1. Uzávěrové systémy, relace a ekvivalence

Množinu všech podmnožin množiny A budeme značit $\mathcal{P}(A)$ a nazývat *potencí* nebo *potenční množinou* A. Je tedy

$$\mathcal{P}(A) = \{B;\quad B \subseteq A\}.$$

Specielně, $A \in \mathcal{P}(A)$ a $\emptyset \in \mathcal{P}(A)$.

Je-li A množina a $\mathcal{C} \subseteq \mathcal{P}(A)$, nazveme $\mathcal{C}$ *uzávěrovým systémem nad* A, jsou-li splněny tyto podmínky:

(i) $A \in \mathcal{C}$,
(ii) Jsou-li $B_i \in \mathcal{C}$, $i \in I \neq \emptyset$, je $\bigcap(B_i;\, i \in I) \in \mathcal{C}$.

Vyjádřeno slovně, systém podmnožin $\mathcal{C}$ množiny A je uzávěrovým systémem nad A, jestliže obsahuje A a je uzavřen na průniky.

Je-li B podmnožina množiny A a $\mathcal{C}$ je uzávěrový systém nad A, tak mezi množinami z $\mathcal{C}$, které obsahují B, je podle (i) jistě množina A. Soustava $\{C \in \mathcal{C};\, B \subseteq C\}$ je proto vždy neprázdná. Označme E průnik $\cap\{C \in \mathcal{C};\, B \subseteq C\}$. Množina E obsahuje množinu B a podle (ii) patří do uzávěrového systému $\mathcal{C}$. Množina E byla přitom definována tak, aby ležela v každé množině z $\mathcal{C}$, jež obsahuje B. Proto je E nejmenší množinou z $\mathcal{C}$, jež obsahuje B. Budeme ji značit $\mathrm{cl}_{\mathcal{C}}(B)$ a nazývat *uzávěrem* B v $\mathcal{C}$ nebo *množinou generovanou v* $\mathcal{C}$ *množinou* B. Všimněte si, že $\mathrm{cl}_{\mathcal{C}}(C) = C$ platí právě když C patří do $\mathcal{C}$.

Zobrazení $\alpha : \mathcal{P}(A) \to \mathcal{P}(A)$ nazýváme *uzávěrový operátor na množině* A, jestliže má tyto vlastnosti:

(i) $B \subseteq \alpha(B)$ pro všechna $B \subseteq A$ (extenzita),
(ii) $\alpha(\alpha(B)) = \alpha(B)$ pro všechna $B \subseteq A$ (idempotence),
(iii) kdykoliv $B \subseteq C \subseteq A$, tak $\alpha(B) \subseteq \alpha(C)$ (monotónnost).

1.1 Tvrzení.

(i) *Je-li* $\mathcal{C}$ *uzávěrový systém nad* A*, je* $\mathrm{cl}_{\mathcal{C}}$ *uzávěrový operátor na* A.
(ii) *Je-li* α *uzávěrový operátor na* A*, tvoří* $\mathcal{C} = \{C \subseteq A;\, \alpha(C) = C\}$ *uzávěrový systém nad* A *a* $\alpha = \mathrm{cl}_{\mathcal{C}}$.

Důkaz. Část (i) plyne přímo z definice uzávěrového systému. Budeme proto dokazovat jen část (ii). Buď α uzávěrový operátor a ať C_i, $i \in I$, je neprázdná soustava podmnožin množiny A takových, že $\alpha(C_i) = C_i$ pro každé $i \in I$. Podle (i) je $\bigcap C_i \subseteq \alpha(\bigcap C_i)$. Podle (iii) je $\alpha(\bigcap C_i) \subseteq \alpha(C_i) = C_i$ pro každé $i \in I$, takže $\alpha(\bigcap C_i) = \bigcap C_i$. Dokázali jsme, že $\mathcal{C}$ je uzávěrový systém. Je-li $B \subseteq A$, je $\alpha(B) \in \mathcal{C}$ podle (ii). Tudíž $\mathrm{cl}_{\mathcal{C}}(B) \subseteq \alpha(B)$. Naopak, z $B \subseteq \mathrm{cl}_{\mathcal{C}}(B)$ dostáváme podle (iii) $\alpha(B) \subseteq \alpha(\mathrm{cl}_{\mathcal{C}}(B)) = \mathrm{cl}_{\mathcal{C}}(B)$. $\square$

Uzávěrové operátory a uzávěrové systémy jsou tudíž ve vzájemně jednoznačném vztahu.

1.2 Tvrzení. *Všechny uzávěrové systémy nad* A *tvoří uzávěrový systém nad* $\mathcal{P}(A)$.

Důkaz. $\mathcal{P}(A)$ je uzávěrový systém nad A. Jsou-li $\mathcal{C}_i$, $i \in I \neq \emptyset$, uzávěrové systémy nad A a pro $j \in J \neq \emptyset$ je $B_j \in \mathcal{C}_i$ pro všechna $i \in I$, je i $\bigcap(B_j;\, j \in J) \in \bigcap(\mathcal{C}_i;\, i \in I)$. $\square$

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

1.3 Lemma. *Buď $\mathcal{A}$ a $\mathcal{B}$ uzávěrové systémy nad A. Je-li $\mathcal{A} \subseteq \mathcal{B}$, tak $\mathrm{cl}_{\mathcal{B}}(C) \subseteq \mathrm{cl}_{\mathcal{A}}(D)$ kdykoliv $C \subseteq D \subseteq A$.*

Důkaz. $\mathrm{cl}_{\mathcal{B}}(C) \subseteq \mathrm{cl}_{\mathcal{B}}(D) \subseteq \mathrm{cl}_{\mathcal{A}}(D)$. □

Relací z A do B rozumíme každou podmnožinu $A \times B$. *Relací na A* rozumíme relaci z A do A. Místo $(a,b) \in \rho$, kde ρ je relace, píšeme často $a\rho b$. Relaci $\{(a,a); a \in A\}$ značíme id_A (čteme *identita na A*). Je-li $\rho \subseteq A \times B$, značí ρ^{-1} *opačnou relaci*, $\rho^{-1} = \{(b,a);\, (a,b) \in \rho\}$.

Je-li ρ relace na A, označuje ρ^+ tu relaci na A, kde $(a,b) \in \rho^+$ právě když existuje posloupnost $c_0, c_1, \ldots, c_k \in A$ taková, že $a = c_0$, $b = c_k$, $k \geq 1$ a $c_{i-1}\rho c_i$ pro všechna $1 \leq i \leq k$.

Buď ρ relace na A. Tato relace se nazývá
- *reflexivní*, jestliže $\mathrm{id}_A \subseteq \rho$;
- *antireflexivní*, jestliže $\mathrm{id}_A \cap \rho = \emptyset$;
- *symetrická*, jestliže $\rho = \rho^{-1}$;
- *antisymetrická*, jestliže $\rho \cap \rho^{-1} = \emptyset$;
- *tranzitivní*, jestliže z $a\rho b$, $b\rho c$ plyne $a\rho c$ pro všechna $a, b, c \in A$.

1.4 Tvrzení. *Reflexivní (resp. symetrické, resp. tranzitivní) relace na množině A tvoří uzávěrový systém nad $A \times A$. Označíme-li tento systém $\mathcal{C}$, je $\mathrm{cl}_{\mathcal{C}}(\rho)$ pro $\rho \subseteq A \times A$ rovno $\rho \cup \mathrm{id}_A$ (resp. $\rho \cup \rho^{-1}$, resp. ρ^+).*

Důkaz. $\rho \cup \mathrm{id}_A$ (resp. $\rho \cup \rho^{-1}$, resp. ρ^+) musí být obsaženo v každé reflexivní (resp. symetrické, resp. tranzitivní) relaci, která obsahuje ρ. Současně ale $\rho \cup \mathrm{id}_A$ (resp. $\rho \cup \rho^{-1}$, resp. ρ^+) je samo reflexivní (resp. symetrické, resp. tranzitivní). □

Relace ρ nad A, která je současně reflexivní, symetrická a tranzitivní, se nazývá *ekvivalence* na A. Z 1.2 a 1.4 vyplývá, že všechny ekvivalence na A tvoří uzávěrový systém nad $A \times A$.

1.5 Lemma. *Buď ρ relace na A.*

(i) *Je-li ρ reflexivní, jsou ρ^+ i $\rho \cup \rho^{-1}$ reflexivní.*
(ii) *Je-li ρ symetrická, je ρ^+ symetrická.*

Důkaz. Snadný. □

Pro ρ relaci na A pišme na chvíli $ref(\rho)$ místo $\rho \cup \mathrm{id}_A$, $sym(\rho)$ místo $\rho \cup \rho^{-1}$ a $tra(\rho)$ místo ρ^+. Podle 1.4 je na místě o ref, sym a tra hovořit jako o reflexivním, symetrickém a tranzitivním uzávěru. Ukážeme, že jejich kombinací lze vždy popsat nejmenší ekvivalenci obsahující danou relaci.

1.6 Tvrzení. *Buď ρ relace na množině A. Potom*

$$tra(sym(ref(\rho))) = ((\rho \cup \mathrm{id}_A) \cup (\rho \cup \mathrm{id}_A)^{-1})^+$$

je nejmenší ekvivalence na A, která obsahuje relaci ρ.

Důkaz. Označme equ uzávěrový operátor příslušející uzávěrovému systému všech ekvivalencí na množině A. Potom z 1.3 dostáváme inkluzi $tra(sym(ref(\rho))) \subseteq equ(equ(equ(\rho))) = equ(\rho)$. Z 1.5 vyplývá, že $tra(sym(ref(\rho)))$ je ekvivalence. □

Je-li ρ ekvivalence na A a $a \in A$, tak $[a]_\rho = \{b;\, a\rho b\}$ budeme nazývat *ekvivalenční třídou* ρ, nebo též ekvivalenční třídou *modulo* ρ. Klademe $A/\rho = \{[a]_\rho;\ a \in A\}$. Množina A/ρ se nazývá *kvocient* A *modulo* ρ.

Je-li A množina, tak $\mathcal{B} \subseteq \mathcal{P}(A)$ nazveme *rozkladem* A, jestliže

(i) $A = \bigcup(B;\ B \in \mathcal{B})$,
(ii) $B \cap C = \emptyset$, jestliže $B, C \in \mathcal{B}$ a $B \neq C$, a
(iii) $\emptyset \notin \mathcal{B}$.

1.7 Tvrzení. *Je-li* ρ *ekvivalence na* A*, je* $\{[a]_\rho;\ a \in A\}$ *rozklad množiny* A.

Důkaz. Pro všechna $a \in A$ je $a \in [a]_\rho$, takže podmínky (i) a (ii) jsou jistě splněny. Jestliže $b, c \in A$ a $d \in [b]_\rho \cap [c]_\rho$, tak pro každé $a \in [b]_\rho$ máme $a\rho b\rho d\rho c$, čili $a \in [c]_\rho$, a tedy $[b]_\rho \subseteq [c]_\rho$. Opačnou inkluzi dostaneme stejným postupem, a proto platí $[b]_\rho = [c]_\rho$. $\square$

Každý rozklad množiny A naopak určuje ekvivalenci na A, jejíž ekvivalenční třídy jsou právě množiny tohoto rozkladu.

Je-li ρ ekvivalence na A, tak platí $\mathrm{id}_A \subseteq \rho \subseteq A \times A$. Ekvivalenci id_A odpovídá rozklad na jednobodové množiny, a obvykle se jí říká *triviální* ekvivalence.

Ekvivalence $A \times A$ odpovídá rozkladu, který obsahuje jedině množinu A. Tato ekvivalence se nejčastěji označuje jako *universální* ekvivalence.

Ekvivalenci ρ nazýváme *vlastní*, jestliže neplatí ani $\rho = \mathrm{id}_A$ ani $\rho = A \times A$.

V algebře, ale i jinde v matematice, se často pracuje s ekvivalencemi kvocientu A/ρ. Předpokládejme, že σ je nějaká další ekvivalence na A, a ať σ obsahuje ρ. Na A/ρ definujeme relaci σ/ρ tak, že pro rozkladové třídy $B, C \in A/\rho$ je

$$(B, C) \in \sigma/\rho \Longleftrightarrow (b, c) \in \sigma \text{ platí pro všechna } \ b \in B \text{ a } \ c \in C.$$

1.8 Lemma.

(i) *Pro* $b, c \in A$ *platí* $([b]_\rho, [c]_\rho) \in \sigma/\rho$ *právě když je* $(b, c) \in \sigma$.
(ii) *Relace* σ/ρ *je ekvivalence.*

Důkaz. (i) Ať je $(b, c) \in \sigma$ a ať $b' \in A$ patří do $[b]_\rho$ a $c' \in A$ do $[c]_\rho$. Je třeba dokázat $(b', c') \in \sigma$. Ovšem $(b', b) \in \rho$ a $(c', c) \in \rho$ implikují $(b', b) \in \sigma$ a $(c', c) \in \sigma$, neboť platí $\rho \subseteq \sigma$. Stačí tedy použít tranzitivitu ekvivalence σ.
(ii) Ať $B, C, D \in A/\rho$ jsou rozkladové třídy ekvivalence ρ. Vyberme prvky $b \in B$, $c \in C$ a $d \in D$. Je tedy $B = [b]_\rho$, $C = [c]_\rho$ a $D = [d]_\rho$. Předpokládejme, že platí $(B, C) \in \sigma/\rho$ a $(C, D) \in \sigma/\rho$. Podle definice musí být $(b, c) \in \sigma$ a $(c, d) \in \sigma$, takže je rovněž $(b, d) \in \sigma$. Ovšem to podle (i) implikuje $(B, D) \in \sigma/\rho$. Relace σ/ρ je tedy tranzitivní. Symetrie a reflexivita se dokáží podobně. $\square$

1.9 Tvrzení. *Ať* ρ *je ekvivalence na množině* A *a ať* η *je ekvivalence na* A/ρ*. Pak existuje právě jedna ekvivalence* $\sigma \supseteq \rho$ *na* A*, pro kterou platí* $\eta = \sigma/\rho$.

Důkaz. Má-li být $\eta = \sigma/\rho$, tak podle 1.8(ii) musí být $(b, c) \in \sigma$ právě když je $([b]_\rho, [c]_\rho) \in \eta$. Tento vztah σ jednoznačně určuje, takže ho lze použít jako definici. Je třeba ukázat, že takto definovaná relace σ je ekvivalence, obsahuje ρ a splňuje $\eta = \sigma/\rho$.

To, že σ je ekvivalence, se okamžitě odvodí z toho, že η je ekvivalence.

Uvažme prvky b, c množiny A,

Je-li $(b, c) \in \rho$, je $[b]_\rho$ rovno $[c]_\rho$, takže jistě platí $([b]_\rho, [c]_\rho) \in \eta$, a tedy i $(b, c) \in \sigma$.

Vztah $([b]_\rho, [c]_\rho) \in \eta$ lze podle definice σ vyjádřit jako $(b, c) \in \sigma$, což podle 1.8(i) nastane právě když platí $([b]_\rho, [c]_\rho) \in \sigma/\rho$. Tím je dokázáno, že ekvivalence η a σ/ρ se shodují. $\square$

Zobrazením $f : A \to B$ rozumíme, jak je obvyklé, takovou relaci z A do B, že pro každé $a \in A$ existuje právě jedno $b \in B$ takové, že $(a, b) \in f$. Přitom píšeme $b = f(a)$.

Zobrazení f se nazývá *injektivní* (*prosté*), jestliže $f(a_1) = f(a_2)$ implikuje $a_1 = a_2$ pro všechna $a_1, a_2 \in A$. Zobrazení f je *surjektivní* (zobrazení *na*), jestliže pro každé $b \in B$ existuje takové $a \in A$, že $b = f(a)$.

Zobrazení f nazveme *bijektivní*, jestliže je současně injektivní a surjektivní.

Je-li dáno zobrazení $f : A \to B$, tak obor hodnot $\{f(a);\ a \in A\}$ označujeme $\mathrm{Im}(f)$. Zobrazení $f : A \to B$ je tedy surjektivní právě když $\mathrm{Im}(f) = B$.

Je-li $f : A \to B$ zobrazení, tak *jádrem* tohoto zobrazení nazýváme ekvivalenci $\ker f$ danou vztahem: $(a, b) \in \ker f$ právě když $f(a) = f(b)$.

Zobrazení z A do A/ρ, $a \mapsto [a]_\rho$ se nazývá *přirozené* (naturální) zobrazení podle ρ a budeme ho značit nat_ρ. (Někdy se tomuto zobrazení také říká *přirozená projekce* a značívá se π_ρ.) Zřejmě platí $\rho = \ker \mathrm{nat}_\rho$.

Jsou-li $f : A \to B$ a $g : B \to C$ dvě zobrazení, tak jejich složení $g \circ f : A \to C$ je pro každé $a \in A$ dána vztahem $(g \circ f)(a) = g(f(a))$.

1.10 Tvrzení. *Buď $f : A \to B$ zobrazení a ρ ekvivalence na A. Zobrazení $g : A/\rho \to B$, které splňuje $g \circ \mathrm{nat}_\rho = f$, existuje právě když platí $\rho \subseteq \ker f$. Je-li $\rho \subseteq \ker f$, je g určeno jednoznačně, $\ker g = (\ker f)/\rho$ a $(g([a])_\rho) = f(a)$ pro každé $a \in A$.*

Zobrazení g je bijektivní právě když f je surjektivní a platí $\rho = \ker f$.

Důkaz. Pro každé $a \in A$ má platit $g([a])_\rho) = (g \circ \mathrm{nat}_\rho)(a) = f(a)$. Zobrazení g proto nemůže být definováno žádným jiným způsobem. Pro $(a, b) \in \rho$ máme $f(a) = g([a])_\rho) = g([b]_\rho) = f(b)$, takže vskutku musí platit $\rho \subseteq \ker f$. Ať tomu tak opravdu je. Potom z $[a]_\rho = [b]_\rho$ plyne $f(a) = f(b)$, takže g lze skutečně vztahem $g([a]_\rho) = f(a)$ definovat.

Pro $a, b \in A$ máme $g([a]_\rho) = g([b]_\rho)$ právě když platí $(a, b) \in \ker f$. To podle 1.8(i) znamená, že $\ker g$ je rovno $(\ker f)/\rho$.

Jelikož $\mathrm{Im}\, g$ se shoduje s $\mathrm{Im}\, f$, je f surjektivní právě když je g surjektivní. Podle 1.9 lze každou ekvivalenci v A/ρ jednoznačně vyjádřit jako σ/ρ, kde $\sigma \supseteq \rho$. Triviální ekvivalenci $\mathrm{id}_{A/\rho}$ vyjadřuje ρ/ρ, takže g je injektivní právě když $\ker g = (\ker f)/\rho$ se rovná ρ/ρ, čili právě když $\rho = \ker f$. $\square$