4. Uspořádané množiny, svazy a Galoisova korespondence

Relaci $\leq$ na množině M nazveme *uspořádáním* M, jestliže $\leq$ je reflexivní, tranzitivní a jestliže pro libovolná $a, b \in M$ z $a \leq b$ a $b \leq a$ plyne $a = b$.

Uspořádání, kde pro libovolné $a, b \in M$ platí $a \leq b$ nebo $b \leq a$, se nazývá *lineární*.

Poznámka. Často se používá jiné terminologie: relace uvedených vlastností se nazývá *částečné uspořádání*, přičemž uspořádáním se míní lineární uspořádání. Částečně uspořádané množiny se pak leckdy označují akronymem *poset* – z anglického 'partially ordered set'.

Dva prvky a, b uspořádané množiny $(M, \leq)$ se nazývají *porovnatelné*, je-li $a \leq b$ nebo $b \leq a$. V opačném případě jsou tyto prvky *neporovnatelné*. Prvek $a \in A \subseteq M$ se nazývá *minimální* prvek A, jestliže pro každé $b \in A$ porovnatelné s a je $a \leq b$. Podobně $a \in A \subseteq M$ se nazývá *maximální* prvek A, jestliže pro každé $b \in A$ porovnatelné s a platí $b \leq a$. Prvek $a \in A \subseteq M$ je *nejmenší* prvek A, pokud $a \leq b$ pro každé $b \in A$. Dále $a \in A \subseteq M$ je *největší* prvek A, je-li $b \leq a$ pro všechna $b \in A$. Každá množina $A \subseteq M$ má zjevně nanejvýš jeden největší a nanejvýš jeden nejmenší prvek.

Prvek $a \in M$ je *dolní závorou* množiny $A \subseteq M$, jestliže $a \leq b$ pro každé $b \in A$. Prvek $a \in M$ je *horní závorou* množiny $A \subseteq M$, jestliže $b \leq a$ pro každé $b \in A$. Všimněte si, že každý prvek $a \in M$ je dolní i horní závorou prázdné množiny.

Buď $A \subseteq M$. Označme na chvíli B množinu horních závor A a C množinu jeho dolních závor. Nejmenší prvek B (pokud existuje) se nazývá *supremum* A (značíme $\sup_{\leq} A$). Podobně největší dolní závoru (pokud existuje) nazýváme *infimum* A ($\inf_{\leq} A$).

Řekneme, že $b \in M$ *pokrývá* $a \in M$, jestliže $a \leq b$, $a \neq b$ a pro $a \leq c \leq b$ je buď $a = c$, nebo $b = c$. Někdy se pak píše $a \lessdot b$.

V $(\mathbb{Z}, \leq)$ je každé číslo k pokryté číslem $k + 1$. Naopak, v $(\mathbb{Q}, \leq)$ žádný prvek pokrytí nemá.

Je-li $(M, \leq)$ konečná uspořádaná množina, má v ní každý prvek pokrytí. Grafické zachycení relace pokrytí (a a b spojíme úsečkou právě když $a \lessdot b$, přičemž b umístíme výše než a) se nazývá *Hasseův diagram*.

Definujeme-li na M relaci $\preccurlyeq$ tak, že $a \preccurlyeq b$ právě když $b \leq a$, dostaneme opět uspořádání. Tomuto uspořádání se říká *opačné*. Při přechodu od $\leq$ k $\preccurlyeq$ se z maximálních prvků stanou minimimální, z horních závor dolní závory, ze suprem infima, a naopak.

4.1 Lemma. *Buď M_i, $i \in I$ podmnožiny uspořádané množiny $(M, \leq)$. Ať pro každé $i \in I$ je $b_i \in M$ supremem množiny M_i. Potom $\sup_{\leq}\{b_i; i \in I\}$ existuje právě když existuje $\sup_{\leq}(\bigcup(M_i;\ i \in I))$. Přitom obě suprema, pokud existují, si jsou rovna.*

Důkaz. Ať $b = \sup_{\leq}\{b_i; i \in I\}$. Je-li $a \in \bigcup(M_i; i \in I)$, je $a \in M_i$ pro nějaké $i \in I$, a tedy $a \leq b_i \leq b$. Je-li c takové, že $a \leq c$ pro všechna $a \in \bigcup(M_i; i \in I)$, je též $b_i \leq c$ pro všechna $i \in I$, takže $b \leq c$. Naopak, ať $m = \sup(\bigcup(M_i; i \in I))$. Pak $m \geq b_i$ pro každé $i \in I$. Je-li $d \geq b_i$ pro všechna $i \in I$, je i $d \geq a$ pro všechna $a \in \bigcup(M_i; i \in I)$, takže $d \geq m$. $\square$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

Podobné lemma lze vyslovit a dokázat též pro infima. Ovšem infima jsou suprema v opačném uspořádání, takže takovéto duální lemma je zřejmé a není nutné ho výslovně uvádět.

Předpokládejme nyní, že $(M, \leq)$ je taková uspořádaná množina, že každé dva prvky z M mají supremum i infimum. Pak z 4.1 indukcí okamžitě vyplývá, že každá konečná neprázdná množina má supremum i infimum. Označíme-li $a \vee b = \sup_{\leq}\{a, b\}$ a $a \wedge b = \inf_{\leq}\{a, b\}$ pro každé $a, b \in M$, dostáváme dvě binární operace na M (nazývají se *spojení* a *průsek*). Pro tyto operace platí

(komutativita)

$$a \wedge b = b \wedge a \quad \text{a} \quad a \vee b = b \vee a$$

(idempotence) $$a \wedge a = a = a \vee a$$

(asociativita)

$$(a \wedge b) \wedge c = a \wedge (b \wedge c) \quad \text{a} \quad (a \vee b) \vee c = a \vee (b \vee c)$$

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

Ověřit uvedené identity je snadné – přitom asociativita vyplývá z 4.1, neboť $(a \vee b) \vee c = \sup_{\leq}\{a, b, c\} = a \vee (b \vee c)$.

Algebra $M = M(\wedge, \vee)$, ve které jsou definovány binární operace $\wedge$ a $\vee$, jež splňují komutativní, idempotentní, asociativní a absorpční zákon, se nazývá *svaz*.

Ve svazu $M = M(\wedge, \vee)$ zaveďme relaci $\leq$ tak, že $a \leq b$ právě když $b = a \vee b$. Potom $a \leq a$ podle idempotentního zákona, $a \leq b$ a $b \leq c$ implikuje $a \vee c = a \vee (b \vee c) = (a \vee b) \vee c = b \vee c = c$ a z $a \leq b$, $b \leq a$ máme $b = a \vee b = b \vee a = a$. $(M, \leq)$ je tedy uspořádaná množina. Přitom pro každé $a, b \in M$ je $a \vee (a \vee b) = (a \vee a) \vee b = a \vee b$, takže $a \leq a \vee b$ a $b \leq a \vee b$. Je-li $c \geq a$ a $c \geq b$, je $c \vee (a \vee b) = (c \vee a) \vee b = c \vee b = c$, takže $a \vee b$ je supremum množiny $\{a, b\}$. Je-li $b = a \vee b$, je $a \wedge b = a \wedge (a \vee b) = a$. Naopak, je-li $a \wedge b = a$, je $a \vee b = a \vee (a \wedge b) = a$. To znamená, že $a \leq b$ platí právě když $a \wedge b = a$. Z této ekvivalentní definice uspořádání se analogicky dokáže, že $\inf\{a, b\} = a \wedge b$.

Z předchozího plyne, že svaz můžeme definovat ekvivalentně jako uspořádanou množinu, kde každé dva prvky mají supremum a infimum. Je zbytečné rozhodovat, zda prvotní by měla být tato definice, nebo definice vycházející z identit. V dalším budeme prostě předpokládat, že ve svazu máme definovány jak operace průseku a spojení, tak uspořádání.

Ve svazu může a nemusí existovat nejmenší a největší prvek. Pokud chceme existenci nejvyššího a nejmenšího prvku algebraicky zachytit, definujeme 'svaz s nulou a jedničkou' $M = M(\wedge, \vee, \mathbf{0}, \mathbf{1})$, kde navíc platí identity

$$a \wedge \mathbf{1} = a = a \vee \mathbf{0}.$$

(Důsledkem absorpčního zákona pak je, že $a \vee \mathbf{1} = \mathbf{1}$ a $a \wedge \mathbf{0} = \mathbf{0}$.)

Svaz nazveme *úplný*, jestliže každá množina má supremum a infimum. V úplném svazu tedy existuje největší a nejmenší prvek (uvědomte si, že největší prvek je infimem prázdné množiny).

Množina všech podmnožin dané množiny s uspořádáním inkluzí a operacemi průniku a sjednocení je úplný svaz. Jeho podsvazem je svaz konečných množin. Sjednocení konečných množin nemusí být konečná množina, proto na nekonečné množině není podsvaz konečných množin úplný. Soustavu $\mathcal{P}(M)$ všech podmnožin dané množiny M bychom však mohli také chápat jako $\mathbf{0}$,$\mathbf{1}$–svaz, ve kterém $\mathbf{0} = \emptyset$ a $\mathbf{1} = M$. Je-li M nekonečná množina, tak ovšem množina všech konečných podmnožin není podalgebra algebry $\mathcal{P}(M)(\cap, \cup, \mathbf{0}, \mathbf{1})$, třebaže je podalgebrou algebry $\mathcal{P}(M)(\cap, \cup)$.

4.2 Tvrzení. *Buď $\mathcal{C}$ uzávěrový systém nad množinou A. Potom $(\mathcal{C}, \subseteq)$ je úplný svaz, ve kterém pro $\mathcal{B} \subseteq \mathcal{C}$ platí $\inf \mathcal{B} = \bigcap(C;\ C \in \mathcal{B})$ a $\sup \mathcal{B} = \mathrm{cl}_{\mathcal{C}}(\bigcup(C;\ C \in \mathcal{B}))$.*

Důkaz. To, že $\inf \mathcal{B} = \bigcap(C;\ C \in \mathcal{B})$, plyne z toho, že $\bigcap(C;\ C \in \mathcal{B})$ je infimum v $\mathcal{P}(A)$. Položme $D = \bigcup(C;\ C \in \mathcal{B})$. Pak $C \subseteq \mathrm{cl}_{\mathcal{C}} D$ pro každé $C \in \mathcal{B}$, takže $\mathrm{cl}_{\mathcal{C}} D$ je horní závora. Je-li $E \in \mathcal{C}$ takové, že $C \subseteq E$ pro každé $C \in \mathcal{B}$, je $D \subseteq E$, a tedy $\mathrm{cl}_{\mathcal{C}} D \subseteq \mathrm{cl}_{\mathcal{C}} E = E$. $\square$

Všechny ekvivalence na množině A tvoří uzávěrový systém nad $A \times A$, takže podle 4.2 můžeme množinu všech ekvivalencí pokládat za svaz. Ze 4.2 a z 1.6 plyne, že spojení $\vee(\rho_i;\ i \in I)$, kde ρ_i jsou ekvivalence na A, je rovno $(\cup(\rho_i;\ i \in I))^+$.

Je-li $A = A(\alpha_1, \dots, \alpha_k)$ algebra, tak podle 2.8 a 2.12 lze za svaz považovat jak množinu všech podalgeber A (značívá se $\mathrm{Sub}(A)$), tak množinu všech kongruencí algebry A (značívá se $\mathrm{Con}(A)$). Sjednocení dvou podalgeber nemusí být podalgebrou, takže $\mathrm{Sub}(A)$ obvykle není podsvazem svazu $\mathcal{P}(A)$. Lze však dokázat (a není to obtížné), že $\mathrm{Con}(A)$ je vždy podsvazem svazu všech ekvivalencí na A.

Jestliže v axiomech svazu zaměníme $\wedge$ a $\vee$, axiomy se nezmění. Proto, když ke svazu $L = L(\wedge, \vee)$ definujeme algebru $L^{op} = L(\wedge_{op}, \vee_{op})$ tak, že $a \wedge_{op} b = a \vee b$ a $a \vee_{op} b = a \wedge b$, dostaneme opět svaz, tento svaz se nazývá svazem *opačným*. Označíme-li uspořádání v L symbolem $\leq$ a uspořádání v L^{op} symbolem $\leq_{op}$, vidíme, že $a \leq_{op} b$ právě když $a = a \wedge_{op} b = a \vee b$, což platí právě když $a \geq b$. Uspořádání v opačném svazu je tedy opačné uspořádání.

Jsou-li $(A, \leq)$ a $(B, \leq)$ dvě uspořádané množiny, tak zobrazení $f : A \to B$ se nazývá *monotonní*, jestliže pro všechna $a, b \in A$ z $a \leq b$ plyne $f(a) \leq f(b)$.

4.3 Lemma. *Buďte $L = L(\wedge, \vee)$ a $M = M(\wedge, \vee)$ dva svazy. Je-li $f : L \to M$ homomorfismus svazů, je f monotonní zobrazení.*

Důkaz. Ať $a, b \in L$ a $a \leq b$. Pak $f(a) \wedge f(b) = f(a \wedge b) = f(a)$, takže je $f(a) \leq f(b)$. $\square$

4.4 Tvrzení. *Buďte $L = L(\wedge, \vee)$ a $M = M(\wedge, \vee)$ dva svazy. Bijektivní zobrazení $f : L \to M$ je izomorfismus těchto svazů právě když f i f^{-1} jsou monotonní.*

Důkaz. Je-li f izomorfismus, jsou f a f^{-1} monotonní dle 4.3. Naopak, buďte f a f^{-1} monotonní a ať $a, b \in L$. Potom $f(a \wedge b) \leq f(a)$, $f(a \wedge b) \leq f(b)$ a pro $d \in M$ takové, že $d \leq f(a)$ a $d \leq f(b)$, existuje $c \in L$, že $f(c) = d$. Tudíž $c = f^{-1}(d) \leq f^{-1}(f(a)) = a$, a stejně tak $c \leq b$. Proto $c \leq a \wedge b$ a $f(c) = d \leq f(a \wedge b)$. Dokázali jsme $f(a \wedge b) = \inf\{f(a), f(b)\}$, takže nutně $f(a \wedge b) = f(a) \wedge f(b)$. Obdobně se ukáže $f(a \vee b) = f(a) \vee f(b)$. $\square$

4.5 Lemma. *Buďte $(A, \leq)$ a $(B, \leq)$ uspořádané množiny a ať $f : A \to B$ je prosté monotonní zobrazení. Je-li $a \in C \subseteq A$ nejmenší (největší) prvek C, je $f(a)$ nejmenší (největší) prvek $f(C) \subseteq B$.*

Důkaz. Buď $d = f(c)$ pro $c \in C$. Pak $a \leq c$, a proto $f(a) \leq f(c) = d$. $\square$

Buďte A a B dvě množiny. Dvojici zobrazení $\alpha : \mathcal{P}(A) \to \mathcal{P}(B)$ a $\beta : \mathcal{P}(B) \to \mathcal{P}(A)$ nazveme *Galoisovou korespondencí*, jestliže platí

(i) Z $A_1 \subseteq A_2 \subseteq A$ plyne $\alpha(A_2) \subseteq \alpha(A_1)$ a z $B_1 \subseteq B_2 \subseteq B$ plyne $\beta(B_2) \subseteq \beta(B_1)$, a to pro všechna $A_1 \subseteq A_2 \subseteq A$ a $B_1 \subseteq B_2 \subseteq B$.

(ii) Pro všechna $A_1 \subseteq A$ a $B_1 \subseteq B$ platí $\beta(\alpha(A_1)) \supseteq A_1$ a $\alpha(\beta(B_1)) \supseteq B_1$.

4.6 Lemma. *Buď $\alpha : \mathcal{P}(A) \to \mathcal{P}(B)$, $\beta : \mathcal{P}(B) \to \mathcal{P}(A)$ Galoisova korespondence. Potom $\alpha\beta\alpha(A_1) = \alpha(A_1)$ pro každé $A_1 \in \mathcal{P}(A)$ a $\beta\alpha\beta(B_1) = \beta(B_1)$ pro všechna $B_1 \in \mathcal{P}(B)$.*

Důkaz. Z (ii) máme $\alpha\beta(\alpha(A_1)) \supseteq \alpha(A_1)$ a $\beta\alpha(\beta(B_1)) \supseteq \beta(B_1)$. Naopak z $\beta\alpha(A_1) \supseteq A_1$ a $\alpha\beta(B_1) \supseteq B_1$ podle (i) plyne $\alpha\beta\alpha(A_1) \subseteq \alpha(A_1)$ a $\beta\alpha\beta(B_1) \subseteq \beta(B_1)$. □

4.7 Tvrzení. *Buď $\alpha : \mathcal{P}(A) \to \mathcal{P}(B)$, $\beta : \mathcal{P}(B) \to \mathcal{P}(A)$ Galoisova korespondence. Potom $\beta\alpha : \mathcal{P}(A) \to \mathcal{P}(A)$ a $\alpha\beta : \mathcal{P}(B) \to \mathcal{P}(B)$ jsou uzávěrové operátory. Označme $\mathcal{A} \subseteq \mathcal{P}(A)$ a $\mathcal{B} \subseteq \mathcal{P}(B)$ příslušné uzávěrové systémy. Pak $\alpha(A_1) \in \mathcal{B}$ a $\beta(B_1) \in \mathcal{A}$ pro všechna $A_1 \subseteq A$, $B_1 \subseteq B$. Označme $\alpha' : \mathcal{A} \to \mathcal{B}$ a $\beta' : \mathcal{B} \to \mathcal{A}$ odpovídající zúžení α a β. Zobrazení α' a β' jsou bijektivní a $\alpha' = (\beta')^{-1}$. Pro $A_1, A_2 \in \mathcal{A}$ je $A_1 \subseteq A_2$ právě když $\alpha(A_1) \supseteq \alpha(A_2)$.*

Důkaz. Z $A_1 \subseteq A_2 \subseteq A$ podle (i) dostáváme $\alpha(A_1) \supseteq \alpha(A_2)$, a opět podle (i) $\beta\alpha(A_1) \subseteq \beta\alpha(A_2)$. Podle 4.6 je $\beta\alpha\beta\alpha(A_1) = \beta\alpha(A_1)$. Dokázali jsme, že $\beta\alpha$ je uzávěrový operátor. Podobně je i $\alpha\beta$ uzávěrový operátor. Je-li $A_1 \subseteq A$, je $\alpha\beta\alpha(A_1) = \alpha(A_1)$, a tudíž $\alpha(A_1) \in \mathcal{B}$. Podobně $\beta(B_1) \in \mathcal{A}$ pro $B_1 \subseteq B$. Pro $A_1 \in \mathcal{A}$ je $\beta\alpha(A_1) = A_1$ a pro $B_1 \in \mathcal{B}$ je $\alpha\beta(B_1) = B_1$, takže α' a β' jsou vzájemně inverzní. Jsou-li $A_1, A_2 \in \mathcal{A}$, tak z $A_1 \subseteq A_2$ plyne $\alpha(A_1) \supseteq \alpha(A_2)$ podle (i). Platí-li $\alpha(A_1) \supseteq \alpha(A_2)$, tak $A_1 = \beta\alpha(A_1) \subseteq \beta\alpha(A_2) = A_2$. □

Poznámka. Díváme-li se na $\mathcal{A}$ a na $\mathcal{B}$ jako na svazy (viz 4.2), tak podle 4.4 je α' izomorfismus svazů $\mathcal{A}$ a $\mathcal{B}^{op}$. Izomorfismu svazu a opačného svazu se říká *antiizomorfismus.* (Je-li $f : L \to M$ antiizomorfismus svazů, je $f(a \wedge b) = f(a) \vee f(b)$ a $f(a \vee b) = f(a) \wedge f(b)$ pro libovolná $a, b \in L$.)

Tuto kapitolu zakončíme následujícím příkladem.

Buď $\rho \subseteq A \times B$. Definujme zobrazení $\alpha_\rho : \mathcal{P}(A) \to \mathcal{P}(B)$ tak, že pro $A_1 \subseteq A$ je $\alpha_\rho(A_1) = \{b \in B;\ a\rho b$ pro každé $a \in A_1\}$, a zobrazení $\beta_\rho : \mathcal{P}(B) \to \mathcal{P}(A)$ tak, že pro $B_1 \subseteq B$ je $\beta(B_1) = \{a \in A;\ a\rho b$ pro každé $b \in B_1\}$.

4.8 Tvrzení. *Buď dána relace $\rho \subseteq A \times B$. Potom $\alpha_\rho : \mathcal{P}(A) \to \mathcal{P}(B)$ a $\beta_\rho : \mathcal{P}(B) \to \mathcal{P}(A)$ tvoří Galoisovu korespondenci.*

Důkaz. Buď $A_1 \subseteq A$. Potom $\beta_\rho\alpha_\rho(A_1) = \{a' \in A;\ a'\rho b$ pro všechna $b \in \alpha_\rho(A_1)\}$. Je-li $a \in A_1$, je $a\rho b$ pro každé $b \in \alpha_\rho(A_1)$, takže $A_1 \subseteq \beta_\rho\alpha_\rho(A_1)$. Podobně $B_1 \subseteq \alpha_\rho\beta_\rho(B_1)$ pro libovolné $B_1 \subseteq B$. Pro $A_1 \subseteq A_2 \subseteq A$ je zjevně $\{b \in B;\ a\rho b$ pro všechna $a \in A_1\} \supseteq \{b \in B;\ a\rho b$ pro všechna $a \in A_2\}$, takže $\alpha_\rho(A_1) \supseteq \alpha_\rho(A_2)$, a obdobně $\beta_\rho(B_1) \supseteq \beta_\rho(B_2)$ pro $B_1 \subseteq B_2 \subseteq B$. □

Představme si nyní, že množina A je množina nějakých objektů, že množina B je množina vlastností (atributů) a že relace ρ značí, že objekt $a \in A$ má vlastnost $b \in B$. Buď $\mathcal{A} \subseteq \mathcal{P}(A)$ a $\mathcal{B} \subseteq \mathcal{P}(B)$ uzávěrové systémy dané Galoisovou korespondencí

α_ρ, β_ρ. Dvojici (C,D), kde $C \in \mathcal{A}$, $D \in \mathcal{B}$ a $D = \alpha_\rho(C)$, budeme říkat *koncept.* Koncept je tedy každá dvojice (C,D), kde $C \subseteq A$, $D \subseteq B$, $D = \alpha_\rho(C)$ a $C = \beta_\rho(D)$. Lze také říci, že koncept je dvojice množin objektů C a množin vlastností D, kde:

(1) každý objekt z C má všechny vlastnosti D,
(2) objekty z C nemají žádnou společnou vlastnost z $B \backslash D$,
(3) všechny objekty A, které mají všechny vlastnosti D, patří do C.

Přiřazení $C \mapsto (C,D)$ je bijekce $\mathcal{A}$ na množinu všech konceptů $\mathcal{K}$. Protože A je svaz, indukuje tato bijekce svazové operace na $\mathcal{K}$. Můžeme proto mluvit o *svazu konceptů.* Uspořádání ve svazu konceptů je tedy zvoleno tak, že jeden koncept je 'větší' než druhý, jestliže se týká většího množství objektů, tj. jestliže je obecnější.

Vytváření svazů konceptů je jedním z nástrojů *pojmové analýzy.*