_1 \vee h_2).$$
$$(g_1, h_1) \wedge (g_2, h_2) = (g_1 \wedge g_2, h_1 \wedge h_2).$$

Věta 5.1. *Za předpokladů učiněných v předchozí definici tvoří* $(G \times H, \vee, \wedge)$ *svaz.*

Důkaz. Důkaz je velmi snadný, ukažme například, že operace $\vee$ je komutativní: Pro každé $g_1, g_2 \in G$, $h_1, h_2 \in H$ platí

$$(g_1, h_1) \vee (g_2, h_2) = (g_1 \vee g_2, h_1 \vee h_2) = (g_2 \vee g_1, h_2 \vee h_1) = (g_2, h_2) \vee (g_1, h_1).$$

Všechny ostatní potřebné rovnosti se dokáží analogicky, vždy se využije, že dokazovaná rovnost platí v každém z obou svazů.

Poznámka. Jak jsme viděli v předchozím důkaze, v součinu svazů platí všechny rovnosti platné v obou svazech. Vlastnosti, které se však nedají vyjádřit jako konjunkce rovností, už součin svazů zdědit nemusí. Například vlastnost být řetězec můžeme zachytit takto: pro každé dva prvky x, y platí $x \leq y$ nebo $x \geq y$, což pomocí svazových operací lze zapsat podmínkou $x \wedge y = x$ nebo $x \wedge y = y$. To ale není konjunkce rovností, ale disjunkce. A skutečně, tato vlastnost se součinem nedědí: součinem dvou dvouprvkových řetězců je čtyřprvkový svaz, který není řetězec (to, že to tak opravdu dopadne, si promyslete sami).

Poznámka. Podobně jako součin dvou svazů jsme mohli definovat i součin n svazů pro libovolné $n \in \mathbb{N}$: na kartézském součinu nosných množin daných svazů se nové operace $\vee$ a $\wedge$ definují po složkách.

6. Modulární svazy

Poznámka. Viděli jsme ve větě 2.3, že v libovolném svazu G pro každou trojici prvků $a, b, c \in G$ takových, že $c \leq a$, platí modulární nerovnost

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

Definice. *Svaz G se nazývá modulární, jestliže pro každou trojici prvků $a, b, c \in G$ takových, že $c \leq a$, platí modulární rovnost*

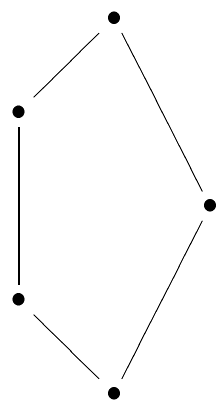
$$(a \wedge b) \vee c = a \wedge (b \vee c).$$

Příklad. Příklady modulárních svazů jsou svaz $(2^X, \cup, \cap)$ všech podmnožin nějaké množiny X nebo libovolný řetězec.

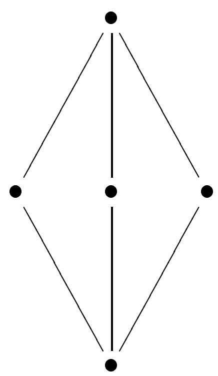
Příklad. Ukážeme, že svaz N_5, zvaný též pětiúhelník, není modulární, kdežto svaz M_5, zvaný též diamant, modulární je (viz Hasseovy diagramy na následujícím obrázku). Označme $0 < c < a < 1$ ony čtyři prvky, které jsou v Hasseově diagramu svazu N_5 nakresleny nad sebou vlevo, a b jeho pátý prvek. Pak nerovnost

$$(a \wedge b) \vee c = 0 \vee c = c < a = a \wedge 1 = a \wedge (b \vee c).$$

ukazuje, že svaz N_5 není modulární.



Svaz N_5 (pětiúhelník)



Svaz M_5 (diamant)

Nyní probírkou všech možností dokažme, že svaz M_5 je modulární. Označme 0 nejmenší a 1 největší prvek tohoto svazu. Nechť tedy $a, b, c \in M_5$ jsou libovolné takové, že $c \leq a$. Jestliže $a = c$, plyne modulární rovnost z absorpčních zákonů. Jestliže $c < a$, pak na Hasseově diagramu svazu M_5 vidíme, že buď $c = 0$ nebo $a = 1$. V obou případech je modulární rovnost zřejmá.

Věta 6.1. *Svaz všech normálních podgrup dané grupy je modulární.*

Důkaz. Nechť $(H, \cdot)$ je grupa, K, L její podgrupy. Každá podgrupa grupy $(H, \cdot)$, obsahující obě podgrupy K, L, musí obsahovat i množinu

$$K \cdot L = \{k \cdot l;\ k \in K, l \in L\}.$$

Tato množina obecně nemusí být podgrupou grupy $(H, \cdot)$. Ukažme, že pokud je K dokonce normální podgrupa grupy $(H, \cdot)$, pak je $K \cdot L$

podgrupou grupy $(H, \cdot)$. Jistě $K \cdot L \neq \emptyset$. Pro libovolné $k \in K$, $l \in L$ platí

$$(k \cdot l)^{-1} = l^{-1} \cdot k^{-1} = (l^{-1} \cdot k^{-1} \cdot l) \cdot l^{-1} \in K \cdot L,$$

neboť $l^{-1} \cdot k^{-1} \cdot l \in K$ díky tomu, že K je normální podgrupa grupy $(H, \cdot)$. Podobně pro libovolné $k_1, k_2 \in K$, $l_1, l_2 \in L$ platí

$$(k_1 \cdot l_1) \cdot (k_2 \cdot l_2) = k_1 \cdot (l_1 \cdot k_2 \cdot l_1^{-1}) \cdot (l_1 \cdot l_2) \in K \cdot L,$$

neboť opět $l_1 \cdot k_2 \cdot l_1^{-1} \in K$. Dokázali jsme, že $K \cdot L$ je podgrupou grupy $(H, \cdot)$. Protože $K \cdot L$ obsahuje podgrupy K i L, je tedy $K \cdot L$ nejmenší podgrupou grupy $(H, \cdot)$ obsahující obě podgrupy K, L. Přitom platí, že pokud jsou obě K i L normálními podgrupami grupy $(H, \cdot)$, pak je $K \cdot L$ též normální podgrupou grupy $(H, \cdot)$. Totiž pro libovolné $h \in H$ a libovolné $k \in K$, $l \in L$ platí

$$h \cdot (k \cdot l) \cdot h^{-1} = (h \cdot k \cdot h^{-1}) \cdot (h \cdot l \cdot h^{-1}) \in K \cdot L,$$

což bylo třeba dokázat.

Označme S množinu všech normálních podgrup grupy $(H, \cdot)$. Protože průnikem normálních podgrup je normální podgrupa, je $(S, \subseteq)$ svaz, v němž pro libovolné $K, L \in S$ platí

$$K \wedge L = K \cap L, \qquad K \vee L = K \cdot L.$$

Dokážeme, že je tento svaz modulární. Zvolme proto libovolně $K, L, M \in S$ tak, že $M \subseteq K$. Pak platí

$$(K \wedge L) \vee M = (K \cap L) \cdot M, \qquad K \wedge (L \vee M) = K \cap (L \cdot M).$$

Máme tedy ukázat, že platí

$$(K \cap L) \cdot M \supseteq K \cap (L \cdot M),$$

neboť opačná inkluze je modulární nerovnost platná v každém svazu (věta 2.3). Nechť je tedy $k \in K \cap (L \cdot M)$ libovolné. Pak existují $l \in L$, $m \in M$ takové, že platí $l \cdot m = k$. Z $M \subseteq K$ plyne $m \in K$, odkud $l = k \cdot m^{-1} \in K$. Je tedy $l \in (K \cap L)$ a platí $k = l \cdot m \in (K \cap L) \cdot M$, což jsme chtěli dokázat.

Důsledek. *Svaz všech podgrup dané komutativní grupy je modulární.*

Důkaz. V komutativní grupě je každá podgrupa normální.

Věta 6.2. *Podsvaz modulárního svazu je modulární svaz.*

Důkaz. Plyne přímo z definice: v podsvazu se suprema i infima počítají jako v původním svazu, proto je tam i stejné uspořádání.

Příklad. Svaz všech podprostorů daného vektorového prostoru V nad tělesem T je podle předchozí věty modulární. Je totiž podsvazem modulárního svazu všech podgrup grupy vektorů V – k tomu si stačí uvědomit, že každý podprostor je podgrupou, a ověřit, že infima i suprema se ve svazu všech podprostorů počítají stejně jako ve svazu podgrup: infimem je množinový průnik a supremem součet podprostorů.

Věta 6.3. *Svaz G je modulární, právě když pro každou trojici prvků $a, b, c \in G$ platí*

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

Důkaz. Je-li svaz modulární, plyne předchozí rovnost z modulární rovnosti pro prvky $a, b, a \wedge c$ a zřejmé nerovnosti $a \wedge c \leq a$. Naopak, nechť svaz G

splňuje rovnost této věty a nechť $a, b, c \in G$ jsou libovolné takové, že $c \leq a$. Pak platí $a \wedge c = c$, a tedy

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

což jsme měli dokázat.

Důsledek. *Součin modulárních svazů je modulární svaz. Homomorfní obraz modulárního svazu je modulární svaz.*

Důkaz. Už jsme zmiňovali v důkaze věty 5.1, že součin zdědí libovolnou rovnost platnou v obou svazech. Také tvrzení o homomorfních obrazech plyne z toho, že modularita je charakterizována rovností.

Věta 6.4. *Svaz G je modulární, právě když pro každou trojici prvků $a, b, c \in G$ platí implikace*

$$a \geq c,\ a \wedge b = c \wedge b,\ a \vee b = c \vee b \Longrightarrow a = c. \tag{1}$$

Důkaz. Předpokládejme, že svaz G je modulární a že pro trojici prvků $a, b, c \in G$ platí $c \leq a$, $a \wedge b = c \wedge b$, $a \vee b = c \vee b$. Pak z absorpčních zákonů a modulární rovnosti plyne

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

Naopak, předpokládejme, že ve svazu G platí implikace (1), a dokažme, že svaz je modulární. Zvolme libovolně trojici prvků $a, b, c \in G$ tak, že $c \leq a$, a označme $x = (a \wedge b) \vee c$, $y = a \wedge (b \vee c)$. Z modulární nerovnosti (věta 2.3) víme, že $x \leq y$. Ukážeme-li, že též platí $x \wedge b = y \wedge b$, $x \vee b = y \vee b$, podle implikace (1) dostaneme $x = y$, což je modulární rovnost pro prvky a, b, c. Z $x \leq y$ plyne $x \vee b \leq y \vee b$, neboť z $y \vee b \geq y \geq x$, $y \vee b \geq b$ je jasné, že $y \vee b$ je horní závora prvků x, b. Analogicky $x \wedge b \leq y \wedge b$. Ovšem

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

jistě $b \vee c \geq a \wedge (b \vee c) = y$ a $b \vee c \geq b$. To pak znamená $x \vee b = b \vee c \geq y \vee b$, což spolu s dříve odvozenou opačnou nerovností znamená $x \vee b = y \vee b$. Analogicky

$$y \wedge b = (a \wedge (b \vee c)) \wedge b = a \wedge ((b \vee c) \wedge b) = a \wedge b \leq (a \wedge b) \vee c = x,$$

jistě též $y \wedge b = a \wedge b \leq b$, proto $y \wedge b \leq x \wedge b$, opět s opačnou nerovností dostáváme potřebnou rovnost $x \wedge b = y \wedge b$.

Poznámka. Následující věta ukazuje, že modularitu je možné charakterizovat pomocí svazu N_5 (tj. pětiúhelníku, viz Hasseův diagram na straně 15).

Věta 6.5. *Svaz G je modulární, právě když neobsahuje podsvaz izomorfní se svazem N_5.*

Důkaz. Je-li svaz G modulární, pak podle věty 6.2 je každý jeho podsvaz modulární, proto svaz G neobsahuje podsvaz izomorfní se svazem N_5, neboť ten modulární není.

Naopak, předpokládejme, že svaz G není modulární. Podle předchozí věty existují $a, b, c \in G$ tak, že ačkoliv platí $a \geq c$, $a \wedge b = c \wedge b$, $a \vee b = c \vee b$, přesto $a \neq c$. Tedy $a > c$. Snadno se ověří, že pak nemůže nastat žádný z případů $b \geq c$ (pak by totiž $b = b \vee c = b \vee a$, tedy $b \geq a$, odkud $b \wedge a = a > c = b \wedge c$) ani $b \leq a$ (pak by $b = b \wedge a = b \wedge c$, tedy $b \leq c$, odkud $b \vee c = c < a = b \vee a$). Je tedy b s každým z prvků a, c nesrovnatelný. Proto jsou prvky $a, b, c, a \wedge b, a \vee b$ různé. Zřejmě tvoří pětiprvkový podsvaz svazu G izomorfní se svazem N_5.

Důsledek. *Duální svaz k modulárnímu svazu je opět modulární.*

Důkaz. Plyne z toho, že duální svaz ke svazu N_5 je izomorfní s N_5, a toho, že dualitou se podsvazy převádějí na podsvazy.

Poznámka. Předchozí důsledek je také možné snadno dokázat přímo: podmínka, kterou jsou modulární svazy definovány, je samoduální.

7. Distributivní svazy

Poznámka. Podle věty 2.3 v libovolném svazu G pro každou trojici prvků $a, b, c \in G$ platí distributivní nerovnosti

$$\begin{aligned} (a \vee b) \wedge (a \vee c) &\geq a \vee (b \wedge c), \\ (a \wedge b) \vee (a \wedge c) &\leq a \wedge (b \vee c). \end{aligned}$$

Definice. *Svaz G se nazývá distributivní, jestliže pro každou trojici prvků $a, b, c \in G$ platí distributivní rovnost*

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

Příklad. Příklady distributivních svazů jsou svaz všech podmnožin nějaké množiny nebo libovolný řetězec.

Příklad. Ověřte sami, že svazy N_5 (pětiúhelník) a M_5 (diamant) nejsou distributivní (viz Hasseovy diagramy na obrázku na straně 15). V obou svazech při ověřování zvolte tři různé prvky a, b, c tak, aby b bylo nesrovnatelné s a i c (a v N_5 navíc $a > c$).

Věta 7.1. *Nechť G je distributivní svaz. Pak pro každou trojici prvků $a, b, c \in G$ platí i následující distributivní rovnost*

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

Důkaz. Z distributivity a absorpčního zákona dostáváme

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

Poznámka. Duální tvrzení k předchozí větě znamená, že z podmínky z věty plyne podmínka z definice. Je tedy lhostejné, kterou z obou distributivních rovností užijeme v definici, mohli jsme užít i obě najednou.

Důsledek. *Duální svaz k distributivnímu svazu je opět distributivní.*

Věta 7.2. *Každý distributivní svaz je modulární.*

Důkaz. Předpokládejme, že G je distributivní svaz, $a, b, c \in G$ jsou takové, že $c \leq a$. Pak platí

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

což je modulární rovnost.

Věta 7.3. *Podsvaz distributivního svazu je distributivní svaz.*

Důkaz. Plyne přímo z definice: v podsvazu se suprema i infima počítají jako v původním svazu.

Věta 7.4. *Součin distributivních svazů je distributivní svaz. Homomorfní obraz distributivního svazu je distributivní svaz.*

Důkaz. Plyne z toho, že vlastnost být distributivní je definována rovností.

Věta 7.5. *Svaz G je distributivní, právě když pro každou trojici prvků $a, b, c \in G$ platí implikace*

$$a \wedge b = c \wedge b,\ a \vee b = c \vee b \Longrightarrow a = c. \tag{2}$$

Důkaz. Předpokládejme, že svaz G je distributivní a že pro trojici prvků $a, b, c \in G$ platí $a \wedge b = c \wedge b$, $a \vee b = c \vee b$. Pak z absorpčních zákonů a distributivity plyne

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

Naopak, předpokládejme, že svaz G splňuje implikaci (2). Podle věty 6.4 je G modulární, neboť splňuje implikaci (1). Nechť $x, y, z \in G$ jsou libovolné. Označme

$$a = ((y \vee x) \wedge z) \vee (x \wedge y),\\ b = y,\\ c = ((y \vee z) \wedge x) \vee (z \wedge y).$$

Tyto definice jsou voleny tak, že při záměně $x \leftrightarrow z$ se zamění $a \leftrightarrow c$. Protože $x \wedge y \leq y \vee x$, z modularity plyne

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

a podobně

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

Z komutativity, absorpce a modularity (díky $x \wedge y \leq y$) plyne

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

Stejnými úpravami při záměně $a \leftrightarrow c$ a $x \leftrightarrow z$

$$c \wedge b = b \wedge c = y \wedge (y \vee z) \wedge (x \vee (z \wedge y)) = y \wedge (x \vee (z \wedge y)) = (y \wedge x) \vee (z \wedge y).$$

Je tedy $a \wedge b = c \wedge b$. Z absorpce a modularity (díky $y \leq y \vee x$) dále plyne

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

Stejnými úpravami při záměně $a \leftrightarrow c$ a $x \leftrightarrow z$

$$c \vee b = ((y \vee z) \wedge x) \vee (z \wedge y) \vee y = ((y \vee z) \wedge x) \vee y = (y \vee z) \wedge (x \vee y).$$

Je tedy také $a \vee b = c \vee b$, což spolu s $a \wedge b = c \wedge b$ pomocí implikace (2) dává $a = c$. Z absorpce a modularity (díky $x \wedge y \leq x$) dostáváme

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

Podobně z komutativity a absorpce

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

Celkem tedy z toho, že $a = c$, a z komutativity plyne

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

Protože $x, y, z \in G$ byly libovolné, znamená to, že G je distributivní svaz, což jsme měli dokázat.

Poznámka. Z následující věty a věty 6.5 plyne analogie věty 6.5 pro distributivní svazy: Svaz G je distributivní, právě když neobsahuje ani podsvaz izomorfní se svazem M_5 (tj. diamant) ani podsvaz izomorfní se svazem N_5 (tj. pětiúhelník, viz Hasseovy diagramy na straně 15).

Věta 7.6. *Modulární svaz G je distributivní, právě když neobsahuje podsvaz izomorfní se svazem M_5.*

Důkaz. Je-li svaz G distributivní, pak podle věty 7.3 je každý jeho podsvaz distributivní, proto svaz G neobsahuje podsvaz izomorfní se svazem M_5, neboť ten distributivní není.

Naopak, předpokládejme, že svaz G není distributivní. Podle předchozí věty existují $a, b, c \in G$ tak, že ačkoliv platí $a \wedge b = c \wedge b$, $a \vee b = c \vee b$, přesto $a \neq c$. Kdyby $a \leq c$ nebo $c \leq a$, podle věty 6.4 by z modularity svazu plynulo $a = c$, což neplatí. Jsou tedy a a c nesrovnatelné. Označme

$$\begin{aligned} i &= a \wedge b = c \wedge b, \\ s &= a \vee b = c \vee b, \\ m &= ((a \vee c) \wedge b) \vee (a \wedge c). \end{aligned}$$

Je zřejmé, že $i \leq c$, a tedy $i = i \wedge c = a \wedge b \wedge c$. Podobně $s = a \vee b \vee c$. Z absorpce a modularity (díky $a \leq a \vee c$) plyne

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

Ovšem $b \vee a = s = a \vee b \vee c \geq a \vee c$, odkud $m \vee a = a \vee c$. Analogicky (záměnou $a \leftrightarrow c$) se dokáže, že $m \vee c = a \vee c$. Protože $a \wedge c \leq a \vee c$, plyne z modularity

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

Z absorpce a modularity (díky $a \wedge c \leq a$) plyne

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

Ovšem $a \wedge b = i = a \wedge b \wedge c \leq a \wedge c$, odkud $m \wedge a = a \wedge c$. Analogicky (záměnou $a \leftrightarrow c$) se dokáže, že $m \wedge c = a \wedge c$. Tvoří tedy $\{a, c, m, a \vee c, a \wedge c\}$ podsvaz svazu G. Ukažme, že c a m jsou nesrovnatelné. Z $c \leq m$ plyne $c = m \wedge c = a \wedge c$, odkud $c \leq a$, spor. Podobně z $c \geq m$ plyne $c = m \vee c = c \vee a$, odkud $a \leq c$, opět spor. Analogicky (záměnou $a \leftrightarrow c$) se dokáže, že a a m jsou nesrovnatelné. Proto podsvaz $\{a, c, m, a \vee c, a \wedge c\}$ svazu G je izomorfní se svazem M_5, což jsme chtěli dokázat.

Poznámka. Na závěr kapitoly o distributivních svazech si uvedeme charakterizaci konečných distributivních svazů.

Definice. *Prvek a svazu G se nazývá $\vee$-nedosažitelný, jestliže pro každé $b, c \in G$ takové, že $a = b \vee c$, platí $a = b$ nebo $a = c$.*

Poznámka. Prvek a svazu G je tedy $\vee$-nedosažitelný, jestliže není supremem žádných dvou prvků ostře menších než on, tj. neexistují $b, c \in G$ splňující $b < a$, $c < a$, $a = b \vee c$. Ekvivalentně lze tuto podmínku vyjádřit také takto: prvek a svazu G je $\vee$-nedosažitelný, jestliže pro každé $b, c \in G$ takové, že $b < a$ a současně $c < a$, platí $b \vee c < a$. Odtud se snadno dokáže indukcí, že takový prvek není supremem ani žádné neprázdné konečné množiny prvků ostře menších než on.

Označení. Množinu všech $\vee$-nedosažitelných prvků svazu G označíme $J(G)$.

Věta 7.7. *V konečném distributivním svazu G je libovolný prvek a roven supremu množiny všech $\vee$-nedosažitelných prvků, které neostře převyšuje, tj.*

$$a = \bigvee_{b \in J(G),\, b \leq a} b = \bigvee (a\!\downarrow \cap J(G)).$$

Důkaz. Budeme postupovat indukcí vzhledem k mohutnosti m nosné množiny svazu G. Je-li $m = 0$, není co dokazovat. Je-li $m = 1$, pak svaz obsahuje jediný prvek, který je $\vee$-nedosažitelný, a tedy tvrzení platí.

Předpokládejme tedy, že $m > 1$ a že pro všechny distributivní svazy o méně než m prvcích byla již věta dokázána. Nechť $a \in G$ je libovolný. Pokud $a \in J(G)$, zřejmě je a největším prvkem množiny $a\!\downarrow \cap J(G)$ a dokazovaná podmínka je pro něj zřejmě splněna. Nechť tedy $a \notin J(G)$, pak existují $b, c \in G$ splňující $b < a$, $c < a$, $a = b \vee c$. Uvažujme ideál $b\!\downarrow$. Zřejmě jde o podsvaz svazu G neobsahující a, tedy $|b\!\downarrow| < m$. Jako podsvaz distributivního svazu je distributivní a tedy podle indukčního předpokladu platí $b = \bigvee(b\!\downarrow \cap J(b\!\downarrow)) = \bigvee(b\!\downarrow \cap J(G))$, protože z definice ideálu plyne, že každý $\vee$-nedosažitelný prvek v podsvazu $b\!\downarrow$ je $\vee$-nedosažitelný vzhledem k celému G. Podobně platí $c = \bigvee(c\!\downarrow \cap J(G))$. Tedy $a = b \vee c = \bigvee(b\!\downarrow \cap J(G)) \vee \bigvee(c\!\downarrow \cap J(G)) = \bigvee D$, kde $D = (b\!\downarrow \cup c\!\downarrow) \cap J(G) \subseteq a\!\downarrow \cap J(G)$. Nechť $d = \bigvee(a\!\downarrow \cap J(G))$. Protože G je konečná množina, můžeme psát $a\!\downarrow \cap J(G) = \{a_1, \ldots, a_n\}$ pro nějaké přirozené n (tato množina není prázdná, neboť jistě obsahuje nejmenší prvek svazu G). Pak platí $d = \bigvee(a\!\downarrow \cap J(G)) = \bigvee_{i=1}^{n} a_i$, tedy pro infimum $a \wedge d$ díky distributivitě platí

$$a \wedge d = a \wedge \bigvee_{i=1}^{n} a_i = \bigvee_{i=1}^{n} (a \wedge a_i) = \bigvee_{i=1}^{n} a_i = d,$$

odkud dostáváme $a \geq d = \bigvee(a\!\downarrow \cap J(G)) \geq \bigvee D = a$, tedy

$$a = \bigvee (a\!\downarrow \cap J(G)),$$

což jsme chtěli dokázat.

Definice. *Nechť $(A, \leq)$ je uspořádaná množina. Množina $B \subseteq A$ se nazývá (dolů) dědičná, pokud pro každý prvek $b \in B$ a každý $a \in A$, $a \leq b$, platí $a \in B$.*

Poznámka. Množina $B \subseteq A$ je tedy dědičná, jestliže s každým svým prvkem obsahuje všechny prvky množiny A, které jsou ještě menší. Pomocí této vlastnosti můžeme charakterizovat ideály svazu: jsou to právě dědičné podsvazy. Připomeňme, že na svazy se můžeme dívat jako na uspořádané množiny a že dva svazy jsou izomorfní, právě když jsou izomorfní jako uspořádané množiny (věta 3.3).

Označení. Množinu všech neprázdných dědičných podmnožin uspořádané množiny A značíme $D(A)$.

Věta 7.8. *Pro konečný distributivní svaz G uvažme množinu $J(G)$ všech $\vee$-nedosažitelných prvků svazu G spolu s uspořádáním, které na $J(G)$ indukuje uspořádání svazu G. Pak uspořádaná množina $(D(J(G)), \subseteq)$ je izomorfní se svazem G (chápaným jako uspořádaná množina).*

Důkaz. Je-li G prázdný svaz, je i $D(J(G))$ prázdná množina a tedy věta platí. Dále předpokládejme, že G je neprázdný. Definujeme zobrazení $\eta : G \to D(J(G))$ předpisem $\eta(a) = a{\downarrow} \cap J(G)$. Zřejmě $a{\downarrow}$ je dědičná množina v G a její průnik s $J(G)$ je dědičnou množinou v $J(G)$. Navíc $a{\downarrow} \cap J(G)$ obsahuje nejmenší prvek svazu G, a tedy je prvkem $D(J(G))$. Ukážeme, že se jedná o izotonní zobrazení. Nechť $a, b \in G$ jsou libovolné takové, že $a \leq b$. Pak $a{\downarrow} \subseteq b{\downarrow}$, tedy $\eta(a) = a{\downarrow} \cap J(G) \subseteq b{\downarrow} \cap J(G) = \eta(b)$. Dále definujeme zobrazení $\vartheta : D(J(G)) \to G$ předpisem $\vartheta(X) = \bigvee X$, tj. $\vartheta(X)$ je supremem všech prvků množiny X. I toto zobrazení je izotonní, protože pro libovolné $X, Y \in D(J(G))$ takové, že $X \subseteq Y$, platí $\vartheta(X) = \bigvee X \leq \bigvee Y = \vartheta(Y)$. Ukážeme, že zobrazení η a ϑ jsou navzájem inverzní. Nechť $a \in L$, pak $\vartheta \circ \eta(a) = \vartheta(a{\downarrow} \cap J(G)) = \bigvee(a{\downarrow} \cap J(G)) = a$ podle věty 7.7. Nechť naopak $X \in D(J(G))$. Pak $\eta \circ \vartheta(X) = (\bigvee X){\downarrow} \cap J(G)$. Chceme, aby se složení zobrazení rovnalo identitě na množině $D(J(G))$, tedy aby

$$(\bigvee X){\downarrow} \cap J(G) = X.$$

Označme Y levou stranu požadované rovnosti. Inkluzi $X \subseteq Y$ dokážeme snadno: pro každé $x \in X$ zřejmě platí $x \leq \bigvee X$, a tedy $x \in (\bigvee X){\downarrow}$, a protože $x \in X \subseteq J(G)$, inkluze $X \subseteq Y$ platí. Nechť nyní $y \in Y$. Ptáme se, zda $y \in X$. Pro y však platí $y \leq \bigvee X$ a X je konečná neprázdná množina. Můžeme tedy psát $X = \{x_1, \ldots, x_n\}$ pro nějaké přirozené n, a tedy z distributivity

$$y = y \wedge \bigvee X = y \wedge \bigvee_{i=1}^{n} x_i = \bigvee_{i=1}^{n} (y \wedge x_i).$$

Ovšem $y \in J(G)$, a tedy y je $\vee$-nedosažitelný. Proto y nemůže být supremem menších prvků (viz poznámku za definicí $\vee$-nedosažitelnosti). Existuje tedy $i \in \{1 \ldots n\}$ tak, že $y = y \wedge x_i$, což znamená, že $y \leq x_i$. Ovšem $x_i \in X$, která je dědičná, tedy $y \in X$, což jsme potřebovali dokázat. Celkem tedy máme izotonní bijekci $\eta : G \to D(J(G))$ a její izotonní inverzi $\vartheta : D(J(G)) \to G$, jedná se tedy o izomorfismus uspořádaných množin.

Poznámka. Věta mimo jiné říká, že je-li G konečný distributivní svaz, pak i $D(J(G))$ je konečný distributivní svaz. Protože sjednocení i průnik dědičných množin je opět dědičná množina, jsou operacemi suprema a infima v $D(J(G))$ právě množinový průnik a sjednocení. Je tedy $D(J(G))$ podsvazem svazu všech podmnožin množiny $J(G)$.

Důsledek. *Každý konečný distributivní svaz je izomorfní s některým podsvazem svazu všech podmnožin nějaké konečné množiny.*

Poznámka. Podle předchozího důsledku každý konečný distributivní svaz můžeme chápat jako inkluzí uspořádaný systém množin, který je uzavřený na průniky a sjednocení. Protože naopak každý inkluzí uspořádaný systém množin, který je uzavřený na průniky a sjednocení, je zřejmě distributivním svazem, dostali jsme tak slíbenou charakterizaci konečných distributivních svazů. Uvědomte si, že podmínka uzavřenosti na množinový průnik a sjednocení je zde podstatná, vždyť například i nedistributivní svaz M_5 (diamant) je izomorfní se systémem množin $\{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2, 3\}\}$ uspořádaným inkluzí.

8. Booleovy algebry

Definice. *Nechť G je svaz s nejmenším prvkem 0 a největším prvkem 1. Řekneme, že prvek $b \in G$ je komplementem prvku $a \in G$ ve svazu G, jestliže platí $a \wedge b = 0$, $a \vee b = 1$. Svaz G se nazývá komplementární, jestliže ke každému prvku existuje aspoň jeden komplement.*

Poznámka. Z komutativity obou operací plyne, že je-li prvek b komplementem prvku a, pak je prvek a komplementem prvku b.

Příklad. Svazy M_5 a N_5 jsou komplementární (viz Hasseův diagram na straně 15), avšak k některým prvkům existuje komplementů více než jeden (nalezněte v každém z těchto svazů aspoň jeden takový prvek).

Příklad. Řetězec mající aspoň tři prvky není komplementární.

Poznámka. Podsvaz komplementárního svazu nemusí být komplementární: komplementární svaz N_5 obsahuje čtyřprvkový řetězec jako podsvaz.

Věta 8.1. *Součin komplementárních svazů je komplementární svaz.*

Důkaz. Nechť G a H jsou komplementární svazy, uvažme jejich součin $G \times H$. Protože pro každé $g \in G$, $h \in H$ platí

$$(g, h) \wedge (0, 0) = (g \wedge 0, h \wedge 0) = (0, 0),$$

je $(0,0)$ nejmenším prvkem svazu $G \times H$. Podobně se ověří, že $(1,1)$ je největším prvkem svazu $G \times H$. Pak pro libovolný komplement g_1 prvku g ve svazu G a pro libovolný komplement h_1 prvku h ve svazu H platí

$$\begin{aligned}(g,h) \wedge (g_1,h_1) &= (g \wedge g_1, h \wedge h_1) = (0,0),\\ (g,h) \vee (g_1,h_1) &= (g \vee g_1, h \vee h_1) = (1,1),\end{aligned}$$

a tedy (g_1,h_1) je komplementem prvku (g,h) ve svazu $G \times H$.

Poznámka. Duální svaz ke komplementárnímu svazu je komplementární (komplementy se zachovávají).

Věta 8.2. *V distributivním svazu je komplement prvku, pokud existuje, určen jednoznačně.*

Důkaz. Nechť a_1, a_2 jsou komplementy prvku b. Pak platí

$$a_1 \wedge b = 0 = a_2 \wedge b, \qquad a_1 \vee b = 1 = a_2 \vee b.$$

Podle věty 7.5 odtud plyne $a_1 = a_2$.

Definice. *Distributivní komplementární svaz se nazývá Booleova algebra.*

Poznámka. Nejmenší prvek Booleovy algebry budeme v dalším textu vždy značit 0 a její největší prvek 1. Komplement prvku $a \in G$ je dle předchozí věty určen jednoznačně, značíme jej a'.

Příklad. Prázdný svaz není Booleova algebra.

Příklad. V libovolné Booleově algebře platí $0' = 1$, $1' = 0$.

Příklad. Připomeňme, že pro libovolnou množinu X symbolem 2^X označujeme množinu všech podmnožin množiny X. Pro každou množinu X je $(2^X, \cup, \cap)$ Booleova algebra (uspořádáním je množinová inkluze): nejmenší prvek je $\emptyset$, největší prvek je X a komplementem prvku $A \subseteq X$ je prvek $X - A$.

Poznámka. Promyslete si, že duální svaz k Booleově algebře je Booleova algebra (komplementy se zachovávají, 0 a 1 se v dualitě vymění).

Věta 8.3. *Součinem Booleových algeber je Booleova algebra.*

Důkaz. Plyne z vět 7.4 a 8.1.

Věta 8.4. *V libovolné Booleově algebře pro každé prvky a, b platí*

1. $a'' = a$,
2. $(a \vee b)' = a' \wedge b'$,
3. $(a \wedge b)' = a' \vee b'$.

Důkaz. Prvky a'' i a jsou komplementy prvku a', z jednoznačnosti komplementu $a'' = a$. Druhou rovnost odvodíme z distributivního zákona:

$$\begin{aligned}(a \vee b) \vee (a' \wedge b') &= ((a \vee b) \vee a') \wedge ((a \vee b) \vee b') = \\ &= ((a \vee a') \vee b) \wedge ((b' \vee b) \vee a) = \\ &= (1 \vee b) \wedge (1 \vee a) = 1 \wedge 1 = 1,\end{aligned}$$

podobně

$$\begin{aligned}(a \vee b) \wedge (a' \wedge b') &= (a \wedge (a' \wedge b')) \vee (b \wedge (a' \wedge b')) = \\ &= ((a \wedge a') \wedge b') \vee ((b \wedge b') \wedge a') = \\ &= (0 \wedge b') \vee (0 \wedge a') = 0 \vee 0 = 0.\end{aligned}$$

Je tedy $a' \wedge b'$ komplementem prvku $a \vee b$, což jsme chtěli ukázat. Třetí rovnost dostaneme z druhé užitím duality.

Definice. *Podsvaz L Booleovy algebry G se nazývá Booleova podalgebra, jestliže $0, 1 \in L$ a pro každé $a \in L$ platí $a' \in L$.*

Příklad. V libovolné Booleově algebře tvoří $\{0, 1\}$ Booleovu podalgebru. Podobně pro každý její prvek a je $\{0, 1, a, a'\}$ Booleova podalgebra.

Příklad. Je-li X nekonečná množina, uvažme množinu

$$Y = \{A \subseteq X;\ A \text{ je konečná nebo } X - A \text{ je konečná}\}.$$

Pak Y je Booleova podalgebra Booleovy algebry $(2^X, \cup, \cap)$.

Věta 8.5. *Libovolná Booleova podalgebra je Booleova algebra.*

Důkaz. Jakožto podsvaz distributivního svazu je Booleova podalgebra distributivní svaz. Protože nejmenší (resp. největší) prvek Booleovy podalgebry je nejmenším (resp. největším) prvkem celé Booleovy algebry, z toho, že operace $\vee$ a $\wedge$ se v podsvazu počítají stejně jako v celém svazu, plyne, že komplement daného prvku v Booleově podalgebře je stejný jako komplement tohoto prvku v celé Booleově algebře. Je tedy Booleova podalgebra komplementární svaz, což jsme měli dokázat.

Definice. *Nechť G a H jsou Booleovy algebry, $f : G \to H$ zobrazení. Řekneme, že je f homomorfismus Booleových algeber, je-li f svazový homomorfismus, pro který platí $f(0) = 0$, $f(1) = 1$. Řekneme, že f je izomorfismus Booleových algeber, je-li f bijektivní homomorfismus Booleových algeber. Booleovy algebry G a H nazveme izomorfní, jestliže existuje izomorfismus Booleových algeber $f : G \to H$.*

Věta 8.6. *Nechť $f : G \to H$ je homomorfismus Booleových algeber, $a \in G$. Pak platí $f(a') = f(a)'$.*

Důkaz. Jistě platí

$$f(a') \vee f(a) = f(a' \vee a) = f(0) = 0, \qquad f(a') \wedge f(a) = f(a' \wedge a) = f(1) = 1,$$

odkud plyne, že $f(a)$ je komplementem prvku $f(a')$ v Booleově algebře H.

Definice. *Nechť G je Booleova algebra, $a \in G$, $a \neq 0$. Řekneme, že a je atom Booleovy algebry G, jestliže kromě* 0 *neexistuje žádný jiný prvek Booleovy algebry G menší než a.*

Věta 8.7. *Nechť G je konečná Booleova algebra, P množina všech jejích atomů. Pak G je izomorfní s Booleovou algebrou $(2^P, \cup, \cap)$.*

Důkaz. Je-li Booleova algebra G jednoprvková, je $P = \emptyset$ a věta zřejmě platí. Dále budeme předpokládat, že Booleova algebra G má aspoň dva prvky. Pro každý prvek $x \in G$, $x \neq 0$, existuje aspoň jeden $p \in P$, $p \leq x$ (jinak by pro každý nenulový prvek $y < x$ existoval nenulový prvek $z < y$, což by umožnilo konstruovat nekonečnou klesající posloupnost prvků, což v konečné množině zřejmě nelze).

Definujme zobrazení $h : G \to 2^P$ předpisem $h(b) = \{a \in P; a \leq b\}$. Ukážeme nejprve, že h je surjekce. Protože G je konečná, je i P konečná a tedy je konečná i libovolná podmnožina množiny P. Pro libovolné $a_1, \dots, a_n \in P$ zřejmě platí $\{a_1, \dots, a_n\} \subseteq h(a_1 \vee \cdots \vee a_n)$. Opačnou inkluzi dokažme sporem: předpokládejme, že existuje $x \in h(a_1 \vee \cdots \vee a_n)$, $x \notin \{a_1, \dots, a_n\}$. Pak $x \wedge a_1 = \cdots = x \wedge a_n = 0$, neboť infimum různých atomů je 0. Z $x \in h(a_1 \vee \cdots \vee a_n)$ plyne $x \leq a_1 \vee \cdots \vee a_n$, a tedy

$$x = x \wedge (a_1 \vee \cdots \vee a_n) = (x \wedge a_1) \vee \cdots \vee (x \wedge a_n) = 0 \vee \cdots \vee 0 = 0,$$

což je spor s tím, že $x \in P$. Je tedy h surjekce.

Ukažme nyní, že h je též injekce. Zvolme libovolně prvek $x \in G$, $x \neq 0$. Dokázali jsme, že existuje aspoň jeden $p \in P$, $p \leq x$. Proto $h(x) \neq \emptyset$. Označme $\{a_1, \dots, a_n\} = h(x)$. Ukážeme-li, že $x = a_1 \vee \cdots \vee a_n$, bude zřejmě h injekce. Označme $y = a_1 \vee \cdots \vee a_n$; protože $a_1 \leq x, \dots, a_n \leq x$, je $y \leq x$. Naším cílem je ukázat $x = y$, předpokládejme tedy, že $y < x$ a dojděme ke sporu. Platí $x = x \wedge 1 = x \wedge (y \vee y') = (x \wedge y) \vee (x \wedge y')$. Protože $y < x$, platí $x \wedge y = y \neq x$, a tedy $x \wedge y' \neq 0$ (uvědomte si, že dosazením $x \wedge y' = 0$ do předchozí rovnosti bychom dostali $x = x \wedge y$). Proto existuje atom p splňující $p \leq x \wedge y'$, tj. $p \leq x$, $p \leq y'$. Ovšem z $p \leq x$ plyne $p \in h(x) = \{a_1, \dots, a_n\}$, tedy $p = a_i$ pro vhodné i. Proto $p \leq a_1 \vee \cdots \vee a_n = y$, což spolu s dříve odvozenou nerovností $p \leq y'$ tedy dává $p \leq y' \wedge y = 0$, spor s tím, že p je atom.

Je tedy $h : G \to 2^P$ bijekce. Pro libovolné $x, y \in G$, $x \leq y$, jistě platí $h(x) \subseteq h(y)$. Naopak, odvodili jsme, že pro libovolné $X \subseteq P$ je $h^{-1}(X)$

supremum všech prvků z X. Odtud snadno plyne, že pro $X \subseteq Y \in 2^P$ platí $h^{-1}(X) \leq h^{-1}(Y)$. Je tedy h izomorfismus uspořádaných množin, a proto izomorfismus svazový. Jistě $h(0) = \emptyset$, $h(1) = P$. Je to tedy izomorfismus Booleových algeber.

9. Booleovy okruhy

Poznámka. V této kapitole ukážeme, že dvě algebraické struktury, totiž Booleovy algebry a speciální okruhy, tzv. Booleovy okruhy, jsou v podstatě totéž. S touto situací, kdy dva odlišné matematické objekty popisují stejnou situaci, jsme se setkali již několikrát: typickým příkladem jsou ekvivalence a rozklady na množině, nebo případ svazů jakožto speciálních uspořádaných množin nebo speciálních algebraických struktur se dvěma operacemi.

Definice. *Okruh $(R, +, \cdot)$ se nazývá Booleův okruh, je-li idempotentní, tj. pro každé $x \in R$ platí $x \cdot x = x$.*

Věta 9.1. *Netriviální Booleův okruh je komutativní okruh charakteristiky 2.*

Důkaz. Platí $1+1 = (1+1)\cdot(1+1) = 1\cdot 1+1\cdot 1+1\cdot 1+1\cdot 1 = 1+1+1+1$. Přičtením $-(1+1)$ dostaneme $1+1 = 0$. Protože okruh není triviální, platí $1 \neq 0$, a tedy má charakteristiku 2. Pro libovolné $x, y \in R$ platí

$$x + y = (x + y) \cdot (x + y) = x \cdot x + x \cdot y + y \cdot x + y \cdot y = x + x \cdot y + y \cdot x + y,$$

odkud $x \cdot y = -y \cdot x = y \cdot x$, což jsme měli dokázat.

Věta 9.2. *Nechť $(G, \vee, \wedge)$ je Booleova algebra. Definujme na množině G operace $+$ a $\cdot$ takto: pro libovolné $x, y \in G$ klademe*

$$x + y = (x \wedge y') \vee (x' \wedge y), \qquad x \cdot y = x \wedge y.$$

Pak $(G, +, \cdot)$ je Booleův okruh.

Poznámka. Všimněte si, že v případě Booleovy algebry $(2^X, \cup, \cap)$ všech podmnožin množiny X je výše definovanou operací $+$ právě symetrický rozdíl množin.

Důkaz. Je zřejmé, že obě operace jsou komutativní, násobení je i asociativní a idempotentní a pro každé $x \in G$ platí $x + 0 = x$, $x + x = 0$, $x \cdot 1 = x$. Dokažme asociativitu sčítání. Nechť $x, y, z \in G$ jsou libovolné. Z definice a věty 8.4 plyne

$$\begin{aligned}(x+y)+z &= \Big(\big((x\wedge y')\vee(x'\wedge y)\big)\wedge z'\Big)\vee\Big(\big((x\wedge y')\vee(x'\wedge y)\big)'\wedge z\Big) = \\ &= \Big(\big((x\wedge y')\vee(x'\wedge y)\big)\wedge z'\Big)\vee\big((x'\vee y)\wedge(x\vee y')\wedge z\big) = \\ &= (x\wedge y'\wedge z')\vee(x'\wedge y\wedge z')\vee \\ &\qquad \vee\Big(\big((x'\wedge x)\vee(x'\wedge y')\vee(y\wedge x)\vee(y\wedge y')\big)\wedge z\Big) = \\ &= (x\wedge y'\wedge z')\vee(x'\wedge y\wedge z')\vee\Big(\big((x'\wedge y')\vee(y\wedge x)\big)\wedge z\Big) = \\ &= (x\wedge y'\wedge z')\vee(x'\wedge y\wedge z')\vee(x'\wedge y'\wedge z)\vee(x\wedge y\wedge z).\end{aligned}$$

Poslední výraz se nezmění, provedeme-li s x, y, z jakoukoli permutaci. Proto

$$(x+y)+z = (y+z)+x = x+(y+z),$$

a tedy sčítání je asociativní, tudíž $(G,+)$ je komutativní grupa. Zbývá ověřit distributivní zákon. Nechť $x, y, z \in G$ jsou opět libovolné. Z definic a věty 8.4 plyne

$$\begin{aligned}x\cdot y + x\cdot z &= \big((x\wedge y)\wedge(x\wedge z)'\big)\vee\big((x\wedge y)'\wedge(x\wedge z)\big) = \\ &= \big(x\wedge y\wedge(x'\vee z')\big)\vee\big((x'\vee y')\wedge x\wedge z\big) = \\ &= (x\wedge y\wedge x')\vee(x\wedge y\wedge z')\vee(x'\wedge x\wedge z)\vee(y'\wedge x\wedge z) = \\ &= (x\wedge y\wedge z')\vee(x\wedge y'\wedge z) = \\ &= x\wedge\big((y\wedge z')\vee(y'\wedge z)\big) = x\cdot(y+z),\end{aligned}$$

což jsme chtěli dokázat.

Věta 9.3. *Nechť $(R,+,\cdot)$ je Booleův okruh. Definujme na množině R operace $\vee$ a $\wedge$ takto: pro libovolné $x, y \in R$ klademe*

$$x\vee y = x\cdot y + x + y, \qquad x\wedge y = x\cdot y.$$

Pak $(R,\vee,\wedge)$ je Booleova algebra, kde pro každé $x \in R$ platí $x' = x+1$.

Důkaz. Je zřejmé, že operace $\wedge$ je komutativní, asociativní a idempotentní. Jistě je též operace $\vee$ komutativní. Snadno se ověří, že také idempotentní. Nechť $x, y, z \in R$ jsou libovolné. Platí

$$\begin{aligned}(x\vee y)\vee z &= (x\cdot y+x+y)\cdot z + (x\cdot y+x+y)+z = \\ &= x\cdot y\cdot z + x\cdot z + y\cdot z + x\cdot y + x + y + z = \\ &= x\cdot(y\cdot z+y+z)+x+y\cdot z+y+z = x\vee(y\vee z),\end{aligned}$$

a tedy je $\vee$ asociativní operace. Ověřme absorpční zákony. Nechť $x, y, z \in R$ jsou opět libovolné. Platí

$$(x \vee y) \wedge x = (x \cdot y + x + y) \cdot x = x \cdot y \cdot x + x \cdot x + y \cdot x = x \cdot y + x \cdot y + x = x,$$

a také

$$(x \wedge y) \vee x = (x \cdot y) \cdot x + (x \cdot y) + x = x \cdot y + x \cdot y + x = x,$$

což jsme chtěli dokázat. Je tedy $(R, \vee, \wedge)$ svaz. Protože pro každé $x \in R$ je $x \wedge 0 = x \cdot 0 = 0$, platí $0 \leq x$, podobně $x \wedge 1 = x \cdot 1 = x$, a tedy $x \leq 1$. Proto je 0 nejmenší a 1 největší prvek tohoto svazu. Ověřme, že skutečně je $x + 1$ komplementem prvku x:

$$\begin{aligned}
x \wedge (x+1) &= x \cdot (x+1) = x \cdot x + x = x + x = 0, \\
x \vee (x+1) &= x \cdot (x+1) + x + (x+1) = 0 + x + x + 1 = 1.
\end{aligned}$$

Je tedy $(R, \vee, \wedge)$ komplementární svaz, zbývá ukázat, že je to též svaz distributivní. Nechť tedy $x, y, z \in R$ jsou opět libovolné. Platí

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

Věta je dokázána.

Věta 9.4. *Předchozí dvě věty nám dávají jednoznačnou korespondenci mezi Booleovými okruhy a Booleovými svazy.*

Důkaz. Je třeba ověřit, že pokud z Booleova okruhu vyrobíme Booleovu algebru a z ní opět Booleův okruh, dostaneme ten, se kterým jsme začínali, a také, že pokud z nějaké Booleovy algebry vyrobíme Booleův okruh a z něj opět Booleovu algebru, je to ta původní. To je zřejmé pro operace $\cdot$ a $\wedge$, které jsou totožné. Musíme to ověřit tedy pouze pro operace $+$ a $\vee$.

Mějme tedy Booleův okruh $(R, +, \cdot)$, uvažme k němu příslušnou Booleovu algebru $(R, \vee, \wedge)$, a k ní příslušný Booleův okruh $(R, \oplus, \cdot)$. Pro libovolné $x, y \in R$ tedy platí

$$\begin{aligned}
x \oplus y &= (x \wedge y') \vee (x' \wedge y) = \\
&= (x \cdot y') \cdot (x' \cdot y) + (x \cdot y') + (x' \cdot y) = \\
&= x \cdot (x+1) \cdot y \cdot (y+1) + x \cdot (y+1) + (x+1) \cdot y = \\
&= 0 + x \cdot y + x + x \cdot y + y = x + y.
\end{aligned}$$

Naopak, mějme nyní Booleovu algebru $(R, \vee, \wedge)$, uvažme k ní příslušný Booleův okruh $(R, +, \cdot)$, a k němu příslušnou Booleovu algebru $(R, \sqcup, \wedge)$. Pro libovolné $x, y \in R$ pak platí

$$\begin{aligned}
x \sqcup y &= x \cdot y + x + y = x + y + (x \wedge y) = \\
&= x + \Big(\big(y \wedge (x \wedge y)'\big) \vee \big(y' \wedge (x \wedge y)\big)\Big) = x + \Big(\big(y \wedge (x' \vee y')\big) \vee 0\Big) = \\
&= x + \big((y \wedge x') \vee (y \wedge y')\big) = x + \big((y \wedge x') \vee 0\big) = x + (y \wedge x') = \\
&= \big(x \wedge (y \wedge x')'\big) \vee \big(x' \wedge (y \wedge x')\big) = \big(x \wedge (y' \vee x)\big) \vee (x' \wedge y) = \\
&= x \vee (x' \wedge y) = (x \vee x') \wedge (x \vee y) = 1 \wedge (x \vee y) = x \vee y
\end{aligned}$$

což bylo třeba ověřit.

Poznámka. Podobné dvojí pohledy na jeden objekt bývají v matematice velmi cenné, neboť mnohdy ukáží nečekané souvislosti. Příkladem může být dualita, která je pro Booleovy algebry naprosto zřejmá. Výše uvedenou korespondencí se převádí též na Booleovy okruhy, kde už však není tak snadné si jí všimnout.