INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

Modernizace studijního programu Matematika
na PřF Univerzity Palackého v Olomouci

CZ.1.07/2.2.00/28.0141

Relace, zobrazení, algebraické struktury

Michal Botur

Přednáška 1

KAG/DLA1M: Lineární algebra 1

1 Relace

Cílem je zavést matematický způsob jak modelovat vztahy mezi objekty. V matematice se vyskytuje celá škála vztahů mezi jednotlivými prvky některých množin jako např. rovnost výrazů, podobnost či shodnost geometrických útvarů, uspořádání reálných čísel, množinová inkluze ($\subseteq$) apod. V této přednášce si uvedeme jak se relace modelují pomocí množin a jaké základní typy relací se v matematické teorii vyskytují nejčastěji.

Připomeňme si, že kartézským součinem množin $A \times B$ rozumíme množinu všech dvojic (a, b) takových, že $a \in A$ a $b \in B$. Formálně

$$A \times B = \{(a, b) \mid a \in A, b \in B\}.$$

Definice 1.1 *Binární relací* mezi množinami A a B rozumíme libovolnou podmnožinu $\rho \subseteq A \times B$.

Binární relací na množině A rozumíme libovolnou podmnožinu $\rho \subseteq A^2$.

Slovo „binární“ odkazuje na to, že modelujeme vztahy mezi dvěma objekty. Analogicky se definují např ternární či opecně n-nární relace. Jelikož budeme pracovat výhradně s binárními relacemi, budeme nadále slovo „binární“ vypouštět.

Relaci $\rho \subseteq A \times B$ můžeme chápat jako seznam dvojic (a, b), které jsou v modelovaném vztahu. Například relace $<$ na množině $\mathbb{N}$ je modelována množinou všech dvoji (m, n), kde $m, n \in \mathbb{N}$ a současně $m < n$, tedy množinou

$$\{(m, n) \in \mathbb{N}^2 \mid \exists k \in \mathbb{N} \colon m + k = n\}.$$

Značení relací může vzbuzovat nejasnosti. Definice nám říká, že relace je množina. Ke značení ovšem užíváme obvykle takzvané relační symboly (např. $\leq$, $\sim$, $\|$, $\sqsubseteq$, $\lhd$ apod.). Potom skutečnost, že prvky a a b jsou v relaci $\lhd$ lze značit $(a, b) \in \lhd$, ale obvykleji používáme zápis $a \lhd b$, který ovšem značí totéž.

Pokud používáme pro označení relace znak z některé abecedy (např. ρ), potom opět můžeme použít oba zápisy $(a, b) \in \rho$ či $a\rho b$. Druhý obvyklejší způsop zápisu budu nadále preferovat.

Definice 1.2 Řekneme, že relace ρ na množině A je

i) *reflexivní*, jestliže pro libovolné $a \in A$ platí $a\rho a$,

ii) *symetrická*, jestliže pro libovolné $a, b \in A$ platí, že z $a\rho b$ plyne $b\rho a$,

iii) *tranzitivní*, jestliže pro libovolné $a, b, c \in A$ platí, že z $a\rho b$ a $b\rho c$ plyne $a\rho c$,

iv) *antisymetrická*, jestliže pro libovolné $a, b \in A$ platí, že z $a\rho b$ a $b\rho a$ plyne $a = b$.

v) *asymetrická*, jestliže pro libovolné $a, b \in A$ platí, že z $a\rho b$ plyne, že není pravda $b\rho a$.

Zamyslete se, které z definovaných vlastností mají následující relace: $\leq$ na množině $\mathbb{R}$, $<$ na množině $\mathbb{R}$, rovnoběžnost přímek v rovině, rovnoběžnost na množině všech přímek a rovin v klasickém prostoru (3-dimenzním), být sourozencem na množině lidí (lze definovat dvěma způsoby: osoby jsou sourozenci mají-li oba stejné rodiče nebo mají-li společného alespoň jednoho rodiče; jaký je rozdíl?), apod.

1.1 Relace ekvivalence, faktorizace množiny podle ekvivalence

Definice 1.3 Relace $\sim$ na množině A nazýváme *relace ekvivalence* jestliže je reflexivní, symetrická a tranzitivní

Definice 1.4 Mějme množinu A a systém podmnožin $\{A_i \mid i \in I\}$ (tedy $A_i \subseteq A$ pro všechna $i \in I$). Potom tento systém nazveme *rozkladem množiny A na třídy* jestliže platí

i) pro všechna $i \in I$ platí $A_i \neq \emptyset$,

ii $A = \bigcup_{i \in I} A_i$,

iii) pro libovolné $i, j \in I$ takové, že $i \neq j$ platí $A_i \cap A_j = \emptyset$.

Relace ekvivalence dává do vztahu objekty, které jsou z nějakého hlediska stejně hodnotné (slovo ekvivalence se dá přeložit jako stejnohodnotnost). Rozklad množiny na třídy je „rozdělení“ celé množiny na menší díly, tak že každý prvek padne právě do jedné množiny rozkladu.

Následující věta, která dává tyto pojmy do souvislosti lze demonstrovat na následujícím příkladu. Mějme množinu všech aut. Uvažujme relaci „stejnobarevnost“, která říká, že auta jsou „stejnobarevá“ jestliže mají stejnou barvu. Je snadno vidět, že se jedná o relaci ekvivalenci. Potom můžeme auta roztřídit – tedy vytvořit rozklad množiny aut na menší množiny nazývané třídy – tak, že do každé třídy dáme právě všechna auta, která mají stejnou barvu. Je snadno vidět, že dostaneme rozklad množiny aut na třídy.

Opačně, pokud někdo roztřídil množinu aut (aniž bychom věděli podle jakého kritéria tak učinil), můžeme definovat ekvivalenci takovou, že auta jsou ekvivalentní právě tehdy, leží-li v jedné třídě. Touto konstrukcí obdržíme z rozkladu ekvivalenci.

Taktéž platí, že tyto dvě konstrukce popisují vzájemně jednoznačný vztah mezi relacemi a rozklady na množině.

Věta 1.1 *1) Jestliže $\sim$ je relace ekvivalence na množině A. Označíme-li*

$$[a]_\sim = \{x \in A \mid a \sim x\},$$

potom množina $A/\!\sim = \{[a]_\sim \mid a \in A\}$ je rozklad množiny A na třídy.

2) Jestliže $R = \{A_i \mid i \in I\}$ je rozklad množiny A na třídy, potom relace $\sim_R$ definovaná předpisem

$$a \sim_R b \text{ tehdy a jen tehdy, jestliže existuje } i \in I \text{ takové, že platí } a, b \in A_i.$$

3) Korespondence mezi rozklady a ekvivalencemi popsané v bodech 1) a 2) jsou vzájemně jednoznačné. Tedy $\sim_{(A/\sim)}$ je rovno relaci $\sim$ a $R = A/\!\sim_R$ pro libovolný rozklad R a ekvivalenci $\sim$ na množině A.

1.2 Zobrazení, operace a algebraické struktury s jednou a dvěma binárními operacemi

Dalším důležitým pojmem v teoretické matematice je zobrazení. Jestliže máme dvě množiny A a B, potom zobrazením f z množiny A do množiny B rozumíme libovolné přiřazení, které každému prvku z množiny A přiřadí jediný prvek z množiny B. Obvykle potom značíme $f\colon A \longrightarrow B$ skutečnost, že f je zobrazením z A do B. Skutečnost, že prvek $a \in A$ se zobrazí na $b \in B$ značíme $f(a) = b$ nebo $f\colon a \mapsto b$. Ukážeme si, že zobrazení je speciálním případem relace mezi množinami A a B. Lze si ji představit jako seznam všech dvojic, kde v prvních složkách jsou obrazy a v druhých vzory.

Speciálním případem zobrazení jsou operace. Příkladem operací je například sčítání reálných čísel, které každým dvěma číslům přiřadí jejich součet. Jestliže na množině máme definovány nějaké operace dostáváme takzvané algebry.

Definice 1.5 Mějme množiny A a B, potom řekneme, že binární relace $f \subseteq A \times B$ je zobrazení, jestliže pro každý prvek $a \in A$ existuje jediný prvek $b \in B$ takový, že platí $(a, b) \in f$.

Nenechte se zmást tím, že jedna skutečnost se dá zapsat několika způsoby. Například v případě zobrazení $f\colon A \longrightarrow B$ značí zápisy $f(a) = b$, $(a, b) \in f$ i afb totéž. Důvody těchto rozdílnosti jsou víceméně historické. Zjednodušeně řečeno, relační zápis i zápis pro zobrazení se zavedl dávno před vynálezem množin a před sjednocením matematických pojmů pomocí množin.

Definice 1.6 Mějme zobrazení $f\colon A \longrightarrow B$, potom řekneme, že f je

i) *injektivní*, jestliže pro libovolné dva prvky $a_1, a_2 \in A$ platí, že z rovnosti $f(a_1) = f(a_2)$ plyne rovnost $a_1 = a_2$.

ii) *surjektivní*, jestliže pro libovolné $b \in B$ existuje $a \in A$ takové, že $f(a) = b$.

iii) *bijektivní* nebo *vzájemně jednoznačné*, jestliže je injektivní i surjektivní současně.

Injektivita říká, že dva různé prvky mají i různé obrazy. Surjektivita říká, že na každý prvek z množiny obrazů se zobrazí některý vzor. Bijektivita nám říká, že každý prvek z množiny obrazů má jediný vzor. Toto nám umožňuje zavést takzvané inverzní zobrazení.

Věta 1.2 *Jestliže $f\colon A \longrightarrow B$ je bijektivní zobrazení, potom existuje jediné zobrazení $f^{-1}\colon B \longrightarrow A$ takové, že platí*

$$f(a) = b \text{ tehdy a jen tehdy, jestliže } f^{-1}(b) = a.$$

Toto zobrazení nazýváme inverzní zobrazení k zobrazení f.

Určete, které z funkcí $\mathbb{R} \longrightarrow \mathbb{R}$ jsou injektivní, surjektivní nebo bijektivní (uvažujte například funkce x^2, x^3, sin, e^x, tg apod.).

Definice 1.7 Mějme zobrazení $f\colon A \longrightarrow B$ a $g\colon B \longrightarrow C$, potom *složením zobrazení f a g* (značíme $f \circ g$) rozumíme zobrazení $f \circ g\colon A \longrightarrow C$ definované předpisem

$$(f \circ g)(x) = g(f(x)).$$

V některých matematických oborech, především v matematické analýze, je obvyklé zavádět skládání „opačně“ pomocí $(g \circ f)(x) = g(f(x))$. Obě značení mají jistou logiku a jsou v něčem názorná. Pro Vás to ale znamená, e je třeba si předem ověřit, kterým způsobem je v používané literatuře složení zavedeno.

Věta 1.3 *1) Jestliže $f\colon A \longrightarrow B$, $g\colon B \longrightarrow C$ a $h\colon C \longrightarrow D$ jsou zobrazení, potom platí*

$$f \circ (g \circ h) = (f \circ g) \circ h.$$

2) Jestliže $f\colon A \longrightarrow B$ je bijekce, potom pro libovolné $a \in A$ a $b \in B$ platí, že $(f \circ f^{-1})(a) = a$ a $(f^{-1} \circ f)(b) = b$.

Definice 1.8 Mějme množinu A, potom n-nární operací rozumíme libovolné zobrazení $F\colon A^n \longrightarrow A$.

V našem výkladu se budeme zabývat pouze binárními operacemi $A^2 \longrightarrow A$. Příkladem operací mohou být $+$, $\cdot$, $-$, $\cap$ apod. Z historických důvodů se opět zobrazování pomocí operací značí $2 + 3 = 5$ místo, pro zobrazení jinak obvyklejšího, $+(2, 3) = 5$.

Definice 1.9 Mějme množinu A a na ní definovanou binární operaci $*\colon A^2 \longrightarrow A$. Potom řekneme, že algebra $(A;*)$ je *grupoid*.

Jestliže grupoid splňuje takzvaný asociativní zákon, který říká, že pro libovolné $a,b,c \in A$ platí

$$a*(b*c) = (a*b)*c,$$

potom řekneme, že $(A;*)$ je *pologrupa*.

Prvek $e \in A$ se nazývá *neutrální prvek*, jestliže pro libovolné $a \in A$ platí $e*a = a = a*e$. Pologrupa s neutrálním prvkem se nazývá *monoid*.

Jestliže máme monoid s neutrálním prvkem e, potom řekneme, že prvek a' je inverzní k prvku a jestliže platí $a'*a = e = a*a'$. Monoid takový, že ke každému prvku existuje prvek inverzní se nazývá *grupa*.

Grupoid, pologrupa, monoid nebo grupa se nazývá *komutativní*, jestliže splňuje tzv. komutativní zákon, který říká, že pro libovolné $a,b \in A$ platí $a*b = b*a$.

Věta 1.4 *V každé pologrupě existuje nejvýše jeden neutrální prvek. V každém monoidu existuje ke každému prvku nejvýše jeden inverzní prvek.*

Věta 1.5 *Značíme-li v grupě a' inverzní prvek k prvku a, potom platí $(a')' = a$.*

Uvažujte operace $+$, $\cdot$ a $-$ na jednotlivých číselných oborech $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ či $\mathbb{C}$. Určete o jakou se jedná strukturu. V případě, že se jedná o monoid určete neutrální prvek, v případě grupy najděte inverzní prvky.

Značíme-li $\wp(A)$ množinu všech podmnožin množiny A (formálně přesně $\wp(A) = \{X \mid X \subseteq A\}$). Dokažte, že $(\wp(A),\cup)$ a $(\wp(A),\cap)$ jsou monoidy a najděte jejich neutrální prvky.

Definice 1.10 Mějme množinu A a na ní definovány binární operace $+$ a $\cdot$. Potom řekneme, že

i) $(A;+,\cdot)$ je *okruh* jestliže $(A;+)$ je komutativní grupa, $(A;\cdot)$ je pologrupa a platí tzv. distributivní zákony; tj. pro libovolné $a,b,c \in A$ platí

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

$$(a+b)\cdot c = (a\cdot c)+(b\cdot c).$$

Neutrální prvek v grupě $(A;+)$ obvykle nazýváme *nulový prvek*, inverzní prvek k prvku a nazýváme *opačný prvek* a značíme jej $-a$.

ii) $(A;+,\cdot)$ je *těleso*, jestliže se jedná o okruh takový, že struktura $(A\setminus\{0\},\cdot)$ je grupa.

Okruh nebo těleso se nazývá komutativní, jestliže $(A;\cdot)$ je komutativní.

! Operace $+$ a $\cdot$ v definici okruhu a tělesa nemusí nutně značit klasické sčítání či násobení čísel, přestože v našem případě nebudeme užívat jiná tělesa než $\mathbb{R}$ či $\mathbb{Q}$. Například v teoretické informatice je užitečné zavést operace $+$ a $\cdot$ na dvouprvkové množině $\{0,1\}$ tak, že výsledná struktura je těleso (oproti přirozenému sčítání a násobení zde pouze zavedeme $1+1=0$).

Reference

[1] D. Hort, J. Rachůnek: Algebra I., [Univerzita Palackého V Olomouci, 2003].

[2] Bican L.: Lineární algebra, [SNTL Praha, 1979.].

[3] Waerden, L.: Algebra I., [Springer-Verlag Berlin, Heidelberg, New York, 1971.].